



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

ANEXO I

APÊNDICE A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE TIC

1. Item 1 - Subscrição Symantec Endpoint Security Complete – SKU: SESC-SES-CLD-SUB

1.1.A Subscrição Symantec Endpoint Security Complete deve fornecer uma defesa contra malware para laptops, desktops e servidores e combinar no mínimo os módulos e serviços:

1.1.1. Antivírus com uma prevenção avançada contra ameaças;

1.1.2. IPS / IDS;

1.1.3. Firewall;

1.1.4. Serviço de proteção para dispositivos móveis;

1.1.5. Proteção contra exploração do ambiente Active Directory;

1.2. Características gerais dos módulos

1.2.1. Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

1.2.2. Fornecer console de gerenciamento do módulo;

1.2.3. Implementar, no mínimo, as seguintes funcionalidades e tecnologias:

1.2.3.1. Reputação de Arquivos tanto locais, quanto no acesso web;

1.2.3.2. Aprendizado de Máquinas (Machine Learning);



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.2.3.3. Análise Comportamental (Behavioral Analysis);
 - 1.2.3.4. IPS de Próxima Geração (Next Generation IPS);
 - 1.2.3.5. Proteção de Navegadores (Browser Protection);
 - 1.2.3.6. Proteção contra ameaças avançadas ou persistentes;
 - 1.2.3.7. Mitigação da Exploração de Memória (Memory Exploit Mitigation);
 - 1.2.3.8. Controle de Aplicações (Application Control);
 - 1.2.3.9. Redução da superfície de Ataque ao ambiente;
 - 1.2.3.10. Controle de Dispositivos (Device Control);
 - 1.2.3.11. Emulação para Malware (Emulation for Malware);
 - 1.2.3.12. Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas (Exploit Mitigation); e
 - 1.2.3.13. Verificação em real-time das assinaturas e heurística dos arquivos recebendo as últimas informações do arquivo durante a tarefa de scan protegendo contra outbreaks e novos malwares.
- 1.2.4. A solução deve ter integração com terceiros para ferramentas de Ticketing, Orquestração e Automação e SIEM, para no mínimo:
- 1.2.4.1. Splunk;
 - 1.2.4.2. ServiceNow;
- 1.2.5. A solução de proteção dos endpoints deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações, para no mínimo:
- 1.2.5.1. Adobe PDF;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.2.5.2. Flash;
- 1.2.5.3. Java;
- 1.2.5.4. Navegadores (Internet Explorer, Chrome e Firefox);
- 1.2.6. A solução de proteção do endpoint deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades:
 - 1.2.6.1. SEHOP - Structured Exception Handler Overwrite Protection;
 - 1.2.6.2. Heap Spray (Exploits que iniciam através do HEAP);
 - 1.2.6.3. Java Security Manager;
 - 1.2.6.4. ForceDEP;
 - 1.2.6.5. ForceASLR;
 - 1.2.6.6. NullProt (Null Page Protection);
 - 1.2.6.7. DllLoad;
 - 1.2.6.8. RopCall;
 - 1.2.6.9. RopFlow;
 - 1.2.6.10. StackNX;
- 1.2.7. A solução de proteção do endpoint deve ter a capacidade de bloquear exploits que trabalham em nível de “shell code”, assim como, implementar a funcionalidade de “virtual patching” para as aplicações;
- 1.2.8. Deve ter a capacidade de receber instruções de comando e ações diretamente do módulo de proteção contra ataques de APT (Advanced Persistent Threats), sem a necessidade de interpretação pelo gerenciador



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

do endpoint, possibilitando ações mais rápidas, assertivas e minimizando falsos positivos;

- 1.2.9. Deve possuir reputação de arquivos atualizada em tempo real, para proteção ao acesso a Web sites, defendendo contra mutação dos malwares;
- 1.2.10. A solução deve ter a capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;
- 1.2.11. Deve ter a capacidade de implementar no agente de proteção do endpoint funcionalidades de deception, para no mínimo:
 - 1.2.11.1. Possibilitar a detecção de movimentações laterais dentro do ambiente;
 - 1.2.11.2. Distribuir iscas no ambiente com o objetivo de detectar e interromper tentativas de infiltração;
 - 1.2.11.3. Criar entradas falsas de cache, como Cache de DNS, a fim de enganar um atacante e aplicações maliciosas, identificando ações maliciosas no ambiente;
 - 1.2.11.4. Possibilitar a criação de arquivos falsos nas máquinas dos usuários;
 - 1.2.11.5. Possibilitar a criação e distribuição de senhas falsas nos sistemas afim de identificar atacantes no ambiente;
 - 1.2.11.6. Criação de compartilhamentos de rede falsos em desktops;
 - 1.2.11.7. Enviar alertas quando as “Isclas” falsas são acionadas e/ou modificadas;
 - 1.2.11.8. Revelar tentativas de ataques dentro da rede interna;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.2.11.9. Possuir integração nativa com a Solução para Prevenção de Ataques Avançados via SandBox, permitindo visibilidade, análise, bloqueio e remediação contra ameaças avançadas e de dia-zero nas estações de trabalho e servidores;

1.2.12. Funcionalidades de Compliance e Controle de Acesso à Rede possibilitando a colocação dos equipamentos em quarentena, restringindo o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:

1.2.12.1. Computador deve possuir antivírus, atualizados e ativo;

1.2.12.2. Computador deve possuir firewall ativo;

1.2.12.3. Computador deve possuir antispymware, atualizado e ativo;

1.2.12.4. Computador deve possuir patches instalados, ativos e atualizados;

1.2.12.5. Deve ter a capacidade de iniciar a auto remediação do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;

1.2.12.6. Deve ter a capacidade de alterar automaticamente as regras de firewall nos clientes que falharam na política restringindo o acesso a rede;

1.2.12.7. A auto remediação deve suportar download de programas e arquivos por links de HTTP, FTP e UNC;

1.2.12.8. Deve ter a possibilidade de notificação customizada para o usuário com diferentes ícones e como erro, informação e notificação;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.2.12.9. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre máquinas que não estiverem em conformidade com as políticas do controle de acesso à rede;

1.2.13. Funcionalidade de Quarentena

1.2.13.1. Permite o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;

1.2.13.2. Permite de forma automática o envio dos arquivos da área de isolamento central para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador. Recebimento utilizando o mesmo método e aplicação da vacina recém-criada nas estações infectadas;

1.2.13.3. Possibilita adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;

1.2.13.4. Possibilita o rastreamento agendado contra vírus com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear com periodicidade mínima diária;

1.2.13.5. Possibilita o rastreamento remoto contra vírus com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear;

1.2.14. Funcionalidade de Atualização das vacinas

1.2.14.1. Atualização incremental, remota e em tempo real, da vacina dos Antivírus e mecanismo de verificação (Engine) dos clientes da rede;

1.2.14.2. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, Site do fabricante, Via Servidor de atualização interno e podendo



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

eleger qualquer cliente gerenciado para distribuição das atualizações;

1.2.14.3. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições e espaço em disco utilizado, podendo eleger mais de um cliente para esta função;

1.2.14.4. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la;

1.2.14.5. Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;

1.2.14.6. Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor, utilizando opção e comando do Console podendo utilizar a arquitetura de grupos lógicos da console;

1.2.14.7. Um único e mesmo arquivo de vacina de Vírus para todas as plataformas Windows e versões do antivírus;

1.2.15. Características dos clientes gerenciados

1.2.15.1. Deve ter a capacidade de integrar de forma nativa com a solução de APT do mesmo fabricante, sem a necessidade da implementação de scripts, utilizando apenas configurações realizadas na console padrão da solução;

1.2.15.2. Suportar máquinas com arquitetura 32-bit e 64-bit;

1.2.15.3. O cliente para instalação em estações de trabalho deverá possuir compatibilidade com no mínimo os sistemas operacionais:



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.2.15.3.1. Windows Server 2008, 2008 R2;
- 1.2.15.3.2. Windows Server 2012, 2012 R2;
- 1.2.15.3.3. Windows Server 2016 e 2019;
- 1.2.15.3.4. Windows 7;
- 1.2.15.3.5. Windows 8 e 8.1;
- 1.2.15.3.6. Windows 10 incluso update de maio de 2019;
- 1.2.15.3.7. Mac OS X 10.10 até 10.14;
- 1.2.15.3.8. Red Hat Enterprise Linux;
- 1.2.15.3.9. Debian;
- 1.2.15.3.10. Oracle Linux;
- 1.2.15.3.11. Novell Open Enterprise Server;
- 1.2.15.3.12. SUSE Linux Enterprise (server e desktop);
- 1.2.15.3.13. Fedora;
- 1.2.15.3.14. Ubuntu;
- 1.2.15.3.15. Amazon Linux;
- 1.2.15.3.16. CentOS;
- 1.2.15.4. O cliente para instalação em servidores deverá possuir compatibilidade com no mínimo os sistemas operacionais:
 - 1.2.15.4.1. Windows Server 2008, 2008 R2;
 - 1.2.15.4.2. Windows Small Business Server 2011 (64-bit);



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.2.15.4.3. Windows Server 2012, 2012 R2;
- 1.2.15.4.4. Windows Server 2016;
- 1.2.15.4.5. Windows Server 2019;
- 1.2.15.5. O cliente para instalação em servidores deverá possuir certificação FIPS 140-2;
- 1.2.15.6. O cliente para instalação em estações de trabalho deverá possuir:
 - 1.2.15.6.1. Compatibilidade com o sistema operacional Mac OSX e Linux para as funcionalidades de antivírus, anti-spyware, firewall e EDR;
 - 1.2.15.6.2. Suporte ao Apple Remote Desktop para instalação e atualização remota da solução;
 - 1.2.15.6.3. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-troia, spyware, adwares e outros tipos de códigos maliciosos;
 - 1.2.15.6.4. Permitir que verificação das ameaças da maneira manual e agendada;
 - 1.2.15.6.5. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;
 - 1.2.15.6.6. Permitir a ações de reparar arquivo ou por em quarentena em caso de infecções a arquivos;
 - 1.2.15.6.7. Suporte a instalação de clientes Linux para as distribuições:
 - 1.2.15.6.8. Red Hat Enterprise Linux;
 - 1.2.15.6.9. CentOS Linux;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.2.15.6.10. Ubuntu Server;

1.3. Módulo de gerenciamento híbrido

1.3.1. Console de gerenciamento on-premises

- 1.3.1.1.1. Não deverá onerar em custo a utilização de consoles adicionais, conforme necessidade;
- 1.3.1.1.2. Deve ter administração centralizada da solução por console único de gerenciamento;
- 1.3.1.1.3. Deve ter acesso a console de gerenciamento via tecnologia Web (HTTP e HTTPS);
- 1.3.1.1.4. Deve estabelecer uma correlação de eventos entre os softwares gerenciados, possibilitando priorização nas ações tomadas;
- 1.3.1.1.5. Deve possibilitar a realização das configurações de todos os módulos e serviços, tanto para máquinas físicas quanto virtuais por meio de uma console única
- 1.3.1.1.6. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;
- 1.3.1.1.7. Mecanismo de comunicação randômico (via pull) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;
- 1.3.1.1.8. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.1.1.9. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2008, 2008 R2 ou superior;
- 1.3.1.1.10. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais 32-bit e 64-bit suportando ambiente virtual XEN, VMWARE e Microsoft;
- 1.3.1.1.11. Possuir integração com LDAP, para importação da estrutura organizacional e autenticação dos Administradores;
- 1.3.1.1.12. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;
- 1.3.1.1.13. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:
 - 1.3.1.1.13.1. IP e range de IP;
 - 1.3.1.1.13.2. Endereço de Servidores de DNS, DHCP e WINS;
 - 1.3.1.1.13.3. Conexão com o servidor de gerência;
 - 1.3.1.1.13.4. Conexões de rede como VPN, Ethernet, Wireless e Modem;
- 1.3.1.1.14. Possuir suporte a IPv6;
- 1.3.1.1.15. Possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;
- 1.3.1.1.16. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server nas versões 2008, 2012, 2014, 2016, 2017 e superior;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.1.1.17. Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados ou fornecer uma ferramenta para tal finalidade;
- 1.3.1.1.18. Permitir a opção de instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover;
- 1.3.1.1.19. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);
- 1.3.1.1.20. Possibilidade de instalação dos clientes em endpoints físicos e virtuais de forma remota via console de gerenciamento com opção de remoção de soluções previamente instaladas;
- 1.3.1.1.21. Permitir a instalação remota do software por Group Policy (GPO), Web e via console de gerenciamento;
- 1.3.1.1.22. Descobrir automaticamente os endpoints da rede que não possuem o cliente instalado;
- 1.3.1.1.23. Fornecer ferramenta de pesquisa de endpoints da rede que não possuem o cliente instalado com opção de instalação remota;
- 1.3.1.1.24. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
- 1.3.1.1.25. A console de gerenciamento deve permitir travar as configurações por senha nos endpoints físicos e virtuais definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.1.1.26. A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada subitens de acesso as configurações do cliente;
- 1.3.1.1.27. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;
- 1.3.1.1.28. Instalação e atualização do software sem a intervenção do usuário;
- 1.3.1.1.29. Atualização remota e incremental da versão do software cliente instalado;
- 1.3.1.1.30. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;
- 1.3.1.1.31. Suportar redirecionamentos dos logs para um servidor de Syslog;
- 1.3.1.1.32. Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado;
- 1.3.1.1.33. Console de gerenciamento via tecnologia Web (HTTP e HTTPS) independente da console central da solução;
- 1.3.1.1.34. Possibilidade de executar inventário do ambiente e descobrir os antivírus e respectivas versões;
- 1.3.1.1.35. Detectar e desinstalar soluções de antivírus dos seguintes fabricantes:
 - 1.3.1.1.35.1. CA
 - 1.3.1.1.35.2. ESET
 - 1.3.1.1.35.3. F-Secure



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.1.1.35.4. Kaspersky
- 1.3.1.1.35.5. McAfee
- 1.3.1.1.35.6. Sophos
- 1.3.1.1.35.7. Symantec
- 1.3.1.1.35.8. Trend Micro
- 1.3.1.1.36. Permitir a remoção de outros softwares não desejados;
- 1.3.1.1.37. Criar tarefas de migração baseadas no resultado do inventário de antivírus;
- 1.3.1.1.38. Permitir agendamento e implementar controle de banda para minimizar impacto na rede durante o processo de instalação em clientes;
- 1.3.1.1.39. Possibilidade de recuperar instalação em clientes em caso de falha;
- 1.3.1.1.40. A solução deve ter a capacidade de implementar senha de proteção do endpoint, para no mínimo:
 - 1.3.1.1.40.1. Solicitar senha para abrir a interface do usuário no cliente local;
 - 1.3.1.1.40.2. Solicitar senha para parar o serviço do endpoint;
 - 1.3.1.1.40.3. Solicitar senha para desinstalação do endpoint;
 - 1.3.1.1.40.4. Solicitar senha para importar, assim como, exportar políticas;
 - 1.3.1.1.40.5. Solicitar senha para importar configuração da comunicação entre cliente e gerência;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.1.1.41. Possuir, pelo menos, 20 tipos de relatórios diferentes, permitindo a exportação para o formato HTML;
- 1.3.1.1.42. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;
- 1.3.1.1.43. Possibilidade de exibir a lista de endpoints que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status;
- 1.3.1.1.44. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:
- 1.3.1.1.45. As 10 máquinas com maior ocorrência de códigos maliciosos;
- 1.3.1.1.46. Os 10 usuários com maior ocorrência de códigos maliciosos;
- 1.3.1.1.47. Localização dos códigos maliciosos;
- 1.3.1.1.48. Sumários das ações realizadas;
- 1.3.1.1.49. Número de infecções detectadas diário, semanal e mensal;
- 1.3.1.1.50. Códigos maliciosos detectados;
- 1.3.1.1.51. Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot;
- 1.3.1.1.52. No mínimo, os seguintes cubos devem ser disponibilizados para criação de relatórios:
 - 1.3.1.1.52.1. Alertas;
 - 1.3.1.1.52.2. Clientes;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.1.1.52.3. Políticas;

1.3.1.1.52.4. Rastreamento;

1.3.1.1.53. Possibilidade de criação de indicadores de performance para medir eficácia da solução de segurança;

1.3.1.1.54. Exportar os relatórios criados nos formatos xls, pdf e html;

1.3.2. Console de gerenciamento em nuvem

1.3.2.1. Não deverá incorrer em custo adicional para disponibilização de console centralizada em nuvem;

1.3.2.2. A solução a partir da console em nuvem deverá possibilitar a criação de pacotes de instalação dos endpoints para instalação remota;

1.3.2.3. A solução deverá possibilitar a gerência dos clientes apenas por seu módulo em nuvem, sem a necessidade de comunicação com o sistema de gerenciamento on-premises

1.3.2.4. A solução não necessitará da instalação de nenhum componente local extra para comunicação com a gerência em nuvem, sem necessidade de hubs, servidores e bancos de dados;

1.3.2.5. A solução deverá possibilitar autenticação Single Sign-On com a gerência e, a partir da mesma console em nuvem, possibilitar a gerência dos módulos de proteção do endpoint, proteção de mobile (Mobile Threat Defense - MTD); proteção para ativos exclusivos em nuvem e endpoint data loss prevention;

1.3.2.6. A solução deverá ter a capacidade de verificar em um único ponto todos os eventos relacionados com o endpoint e suas várias tecnologias em uso, gerenciadas pela console em nuvem;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.2.7. A solução deverá possibilitar a migração da console local para a console em nuvem, onde políticas implementadas de forma local que ainda não foram ajustadas terão precedência no endpoint;
- 1.3.2.8. A solução deverá possibilitar um gerenciamento híbrido, com endpoints sendo gerenciados pela console em nuvem e endpoints gerenciados pela console on-premises;
- 1.3.2.9. A solução deve ter a capacidade de orientar os administradores da ferramenta, a partir da console de gerenciamento de forma desassistida, ou seja, sem a intervenção do administrador, com o fornecimento de recomendações de operação, atualizações de políticas, automatização de tarefas e respostas a incidentes utilizando técnicas de inteligência artificial tal como "machine learning";
- 1.3.2.10. A solução deve ter a capacidade de orientar o gerenciamento de segurança dos endpoints a partir da implementação de Inteligência Artificial, possibilitando no mínimo:
 - 1.3.2.10.1. Simplificar fluxos de trabalho para eliminar tarefas de rotina;
 - 1.3.2.10.2. Avaliar e fortalecer continuamente a postura de segurança através do "machine learning" aplicado ao gerenciamento de segurança;
 - 1.3.2.10.3. Implementar Recomendações de segurança automaticamente indicando a justificativa;
 - 1.3.2.10.4. Aplicar no ambiente as Recomendações elencadas, conforme identificado pela Inteligência Artificial que seria uma ação do administrador;
 - 1.3.2.10.5. Retroalimentar a Inteligência Artificial da solução tornando o processo mais assertivo;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.2.10.6. Autogerenciar sua própria segurança, onde fluxos de trabalho se simplificam a cada ciclo de execução;
- 1.3.2.10.7. Indicar as correções das configurações incorretas de segurança, com recomendações sensíveis ao contexto;
- 1.3.2.10.8. Responder de forma automática as epidemias;
- 1.3.2.11. A solução deve ter capacidade de implementar controles de segurança e fluxos de trabalho integrados utilizando inteligência artificial e insights compartilhados, onde incidentes e políticas são ajustados continuamente protegendo o ambiente de eventos semelhantes no futuro.
- 1.3.2.12. A solução deve ter capacidade de implementar a autocorreção, não havendo necessidade de correlações manuais de eventos de segurança detectados, uma vez que o veredicto quanto aos ataques ou comportamento identificado de forma similar por várias tecnologias, através de interações automatizadas entre os recursos, possibilitando que as ações dos administradores sejam simplificadas;
- 1.3.2.13. A solução deve ter capacidade de implementar a partir do seu autogerenciamento a automação de políticas em qualquer fase do ciclo de vida da gerência de segurança, para no mínimo as seguintes fases:
 - 1.3.2.13.1. Avaliação;
 - 1.3.2.13.2. Classificação;
 - 1.3.2.13.3. Recomendação;
 - 1.3.2.13.4. Implementação;
 - 1.3.2.13.5. Aprendizado;
 - 1.3.2.13.6. Administração;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.2.14. A solução deve ter a capacidade de adicionar, renomear, editar, deletar e alterar senha dos administradores;
- 1.3.2.15. A solução deve ter a capacidade de a partir dos super administradores de criar, editar e deletar configurações de todos os domínios licenciados para o cliente;
- 1.3.2.16. A solução deve ter a capacidade de a partir dos administradores de criar, editar e deletar configurações de um dos domínios licenciados para o cliente;
- 1.3.2.17. A solução deve ter a capacidade de a partir dos administradores limitados de criar, editar configurações de todos dos domínios licenciados para o cliente, mas sem a capacidade de rodas comandos e configurações de políticas;
- 1.3.2.18. A solução deve ter a capacidade de a partir dos usuários de visualização em visualizar todas as configurações de todos os domínios licenciados para o cliente;
- 1.3.2.19. A solução deve ter a capacidade de implementar autenticação via SAML 2.0;

1.3.3. Relatórios e Modelos;

- 1.3.3.1. A solução deve ter a capacidade de emitir relatórios para no mínimo:
 - 1.3.3.1.1. Controle de Aplicações;
 - 1.3.3.1.2. Controle de Dispositivos, sendo no mínimo:
 - 1.3.3.1.3. TOP 5 dispositivos bloqueados;
 - 1.3.3.1.4. KPI – Key Performance Indicators;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.3.1.5. Total de equipamentos com dispositivos externos bloqueados;
- 1.3.3.1.6. Total de dispositivos externos bloqueados;
- 1.3.3.1.7. Lista de dispositivos externos gerenciados;
- 1.3.3.1.8. Reportar os eventos dos dispositivos externos bloqueados;
- 1.3.3.2. A solução deve ter a capacidade de fornecer modelos de relatórios, para no mínimo:
 - 1.3.3.2.1. Relatório Diário padrão;
 - 1.3.3.2.2. Relatório Semanal padrão;
 - 1.3.3.2.3. Relatório padrão de IPS;
 - 1.3.3.2.4. Relatório de Isolamento de Aplicação;

1.3.4. Características Gerais dos Clientes MAC e Windows;

- 1.3.4.1. A solução deve ter a capacidade de implementar pacotes de instalação Windows e MAC, possibilitando no mínimo:
 - 1.3.4.1.1. Pacotes para instalação direta;
 - 1.3.4.1.2. Pacotes para distribuição de instalação;
 - 1.3.4.1.3. Pacotes de instalação por e-mail (web link);
 - 1.3.4.1.4. Pacotes de instalação via download e instalação local;

1.3.5. Características Gerais dos Clientes LINUX;

- 1.3.5.1. A solução deve ter a capacidade de implementar pacotes de instalação LINUX, possibilitando:



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.5.1.1. Pacote para instalação direta;

1.3.5.1.2. Pacote para distribuição de instalação.

1.3.6. Quanto às características específicas das políticas da solução:

1.3.6.1. A solução deverá ter a capacidade de implementar políticas de proteção intensiva possibilitando combinar as tecnologias de heurística real-time, reputação de arquivos locais, reputação em real-time de arquivos em nuvem e sites web, assim como heurística na assinatura do antivírus;

1.3.6.2. A solução deverá ter a capacidade de implementar a partir da mesma console no mínimo:

1.3.6.2.1. Políticas de Firewall;

1.3.6.2.2. Políticas de IPS (Intrusion Prevention);

1.3.6.2.3. Políticas de Proteção contra Exploração de Memória;

1.3.6.2.4. Políticas de Controle de Aplicações (Application Control);

1.3.6.2.5. Políticas de Controle de Dispositivos (Device Control);

1.3.6.2.6. Políticas de Análise Comportamental (Behavior analysis);

1.3.6.2.7. Políticas de Whitelist e Blacklist;

1.3.6.2.8. Políticas de Antimalware;

1.3.6.2.9. Políticas de Isolamento de Aplicações;

1.3.6.2.10. Políticas de Isolamento de Navegadores;

1.3.6.3. A solução deve ter a capacidade de implementar políticas de Blacklist e Hardening de aplicações e Sistema Operacional;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.6.4. A solução deve ter a possibilidade de implementar modelos de políticas de forma nativa, baseadas em políticas enviadas pelo fabricante, as quais devem ser atualizadas periodicamente de forma automática pelo fabricante da solução, onde a cada atualização corresponderá a uma versão específica;

1.3.6.5. A solução deverá fornecer políticas modelos para ao menos:

- 1.3.6.5.1. Políticas de Antimalware;
- 1.3.6.5.2. Políticas de Proteção contra Exploração de Memória;
- 1.3.6.5.3. Políticas de Controle de Aplicações;
- 1.3.6.5.4. Políticas de Controle de Dispositivo;
- 1.3.6.5.5. Políticas de Controle e Integridade de Rede;
- 1.3.6.5.6. Políticas de Quarentena de Dispositivo;
- 1.3.6.5.7. Políticas de Blacklist;
- 1.3.6.5.8. Políticas de Whitelist;
- 1.3.6.5.9. Política de EDR;
- 1.3.6.5.10. Políticas de redução da superfície de ataque e isolamento de aplicativos;
- 1.3.6.5.11. Políticas de Isolamento de Navegadores;
- 1.3.6.5.12. Políticas de Isolamento do Office;
- 1.3.6.5.13. Políticas de Isolamento de Aplicações;

1.3.6.6. A solução deve ter a capacidade de criar políticas, sem a necessidade de colocá-las em produção imediatamente após sua



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

criação, possibilitando ao administrador da ferramenta elaborar com mais cuidado sua criação;

1.3.7. Funcionalidades dos Módulos e Serviços

- 1.3.7.1. A solução deve ter capacidade de implementar minimamente os seguintes módulos e serviços a partir de um único agente;

1.3.8. Funcionalidades de Antivírus e AntiSpyware

- 1.3.8.1. Antivirus Scanning, trabalhando com assinaturas e heurística para eliminar malware incluindo virus, worms, Trojans, spyware, bots, adware, rootkits;
- 1.3.8.2. Funcionalidades de Antivírus e AntiSpyware deverá proteger em tempo real contra vírus, trojans, worms, cavalos-de-troia, spyware, adwares e outros tipos de códigos maliciosos;
- 1.3.8.3. Proteção anti-spyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;
- 1.3.8.4. As configurações do anti-spyware deverão ser realizadas através da mesma console de todos os itens da solução;
- 1.3.8.5. Atualizar reputação de arquivos em real-time protegendo o acesso à Web sites, defendendo contra mutação dos malwares;
- 1.3.8.6. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (Adware, Ferramentas de hacker, Programas de brincadeiras, Acesso remoto, Spyware, Trackware e outros);
- 1.3.8.7. Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.8.8. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis: baixo, médio ou alto, nas quais somente os riscos selecionados serão verificados pelo produto;
- 1.3.8.9. Permitir verificação das ameaças de forma manual, agendada e em Tempo Real, para detectar ameaças no nível do Kernel do Sistema Operacional, possibilitando assim a detecção de Rootkits;
- 1.3.8.10. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais;
- 1.3.8.11. Possuir funcionalidades que permitam o isolamento em área de quarentena de arquivos contaminados por códigos maliciosos, que não sejam conhecidos ou que não possam ser reparados no cliente;
- 1.3.8.12. Possuir funcionalidades que permitam o isolamento manual em área de quarentena de arquivos a serem enviados e vistoriados pelo centro de pesquisa do fabricante;
- 1.3.8.13. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar;
- 1.3.8.14. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes no mínimo Outlook e POP3/SMTP;
- 1.3.8.15. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados por ZIP, LHA e ARJ, tendo como abrangência até o 10º (décimo) nível de compactação;
- 1.3.8.16. Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção da sensibilidade da detecção (baixo, médio e alto);



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.8.17. Capacidade de remoção total automática das modificações feitas por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção;
- 1.3.8.18. A remoção automática das modificações feitas deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin, execução de arquivo ou módulo adicional;
- 1.3.8.19. Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede;
- 1.3.8.20. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;
- 1.3.8.21. Criar um backup do arquivo suspeito antes de limpá-lo;
- 1.3.8.22. Gerenciamento integrado à console da solução;
- 1.3.8.23. Possibilitar a criação de um disco (CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;
- 1.3.8.24. Capacidade de executar varreduras em tempo real contra ataques dirigidos à vulnerabilidades do navegador web;
- 1.3.8.25. A solução deve possuir escalabilidade para crescimento futuro suportando a utilização no mínimo dos ambientes virtuais abaixo, com seu uso já licenciado e habilitado sem custo a mais para o Órgão:
 - 1.3.8.25.1. Windows Azure;
 - 1.3.8.25.2. Amazon WorkSpaces;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.8.25.3. VMware WS 5.0, GSX 3.2, ESX 2.5 ou superior;
- 1.3.8.25.4. VMWare ESXi 4.1 – 6.7;
- 1.3.8.25.5. Microsoft Virtual Server 2005;
- 1.3.8.25.6. Microsoft Enterprise Desktop Virtualization (MED-V);
- 1.3.8.25.7. Microsoft Windows Server 2008, 2012 e 2012 R2 e 2016 Hyper-V;
- 1.3.8.25.8. Citrix XenServer 5.6 ou superior;
- 1.3.8.25.9. Virtual Box by Oracle;
- 1.3.8.26. Possuir funcionalidades de otimização de scans em ambientes virtuais, contemplando os virtualizadores VMWare, Citrix e Microsoft, para no mínimo:
- 1.3.8.27. Diferenciação automática entre máquinas físicas e virtuais, possibilitando aplicar as funcionalidades específicas para as máquinas virtuais;
- 1.3.8.28. Proteção com as mesmas funcionalidades aplicáveis em máquinas físicas, para no mínimo:
 - 1.3.8.28.1. Proteção de antivírus e antispymware;
 - 1.3.8.28.2. Proteção de heurística e reputação de arquivos em tempo real;
 - 1.3.8.28.3. Proteção de IPS de rede e “host”;
- 1.3.8.29. Controle de dispositivos e aplicações;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.8.30. Cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;
- 1.3.8.31. Capacidade de verificar “modelos” de máquinas virtuais, excluindo da operação de varredura todos os arquivos categorizados como confiáveis, existentes na máquina virtual utilizada como modelo;
- 1.3.8.32. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;
- 1.3.8.33. Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos;
- 1.3.8.34. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:
 - 1.3.8.34.1. Origem confiável;
 - 1.3.8.34.2. Origem não confiável;
 - 1.3.8.34.3. Tempo de existência do arquivo na internet;
 - 1.3.8.34.4. Comportamento do arquivo;
 - 1.3.8.34.5. Quantidade mínima de usuários que baixaram o arquivo da internet;
- 1.3.8.35. Capacidade de implementar regras distintas por grupo a partir da reputação, quantidade de utilizadores e tempo de existência do arquivo;

1.3.9. Módulo Intrusion Prevention;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.9.1. Políticas de Detecção e Prevenção de Intrusão (IDS\IPS);

1.3.9.2. A solução deve ter a capacidade de implementar políticas de IPS para Windows e Mac OS;

1.3.9.3. A solução deve ter a capacidade de implementar auditoria nas políticas de IPS implementadas para Windows;

1.3.9.4. A solução deve ter a capacidade de implementar exceções nas políticas de IPS implementadas para Windows e Mac OS;

1.3.9.5. A solução deve ter a capacidade de implementar nas políticas de IPS para Windows, no mínimo:

1.3.9.5.1. Permitir habilitar e desabilitar as políticas;

1.3.9.5.2. Proteção de IPS nos Navegadores;

1.3.9.5.3. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;

1.3.9.5.4. Permitir habilitar, desabilitar e somente logar as Proteções de IPS nos Navegadores;

1.3.9.5.5. Bloqueio de ataques baseado na exploração da vulnerabilidade;

1.3.9.5.6. Deverá possuir um conjunto de regras de IPS otimizadas para uso em servidores;

1.3.10. Módulo de Firewall;

1.3.10.1. Módulo de Firewall com as seguintes funcionalidades:

1.3.10.1.1. Suporte aos protocolos TCP, UDP e ICMP;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.10.1.2. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;
- 1.3.10.1.3. Possuir proteção contra exploração de buffer overflow;
- 1.3.10.1.4. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;
- 1.3.10.1.5. Possibilidade de agendar a ativação da regra de Firewall;
- 1.3.10.1.6. Possibilidade de criar regras diferenciadas por aplicações;
- 1.3.10.1.7. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede com base no fingerprint do arquivo;
- 1.3.10.1.8. Proteger o computador por meio da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital sejam executadas no computador;
- 1.3.10.1.9. Funcionalidade de Whitelist e Blacklist com a Impressão digital dos executáveis;
- 1.3.10.1.10. Permitir a criação de zona confiável, possibilitando que determinados IPs, protocolos ou aplicações se comuniquem na rede;
- 1.3.10.1.11. A funcionalidade de firewall deverá ser compatível com, no mínimo, Windows e Mac;
- 1.3.10.1.12. O gerenciamento deve ser integrado à console da solução para gestão das políticas de firewall;
- 1.3.10.1.13. A solução deve ter a capacidade de implementar políticas de Firewall em modo de produção e modo de interação do usuário;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.10.1.14. A solução deve ter a capacidade de implementar políticas de Firewall, possibilitando minimamente:

1.3.10.1.14.1. Permitir que os usuários executem testes de segurança, implementando o modo de interação do usuário;

1.3.10.1.14.2. Permitir que os usuários habilitem e desabilitem o firewall, implementando o modo de interação do usuário, possibilitando no mínimo as seguintes restrições:

1.3.10.1.14.2.1. Administradores do Windows;

1.3.10.1.14.2.2. Todos os usuários;

1.3.10.1.15. A solução deve ter a capacidade de implementar os seguintes comportamentos quando o firewall for desativado pelo usuário:

1.3.10.1.15.1. Permitir todo o tráfego;

1.3.10.1.15.2. Permitir apenas tráfego de saída;

1.3.11. Módulo de proteção para dispositivos móveis;

1.3.11.1. Deverá ser ofertado como um serviço totalmente em nuvem, de forma a garantir suas funcionalidades independentemente da rede que o dispositivo estiver conectado;

1.3.11.2. Deverá possuir console WEB para administração da solução;

1.3.11.3. Possuir dashboard com os principais indicadores da solução, como Distribuição de níveis de risco, dispositivos em não conformidade, total de dispositivos protegidos e incidentes recentes;

1.3.11.4. Apresentar, nos dashboards, uma visão geral dos riscos examinados nos dispositivos móveis, como ameaças de rede, vulnerabilidades e malwares encontrados;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.11.5. Associar o nome do usuário ao nome do dispositivo, o modelo e a versão do sistema operacional, em console gráfica;
- 1.3.11.6. A console deverá apresentar os principais incidentes gerados, contendo todos os detalhes sobre o mesmo e o dispositivo que gerou o incidente;
- 1.3.11.7. A console deverá apresentar, em formato de mapa, onde foram gerados os incidentes de rede;
- 1.3.11.8. A solução deverá apresentar um relatório de ações recomendadas, com um sumário de ações para melhorar a segurança dos dispositivos móveis da empresa;
- 1.3.11.9. É desejável que a solução esteja categorizada como uma solução de MTD (Mobile Threat Defense);
- 1.3.11.10. Deverá ser compatível com os sistemas operacionais IOS e Android;
- 1.3.11.11. Deverá integrar-se com as principais tecnologias de MDM ou EMM do mercado, no mínimo com IBM MaaS360, MobileIron, Microsoft Intune e Airwatch;
- 1.3.11.12. O cliente da solução deverá estar disponível nas lojas oficiais dos fabricantes, sendo Apple Store para IOS e Google Play para Android;
- 1.3.11.13. Permitir configuração no cliente instalado nos dispositivos móveis para que nenhuma informação e alertas seja visível para o usuário final, através de modo não interativo;
- 1.3.11.14. Quando o cliente estiver em modo não interativo, ter opção de customizar uma mensagem para o usuário final, incluindo o uso do logotipo da CONTRATANTE, texto informativo e link de e-mail para suporte;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.11.15. Deverá possuir as seguintes características mínimas de proteção:

- 1.3.11.15.1. Proteção contra Malwares;
- 1.3.11.15.2. Proteção contra apps maliciosos de dia zero;
- 1.3.11.15.3. Identificação de apps suspeitos;
- 1.3.11.15.4. Análise incremental de apps, baseado em assinatura, análise estática e dinâmica, comportamental e permissões utilizadas;
- 1.3.11.15.5. Proteção em tempo real contra malwares conhecidos e desconhecidos;
- 1.3.11.15.6. Proteção contra redes Wi-Fi maliciosas;
- 1.3.11.15.7. Detecção e bloqueio de perfis maliciosos para iOS;
- 1.3.11.15.8. Detecção de descryptografia de rede;
- 1.3.11.15.9. Comunicação com servidores de comando e controle (C&C Servers);
- 1.3.11.15.10. Identificação de ataques como Man-in-the-middle, SSL Downgrading e manipulação de conteúdo;
- 1.3.11.15.11. Monitorar os dispositivos para identificação de vulnerabilidades conhecidas;
- 1.3.11.15.12. Alertar sobre vulnerabilidades existentes nos dispositivos da CONTRATANTE;
- 1.3.11.15.13. Funcionalidade de identificação de upgrades do sistema operacional;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.11.15.14. Funcionalidade de identificação de dispositivo com acesso root;
- 1.3.11.15.15. Funcionalidade de identificação de configurações de segurança, como tela de bloqueio não habilitada;
- 1.3.11.15.16. Deve possibilitar a instalação do cliente da solução através de integração com solução de MDM/EMM ou através da própria console, utilizando e-mail;
- 1.3.11.15.17. A solução deverá verificar a conformidade do dispositivo e bloquear o acesso a recursos corporativos, como Office365 e outros;
- 1.3.11.16. Durante a modificação de uma política de conformidade, a solução deverá simular o impacto que a mudança causará, informando o percentual de dispositivos que ficarão fora de conformidade caso a política seja aplicada, de forma a garantir que a mudança não gere impacto no ambiente;
- 1.3.11.17. Caso a solução detecte que o dispositivo está em uma rede maliciosa, deverá automaticamente fechar um VPN com o Fabricante, garantindo assim que a comunicação dos apps seja criptografada;
- 1.3.11.18. A solução deverá prevenir que perfis maliciosos tentem utilizar uma VPN;
- 1.3.11.19. Deverá ser possível submeter apps suspeitos ao fabricante da solução, para ser analisado o comportamento, se é algum malware e a reputação do desenvolvedor;
- 1.3.11.20. Deverá possuir whitelist de apps;
- 1.3.11.21. Deverá possuir integração com solução de SIEM de mercado, no mínimo para Splunk, IBM Qradar e HP Arcsight;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.11.22. A solução deve apresentar notificações de violações para o usuário final e para os administradores da solução, através de e-mail e Notificações Push;
- 1.3.11.23. Deverá ser possível customizar as notificações para o idioma Português, bem como o formato do e-mail, adicionando logotipo da Contratante;
- 1.3.11.24. Integrar a console de administração com soluções de single sign-on através do protocolo SAML 2.0;
- 1.3.11.25. A solução deve ter capacidade de integração para no mínimo:
 - 1.3.11.25.1. Solução de CASB;
 - 1.3.11.25.2. Solução de Proxy em Nuvem;
 - 1.3.11.25.3. Blackberry API;
 - 1.3.11.25.4. AirWatch API;
 - 1.3.11.25.5. IBM Maas360 API;
 - 1.3.11.25.6. Citrix Xenmobile API;
 - 1.3.11.25.7. Microsoft Intune API;
 - 1.3.11.25.8. OKTA, SSO;
 - 1.3.11.25.9. Azure Active Directory;
 - 1.3.11.25.10. HP ArcSight API;
 - 1.3.11.25.11. SPLUNK API;
 - 1.3.11.25.12. IBM Qradar API;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.11.25.13. CEF Format;
- 1.3.11.25.14. Syslog;
- 1.3.11.25.15. Mobile User Notifications;

1.3.12. Módulo de proteção contra exploração do ambiente Active Directory;

- 1.3.12.1. Capacidade de rodar simulações de ataques descobrindo backdoors e hooks persistentes no Microsoft Active Directory;
- 1.3.12.2. Monitoração Comportamental determinando o risco e por conseguinte o bloqueio da ameaça, protegendo contra os ataques de ransomware e stealthy, tal como scripts maliciosos em Powershell e WMI;
- 1.3.12.3. A solução deve ter a capacidade de ser implementada a partir do cliente de Proteção do Endpoint do próprio fabricante, assim como, de forma stand alone;
- 1.3.12.4. A solução deve ter a capacidade avançada de segurança de endpoints especificamente para ser implementada na defesa do MS Active Directory para lidar contra os ataques de Stealthy e APTs, protegendo o AD contra ataques iniciados a partir de qualquer endpoint com acesso a rede, seja ele dentro ou fora do domínio;
- 1.3.12.5. A solução deve ter a capacidade de detecção, investigação e contenção de intrusões baseada em Inteligência Artificial, desenvolvida especificamente para proteger o MS Active Directory;
- 1.3.12.6. A solução deve ter a capacidade específica de interrompe a atividade de reconhecimento, implementando a contenção de ataques a partir do endpoint, impedindo que os atacantes usem o MS Active Directory para roubar credenciais de domínio e iniciar os ataques de movimentação lateral;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.12.7. A solução deve ter a capacidade de realizar simulações contínuas e automatizadas de ataques para encontrar backdoors e hooks de persistência no MS Active Directory;
- 1.3.12.8. A solução deve ter a capacidade de aprender autonomamente a estrutura do MS Active Directory da organização em sua totalidade e utilizar esses dados para criar uma extensão de estrutura autêntica e ilimitada, possibilitando utilizar este ambiente como isca para os atacantes em uma perspectiva dos ativos conectados ao domínio, utilizando a monitoração da interação dos atacantes com esta estrutura para bloquear ações derivadas, tais como o bloqueio de novos comandos, injeção de códigos em outros aplicativos e até mesmo um simples comando de conectividade (ex.: ping);
- 1.3.12.9. A solução deve ter a capacidade de utilizar metodologias exclusivas de resposta a incidentes para um ambiente corporativo de domínio do MS Active Directory, fornecendo relatórios forenses em tempo real que capturam fases reais de reconhecimento do ambiente atacado, o roubo de credenciais e movimentações laterais que foram executadas pelo atacante;
- 1.3.12.10. A solução deve ter a capacidade de documentar a cadeia de ataque até a vítima zero identificando a origem do ataque, possibilitando avaliar se o ataque é um incidente local, assim como externo;
- 1.3.12.11. A solução deve ter a capacidade de implementar uma mitigação automatizada interrompendo o processo mal-intencionado no endpoint, impedindo, assim, a violação em tempo real, bloqueando sua capacidade de criar outro processo, sobrescrever outra parte da memória, executar comandos de reconhecimento e até mesmo se comunicar com a rede;
- 1.3.12.12. A solução deve ter a capacidade de implementar uma avaliação contínua de ameaças de todo o ambiente do MS Active



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

Directory, examinando erros de configuração de domínio, vulnerabilidades e ameaças persistentes, utilizando-se simulações de ataque para reunir informações detalhadas sobre a segurança do MS Active Directory;

1.3.12.13. A solução deve ter a capacidade de implementar a avaliação de forma automatizada utilizando as simulações de ataque para reunir informações detalhadas sobre a configuração do domínio, contas com privilégios, configurações de segurança, GPO, endpoints, controladores de domínio e Kerberos;

1.3.12.14. A solução deve ter a capacidade de analisar autonomamente cada componente do domínio e a estrutura do MS Active Directory em busca de erros de configuração e backdoors que os atacantes podem ter deixado de forma latente para possível reutilização da metodologia de ataque;

1.3.12.15. A solução deve ter a capacidade de ao verificar uma configuração incorreta ou um backdoor, gerar um alerta e enviá-lo a console central com recomendações sobre correção;

1.3.12.16. A solução deve ter a capacidade de implementar avaliações de forma automática para vulnerabilidades e erros de configurações especificamente para o MS Active Directory, utilizando a técnica de simulação de ataques para no mínimo:

1.3.12.16.1. Avaliação de conta de usuário, implementando a descoberta de contas de administradores potencialmente perigosas;

1.3.12.16.2. Avaliação de vulnerabilidade do Kerberos, implementando a descoberta de controladores de domínio que permitam a modificação de certificado de atributo privilegiado;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.12.16.3. Avaliação de Contas de Serviço, implementando a descoberta de contas de serviço vulneráveis expostos ao cracking do Kerberos;
- 1.3.12.16.4. Avaliação de Local Admin Traversal, implementando a descoberta de rotas de movimento lateral usando a conta de administrador local;
- 1.3.12.16.5. Avaliação de Delegação, implementando a descoberta da delegação de contas de computador;
- 1.3.12.16.6. Avaliação LDAP, validando controladores de domínio que permitem conexões anônimas ou não criptografadas;
- 1.3.12.16.7. Avaliação de hosts que permitem a descoberta de rede;
- 1.3.12.17. A solução deve ter a capacidade de detecções persistentes de ameaças, ataques e más configurações, para no mínimo:
 - 1.3.12.17.1. Hidden SID (Security Identifier);
 - 1.3.12.17.2. Golden Ticket;
 - 1.3.12.17.3. ACL de administrador não privilegiado;
 - 1.3.12.17.4. Silver Ticket;
 - 1.3.12.17.5. Login do DSRM habilitado;
 - 1.3.12.17.6. Backdoor na replicação de domínio;
 - 1.3.12.17.7. Local Admin Traversal;
 - 1.3.12.17.8. Power User Enumeration;
 - 1.3.12.17.9. Group Policy Preferences;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.12.17.10. Conexões LDAP anônimas permitidas;
- 1.3.12.18. A solução deve ter a capacidade de mascarar a topologia do domínio MS Active Directory, dificultando a análise do ambiente, onde toda tentativa de consulta (query) deve ser controlada pelo endpoint;
- 1.3.12.19. A solução deve ter a capacidade de gerar novos objetos mascarados com base no esquema de nomenclatura e topologia atual do Órgão, implementando a capacidade de aprender os computadores, os usuários, as regras de nomenclatura utilizada nos usuários administradores, recriando os novos objetos com base neste aprendizado;
- 1.3.12.20. A solução deve ter a capacidade de configurar conforme a necessidade do Órgão o fator multiplicador de mascaramento de acordo com cada objeto, variando para cima ou para baixo implementado a quantidade desejada de objetos falsos distribuídos pela solução;
- 1.3.12.21. A solução deve ter a capacidade de mascarar minimamente os seguintes objetos dentro do MS Active Directory:
- 1.3.12.21.1. Contas de usuários com acessos;
 - 1.3.12.21.2. Servidores conectados ao domínio;
 - 1.3.12.21.3. Desktop conectados ao domínio;
 - 1.3.12.21.4. Notebooks conectados ao domínio;
 - 1.3.12.21.5. Contas de Serviço expostas a possíveis ataques de "Kerberoasting";
- 1.3.12.22. A solução deve ter a capacidade de quando um ataque for detectado, gerar um alerta a partir do endpoint, em conjunto com uma



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

verificação sob demanda reunindo informações forenses específicas relacionadas ao ataque;

- 1.3.12.23. A solução deve ter a capacidade de automatizar o processo forense e verificar as informações corretas, somente quando um ataque é detectado, garantindo a priorização correta reduzindo a incidência de falsos positivos;
- 1.3.12.24. A solução deve ter a capacidade de utilizar-se da Manipulação de Memória implantada nos endpoints após sua autenticação, sem a necessidade de nenhuma instalação nos Controladores de Domínio e sem o uso de agentes em execução no disco dos endpoints;
- 1.3.12.25. A solução deve ter a capacidade de ser implantada sem a necessidade de monitoramento de rede, sem nenhum tipo de alteração de rede, sem nenhuma alteração no MS Active Directory;
- 1.3.12.26. Deve possuir proteção a integridade do Active Directory (AD), tanto da perspectiva do Endpoint quando do próprio Active Directory;
- 1.3.12.27. Deve possuir proteção contra técnicas de reconhecimento do domínio, sendo capaz de detectar um invasor que utilize técnicas de movimentação lateral e roubo de credenciais válidas;
- 1.3.12.28. Deve proteger contra intrusões realizadas a partir de processos, usuários e terminal;
- 1.3.12.29. Deve ser capaz de identificar vulnerabilidades, erros de configurações e possíveis Backdoors presentes no Active Directory;
- 1.3.12.30. Deve ser capaz de proteger alterações no Active Directory sem a necessidade de instalação de agentes ou de componentes adicionais;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.12.31. Deve ser capaz de detectar e proteger roubos de credenciais no ambiente que utilizem as técnicas Pass-the-Hash e Pass-the-Ticket;
- 1.3.12.32. Deve ter a capacidade de alarmar tentativas de Força-Bruta de máquinas que estejam fora do domínio;
- 1.3.12.33. Deve ser capaz de alarmar conexões não confiáveis de LDAP;
- 1.3.12.34. Deve detectar ataques que ocorram na fase de pós-violação, detectando as fases de reconhecimento, roubo de credenciais e movimentações laterais;
- 1.3.12.35. Deve fornecer proteção contra no mínimo os seguintes ataques:
 - 1.3.12.35.1. Pass-The Ticket;
 - 1.3.12.35.2. Pass-The-Hash;
 - 1.3.12.35.3. Overpass-The-Hash;
 - 1.3.12.35.4. Forged PAC;
 - 1.3.12.35.5. DCSync;
 - 1.3.12.35.6. Skeleton Key;
 - 1.3.12.35.7. Enumeração de Sessão;
 - 1.3.12.35.8. Golden Tickets;
 - 1.3.12.35.9. Silver Tickets;
- 1.3.12.36. Deve detecção escalação de privilégios locais e a nível de domínio;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.12.37. Deve detectar pontos de persistência maliciosos no Sistema;
- 1.3.12.38. Deve ser capaz de listar processos e credenciais carregados na memória em um determinado momento do tempo;
- 1.3.12.39. A solução deve ser capaz de listar, no mínimo:
 - 1.3.12.39.1. Estatísticas avançadas de rede;
 - 1.3.12.39.2. Lista de processos;
 - 1.3.12.39.3. Tickets do Kerberos na memória;
 - 1.3.12.39.4. Tentativas de Pass-the-Hash;
 - 1.3.12.39.5. Histórico de navegação e downloads no endpoint;
- 1.3.12.40. Deve ser capaz de conter um ataque de forma automática ao Active Directory;
- 1.3.12.41. Deve ter a capacidade de a partir das atividades detectadas classificá-las com severidades: Baixa, Média e Alta;
- 1.3.12.42. Deve ser capaz de encontrar vulnerabilidades, Backdoors e má-configurações no Active Directory, fornecer informações relacionadas ao ataque e mitigá-las;

1.3.13. Relatórios Forense

- 1.3.13.1. O relatório forense deve detectar ataques que tenham acontecido no Active Directory, sendo capaz de identificar as atividades executadas pelo atacante como: Técnicas de reconhecimento, tentativas de movimentação lateral e roubo de credenciais;
- 1.3.13.2. Deve possuir informações relacionadas a análise da memória com detalhes sobre cada processo suspeito encontrado;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.13.3. Deve fornecer informações sobre possíveis métodos de persistência encontrados no endpoint;

1.3.13.4. Deve prover evidências da execução de executáveis no endpoint;

1.3.13.5. Deve ser possível exportar o relatório forense da console de gerenciamento;

1.3.13.6. Deve fornecer informações sobre indicadores de comprometimento (IoC's) cobrindo no mínimo os seguintes indicadores:

1.3.13.6.1. Ataques de Pass-The-Hash;

1.3.13.6.2. Tickets do Kerberos injetados;

1.3.13.6.3. Strings suspeitas;

1.3.13.6.4. Extensões Duplas;

1.3.13.6.5. Ofuscação;

1.3.13.6.6. Utilização de recursos falsos (Isclas);

1.3.14. Análise da Memória

1.3.14.1. Deve fornecer no mínimo as seguintes informações sobre processos maliciosos:

1.3.14.1.1. Process ID;

1.3.14.1.2. Token de usuário utilizado;

1.3.15. Características da proteção contra exploração de Memória

1.3.15.1. Deve prevenir ataques de dia Zero e ataques baseados em memória;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.15.2. A detecção Proativa de reconhecimento de novas ameaças deve ter as seguintes funcionalidades:

1.3.15.3. Identificação de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;

1.3.15.4. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinaturas periódicas da técnica de detecção;

1.3.15.5. Capacidade de detectar keyloggers, Trojans, spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

1.3.15.6. Reconhecimento de comportamento malicioso na modificação da configuração de DNS e arquivo Host;

1.3.15.7. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;

1.3.15.8. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Proativa com a base de reputação do fabricante;

1.3.15.9. Possibilidade de agendar o escaneamento da detecção Proativa com periodicidade mínima por minuto e em todos os novos processos;

1.3.16. Quanto as políticas de Memory Exploit Protection;

1.3.16.1. A solução deve ter a capacidade de implementar políticas contra Exploração de Memória, no mínimo nos modos de monitoração, proteção de JAVA e proteção customizada de aplicações;

1.3.16.2. Deve habilitar, desabilitar ou apenas monitorar, para no mínimo as seguintes técnicas de mitigação:

1.3.16.2.1. DllLoad;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.16.2.2. EnhASLR;
 - 1.3.16.2.3. ForceASLR;
 - 1.3.16.2.4. ForceDEP;
 - 1.3.16.2.5. HeapSpray;
 - 1.3.16.2.6. NullProt;
 - 1.3.16.2.7. RopCall;
 - 1.3.16.2.8. RopHeap;
 - 1.3.16.2.9. SEHOP;
 - 1.3.16.2.10. StackNX;
 - 1.3.16.2.11. StackPvt;
 - 1.3.16.2.12. Advanced machine learning;
- 1.3.16.3. Deve ter a capacidade de implementar a funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando, no mínimo, as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos, como também as características de boa pontuação:
- 1.3.16.3.1. Exploração de navegadores com reputação de URL;
 - 1.3.16.3.2. Websites infectados com reputação de URL;
 - 1.3.16.3.3. Office Exploits com reputação de URL;
 - 1.3.16.3.4. Arquivos anexos com reputação de arquivos;
 - 1.3.16.3.5. Download de arquivos com reputação de arquivos;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.16.3.6. Instalação de software com as técnicas de SAPE – Static Attribute Protection Engine;
- 1.3.16.3.7. Instalação de software com as técnicas de Malheur;
- 1.3.16.3.8. Cópia de arquivos com as técnicas de SAPE – Static Attribute Protection Engine;
- 1.3.16.3.9. Cópia de arquivos com as técnicas de Malheur;
- 1.3.16.3.10. Execução do instalador de software com classificação comportamental do instalador (boa e ruim);
- 1.3.16.3.11. Execução do malware de software com classificação comportamental do instalador (boa e ruim);
- 1.3.16.3.12. A funcionalidade de “Machine Learning” deve trabalhar baseado no mínimo nas seguintes premissas:
- 1.3.16.3.13. Atualização da base de reputação das URL’s com a periodicidade de 3 horas ou menos;
- 1.3.16.3.14. Bloqueio de URL’s de má reputação;
- 1.3.16.3.15. Bloqueio das instruções de “Command & Control”;
- 1.3.16.3.16. Atualização da base de reputação de Arquivos com a periodicidade de 3 horas ou menos;
- 1.3.16.3.17. Bloqueio das ameaças polimorfas mesmo em arquivos desconhecidos;
- 1.3.16.3.18. Prevenção de Falso Positivos;
- 1.3.16.3.19. Bloqueio de malwares desconhecidos e suas variantes;
- 1.3.16.3.20. Implementar a classificação comportamental dos arquivos;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

1.3.16.3.21. Aprendizado a partir dos indicadores de compromisso (IoC);

1.3.16.3.22. A funcionalidade de “Machine Learning” deve ter a capacidade de implementar uma análise em tempo real correlacionando entre:

1.3.16.3.22.1. Veredicto das análises entre usuários da plataforma de segurança do mesmo fabricante;

1.3.16.3.22.2. Arquivos de softwares mundialmente espalhados na rede mundial de computadores;

1.3.16.3.22.3. Sites Web mundialmente espalhados pela rede mundial de computadores;

1.3.16.3.22.4. Emulação trabalhando como uma sandbox local contra ataques polimorfos e as mutações dos malwares

1.3.16.3.22.5. A funcionalidade de emulação para malware deve, a partir do software de proteção de endpoint, implementar a emulação em um ambiente virtual (local) possibilitando detectar e impedir as técnicas de evasão de detecção, mesmo que utilizando polimorfismo no seu empacotamento;

1.3.16.3.22.6. A funcionalidade de emulação para malware deve ser suportada para as plataformas Windows (32 e 64 bits), Linux (64 bits) e Mac (64 bits); (EDR local + Javelim)

1.3.17. Funcionalidade de Controle de Dispositivos e Aplicações

1.3.17.1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.2. Controlar o uso de dispositivos com comunicação infravermelho, firewire, PCMCIA, portas seriais e paralelas, através de mecanismos de permissão e bloqueio, identificando pelo "Class ID" e pelo "Device ID" do Dispositivo;
- 1.3.17.3. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;
- 1.3.17.4. Gerenciamento integrado à console da solução;
- 1.3.17.5. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;
- 1.3.17.6. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;
- 1.3.17.7. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para leitura, escrita e execução em MAC OSx, para no mínimo:
 - 1.3.17.7.1. USB;
 - 1.3.17.7.2. Firewire;
 - 1.3.17.7.3. Thunderbolt;
 - 1.3.17.7.4. CD/DVD/BR;
 - 1.3.17.7.5. SD Card;
 - 1.3.17.7.6. eSATA;
- 1.3.17.8. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para MAC OSx, possibilitando regras de "white list" e "black list" utilizando expressões regulares,



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

assim como, possibilidade de implementar teste de regras sem impactar na produção;

1.3.17.9. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para MAC OSx, possibilitando administração por parte dos usuários e administração remota, com a possibilidade de monitoração e relatórios a partir da console de administração;

1.3.17.10. Políticas para Controle de Aplicações;

1.3.17.10.1. A solução deve ter a capacidade de implementar a funcionalidade de Controle de Aplicações em no mínimo 3 (três) modos, sendo eles modo execução, somente monitoração e execução customizada;

1.3.17.10.2. A solução deve ter a capacidade de implementar a funcionalidade de Controle de Aplicações em no modo de execução customizada, possibilitando configura o tipo de aplicativo que os usuários podem manipular, para no mínimo as seguintes opções:

1.3.17.10.2.1. Permitir customizações se os aplicativos forem assinados e tiverem boa reputação;

1.3.17.10.2.2. Permitir customizações se os aplicativos não estiverem assinados, mas tiverem boa reputação;

1.3.17.10.2.3. Permitir customizações se os aplicativos forem assinados, mas tiverem reputação cinza;

1.3.17.10.2.4. Permitir customizações se os aplicativos não estiverem assinados e tiverem reputação cinza;

1.3.17.10.3. A solução deve ter a capacidade de implementar políticas de exceções, baseadas minimamente em:



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.10.3.1. Aplicações com certificados assinados;
- 1.3.17.10.3.2. Nome dos arquivos e aplicações;
- 1.3.17.10.3.3. Nome de domínio web;
- 1.3.17.10.3.4. Hash da aplicação;
- 1.3.17.10.3.5. Caminho (path) da aplicação;
- 1.3.17.10.3.6. Pela extensão do arquivo;
- 1.3.17.10.3.7. Nas políticas de IPS, para no mínimo: Endereçamento IPv4, IPv6, Subnet e Range de endereçamento IP;
- 1.3.17.10.3.8. Capacidades de prevenção contra ataques direcionados ou persistentes
- 1.3.17.11. A solução deverá prover as funcionalidades de gerenciamento centralizado para os módulos de análise dos ambientes de endpoint, rede e e-mail;
- 1.3.17.12. A solução deve ter como característica básica correlacionar as informações detectadas pelo módulo de APT de endpoint, módulo de APT de rede e módulo de APT de e-mail. Não serão aceitas correlações advindas somente das tecnologias de IPS/IDS;
- 1.3.17.13. A solução contra ataques de APT (Advanced Persistent Threats) deve implementar a tecnologia de EDR (Endpoint Detection and Response), fornecendo uma visão única de todos os Indicadores de Comprometimento (IoC - Indicators of Compromise);
- 1.3.17.14. O módulo de análise de e-mail deve ter a capacidade de identificar uma ameaça, mesmo que esta seja originada a partir de uma URL curta, fazendo uma inspeção no conteúdo original, mesmo



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

antes do usuário ter acesso ao conteúdo indicado pela URL, possibilitando categorizar a origem da informação;

1.3.17.15. A tecnologia de Sandbox deve ser executada em ambiente tanto virtual como em bare-metal, utilizando como fonte de informação a rede mundial de inteligência do fabricante, que deve contar com a coleta de informações em no mínimo 80 milhões de máquinas e 3 petabytes de dados em seus registros;

1.3.17.16. O módulo de proteção no endpoint contra ataques de APT não pode ser um novo agente de segurança dentro da máquina cliente, as funções de APT devem ser realizadas pelo mesmo agente de proteção contra vírus e malwares;

1.3.17.17. O agente de proteção no endpoint contra ataques de APT deve executar esta proteção a partir do mesmo módulo que faz a proteção contra vírus e malware, sem a necessidade de novos processos, DLL's, utilizando os já existentes para proteção das ameaças mais comuns (vírus e malwares), mantendo desta forma o mesmo processamento, sem consumo adicional de recursos;

1.3.17.18. A partir da console de gerenciamento da solução contra ataques de APT, deve ser possível identificar o equipamento que está sofrendo ataques e comandar o agente de endpoint, para que aquele determinado equipamento deva ir para uma área de quarentena;

1.3.17.19. A partir da solução contra ataques de APT, deve ser possível trabalhar em no mínimo 3 camadas distintas, conforme abaixo:

1.3.17.19.1. Detectar, onde é possível identificar as incursões;

1.3.17.19.2. Responder, onde é possível fazer a contenção e correção dos problemas;

1.3.17.19.3. Recuperar, onde é possível reestabelecer a operação;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.20. A solução contra ataques deve ser capaz de identificar e agir contra os métodos de evasão dos dados, ou seja, identificar os AET (Advanced Evasive Threat);
- 1.3.17.21. A solução deve ter a capacidade de indicar o índice de comprometimento (IoC Indicators-of-Compromise) de um ataque, indicando em modo gráfico as relações e conexões existentes;
- 1.3.17.22. A solução contra os ataques de ATP deve identificar o índice de comprometimento de um ataque, elencando no mínimo as seguintes informações:
- 1.3.17.22.1. Atividades suspeitas na organização;
 - 1.3.17.22.2. Arquivos utilizados em determinado ataque;
 - 1.3.17.22.3. Mensagens trocadas com os Arquivos suspeitos, identificando sua origem;
 - 1.3.17.22.4. Endereçamentos IPs e domínios dos arquivos suspeitos;
- 1.3.17.23. A partir da console de gerência deve ser possível identificar os IoCs nos agentes de Endpoint, possibilitando a identificação a partir de no mínimo:
- 1.3.17.23.1. Hash do arquivo;
 - 1.3.17.23.2. Nome do arquivo;
 - 1.3.17.23.3. Chave de Registro;
 - 1.3.17.23.4. IP de origem;
 - 1.3.17.23.5. URL;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.24. A partir da console da solução contra os ataques de APT, deve ser possível executar diversas ações sobre os arquivos suspeitos, para no mínimo:
- 1.3.17.24.1. Categorizar e incluir em uma “Blacklist”;
 - 1.3.17.24.2. Categorizar e incluir em uma “Whitelist”;
 - 1.3.17.24.3. Submeter para análise em uma SandBox externa ao ambiente de produção;
 - 1.3.17.24.4. Submeter o arquivo para apreciação de uma organização externa ao fabricante da solução, tal como VirusTotal;
 - 1.3.17.24.5. Copiar o arquivo para uma área de armazenamento possibilitando verificação futura;
 - 1.3.17.24.6. Deleção do Arquivo;
 - 1.3.17.24.7. A solução contra ataques de APT (Advanced Persistent Threats) deve fornecer uma visão gráfica completa de como todos os IoC's estão ligados uns aos outros possibilitando determinar no mínimo:
 - 1.3.17.24.8. Os arquivos usados em um determinado ataque;
 - 1.3.17.24.9. Endereços de e-mail em que os arquivos pertencentes ao ataque foram originados;
 - 1.3.17.24.10. Endereços IP onde os arquivos foram baixados;
- 1.3.17.25. A solução deve ter a capacidade de implementar funcionalidade de Proteção contra Ataques Avançados, para no mínimo os sistemas operacionais, Windows 7, Windows 8, Windows 10, MAC OS e Linux;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.26. A solução deve ter a capacidade de implementar uma investigação forense, sem a necessidade de utilizar usuários com direitos de Super Administradores;
- 1.3.17.27. A solução deve ter a capacidade de implementar Telemetria, Inteligência Artificial, Machine Learning para identificar ataques conhecidos como "hard-to-detect attacks";
- 1.3.17.28. A solução deve ter a capacidade de implementar a partir de consultas a rede de inteligência do fabricante, correlacionando com as tecnologias de Machine Learning, entre outras funcionalidades, a possibilidade de enviar notificações personalizadas e priorizadas com recomendações claras de resposta e remediação;
- 1.3.17.29. A solução deve ter a capacidade de implementar a partir da Inteligência Artificial baseada em nuvem, análise evolutiva sem a necessidade de atualizações intrusivas no ambiente, assim como, nos softwares que suportam a solução;
- 1.3.17.30. A solução deve ter a capacidade de analisar aplicativos identificando ataques direcionados utilizando técnicas de Breach Analytics, PowerShell, Lateral Movement e Command and Control Beacons;
- 1.3.17.31. A solução deve ter a capacidade de utilizar seus próprios resultados em forma de loop melhorando seu grau de assertividade, utilizando-se para isso de Técnicas Analíticas Contra Ataques (Targeted Attack Analytics), Inteligência Artificial e Machine Learning;
- 1.3.17.32. A solução deve ter a capacidade a partir de sua telemetria de analisar os dados dos endpoints comprometidos, tanto a nível de processos, quanto de arquivos, da mesma forma que possibilita a avaliação das ferramentas utilizadas no momento do comprometimento, bem como as atividades de rede;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.33. A solução deve ter a capacidade de a partir de sua telemetria municiar a funcionalidade de Machine Learning com dados, possibilitando auxiliá-la na identificação de como uma incursão direcionada se comporta, possibilitando a identificação de um comportamento suspeito semelhante, capacitando a solução à identificar um incidentes em tempo real;
- 1.3.17.34. A solução deve ter a capacidade de detectar violações baseadas em aplicações conhecidas e comportamentos de rede nos endpoints comprometidos, possibilitando alertar e identificar endpoints com comportamentos similares;
- 1.3.17.35. A solução deve ter a capacidade de implementar funcionalidade de Machine Learning fazendo uso de algoritmos de Inteligência Avançada para detectar atividades suspeitas e em seguida reportar em tempo-real, em forma de um incidente, executar uma análise detalhada do atacante, informar as técnicas utilizadas, quais usuários foram afetados, endpoints impactados e sugerir as orientações para mitigação, quando todas as informações são enviadas a console de gerenciamento;
- 1.3.17.36. A solução deve relatar automaticamente o status operacional e as configurações para a console, com base em uma agenda pre-estabelecida, garantindo a capacidade de operação dentro dos padrões estabelecidos;
- 1.3.17.37. A solução deve ter a capacidade de enviar alertas configuráveis com base em critérios definidos e em intervalos pré-definidos pelo administrador;
- 1.3.17.38. A solução deve ter a capacidade de capturar, registrar e analisar automaticamente dados pré-definidos de parâmetros e eventos do endpoint, a fim de avaliar as operações do sistema, suportar a atividade de gerenciamento de riscos, possibilitar atividades de busca e atividades forenses, reportando minimamente:



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.38.1. Alterações nas Chaves de Registros (e seus processos associados; incluindo chaves de execução automática);
- 1.3.17.38.2. Listas de Controle de Acesso (ACLs);
- 1.3.17.38.3. Chaves de licença, propriedade e direitos administrativos;
- 1.3.17.38.4. Autenticação e atividades de usuários privilegiados;
- 1.3.17.38.5. Transferências de arquivos;
- 1.3.17.38.6. Conexões abertas e fechadas;
- 1.3.17.38.7. Destino (Uniform Resource Locator);
- 1.3.17.38.8. Protocolos da Internet;
- 1.3.17.38.9. Tipo de tráfego;
- 1.3.17.38.10. Método de criptografia (por exemplo, protocolo de transferência de arquivos, protocolo de transferência segura de arquivos, bloco de mensagens do servidor, segurança na camada de transporte);
- 1.3.17.38.11. Partidas e paradas automáticas e manuais;
- 1.3.17.38.12. Relacionamentos de processos pais e filhos;
- 1.3.17.38.13. Bibliotecas de vínculo dinâmico carregadas e descarregadas;
- 1.3.17.38.14. Alterações de Software:
- 1.3.17.38.15. Sistema operacional;
- 1.3.17.38.16. Driver e Programas;
- 1.3.17.38.17. Informações de instalação, desinstalação, patch;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.38.18. Conexões com fio e sem fio a dispositivos periféricos;
- 1.3.17.38.19. Arquivos criados, Abertos, Fechados, Salvos, Modificados, Movidos e Excluídos;
- 1.3.17.38.20. Atividades na memória associadas ao ato potencialmente mal-intencionado, incluindo mutexes;
- 1.3.17.38.21. Detecção, Alteração, Modificação de dispositivos periféricos e Remoção de Hardware;
- 1.3.17.39. A solução deve ter a capacidade de relatar automaticamente a detecção de eventos potencialmente mal-intencionados e fornecer informações em formatos padrão não proprietários sendo no mínimo o padrão STIX - Structured Threat Information eXpression);
- 1.3.17.40. A solução deve ter a capacidade de aplicar controles de usuário e máquina para monitoração e impedir que pessoas manipulem dados rotulados (TAG) como "informações confidenciais", exportando para fontes externas, com critérios:
 - 1.3.17.40.1. Baseado em tempo (da informação ou usuário);
 - 1.3.17.40.2. Armazenamento removível, USB, CD, DVD, etc.;
 - 1.3.17.40.3. Anexo para destinatário de e-mail externo (WebMail, SMTP, Exchange);
 - 1.3.17.40.4. Utilizando uma rede não corporativa;
 - 1.3.17.40.5. Para Web (HTTP e HTTPS), independente da tecnologia usada, sem a necessidade de plug-in do navegador;
 - 1.3.17.40.6. Para impressora (rede e local);



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.40.7. Serviços de armazenamento baseados na Internet (Box, Google Drive, etc), independentemente do tipo de tecnologia, sem a necessidade de plug-in;
- 1.3.17.40.8. Impedir a impressão de tela (Ctrl-prtsc e Snip-it software);
- 1.3.17.41. A solução deve ter a capacidade de interromper a execução de exclusões de arquivos de sistema e dados, exceto usuários autenticados autorizados;
- 1.3.17.42. A solução deve ter a capacidade de visibilidade do sistema de arquivos para atividades, incluindo: leitura, gravação de arquivos, exclusão, renomeação, cópia e transferência;
- 1.3.17.43. A solução deve ter a capacidade de criar filtros definidos que excluem o log de funções normais do sistema;
- 1.3.17.44. A solução deve ter a capacidade de evitar atualizações de softwares confiáveis com a inclusão de porções mal-intencionadas;
- 1.3.17.45. A solução deve ter a capacidade de proteção contra utilização de software mal-intencionado conhecidos, tais como C-Cleaner e Python lib;
- 1.3.17.46. A solução deve ter a capacidade de registrar todas as atividades de eventos de atualização de software e seus status;
- 1.3.17.47. A solução deve ter a capacidade de evitar que componentes de hardware internos ou externos comprometidos, sejam eles conhecidos ou desconhecidos executem qualquer rotina;
- 1.3.17.48. A solução deve ter a capacidade de enviar uma tradução da assinatura da política comportamental (BPE - Behavioral Policy Enforcement) para a descrição com informações do MITRE (Massachusetts Institute of Technology Research & Engineering) e quais eventos poderão se tornar um incidente;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.17.49. A solução deve ter a capacidade de a partir dos incidentes, incluírem os eventos subsequentes com dados MITRE TTP (advanced attack techniques and others);

1.3.18. Características de execução de artefatos em Sandbox

- 1.3.18.1. A solução deve ter a capacidade de detectar automaticamente o comportamento do código potencialmente malicioso em execução no contêiner de isolamento;
- 1.3.18.2. A solução deve capturar automaticamente os detalhes necessários, portas e protocolos em uso, executáveis e serviços, plug-ins de navegador em uso, detalhes de eventos, assim como a própria atividade maliciosa, que possa estar ocorrendo no contêiner de isolamento, e assim, suportar análise pós-evento, retrospectiva, análise de ameaças e consciência situacional;
- 1.3.18.3. A solução deve possibilitar a configuração para controlar a capacidade de aplicativos em execução dentro do contêiner de isolamento, que possam acessar (ou não) apenas recursos dos sistemas especificados (por exemplo, dispositivos de armazenamento, recursos de rede, dispositivos de interface humana etc.);
- 1.3.18.4. A solução deve ter a capacidade de fornecer uma verificação contínua da integridade do contêiner de isolamento garantindo que não haja acesso mal-intencionado, não autorizado e qualquer tipo de modificação persistente;

1.3.19. Características quanto ao gerenciamento da Solução no módulo On-Premises

- 1.3.19.1. Implementar gerenciamento centralizado com no mínimo as seguintes funções: criação de regras de tratamento de malware, administração de usuários, configurações de host e network;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.19.2. Implementar a funcionalidade de event server, com mecanismo de rotacionamento automático dos arquivos de evento;
- 1.3.19.3. Implementar mecanismo de triangulação e correlação dos vetores de ataque;
- 1.3.19.4. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;
- 1.3.19.5. Implementar interface CLI segura através do protocolo SSH ou interface serial RS-232 ou similar;
- 1.3.19.6. Implementar base de usuários local e consulta a base de usuários externa através do protocolo LDAP;
- 1.3.19.7. Implementar sincronização de hora através de protocolo NTP;
- 1.3.19.8. Implementar no mínimo 02 (dois) níveis de administração distintos (administrador e usuário);
- 1.3.19.9. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao hardware, log do mecanismo de health-check e log da base de dados;
- 1.3.19.10. Implementar através da interface gráfica mecanismo de atualização da base de dados e de firmware da solução;
- 1.3.19.11. Implementar através da interface gráfica mecanismo de dashboard onde seja possível a visualização de no mínimo as seguintes informações: Sumário de detecção e proteção, gráfico de top infecções, e gráfico da quantidade de e-mails monitorados;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.19.12. Implementar através da interface de administração, configuração de mecanismo de alerta onde seja possível configurar o modo de operação;
- 1.3.19.13. Implementar a atualização (updates) dos appliances via mecanismo de push dos seguintes módulos: segurança de conteúdo e atualização de patch;
- 1.3.19.14. Implementar através da interface gráfica mecanismo para configuração de notificações dos alertas;
- 1.3.19.15. Implementar através da interface gráfica mecanismo de dashboard onde seja possível a visualização das seguintes informações ou similares: Sumário de detecção e proteção, gráfico de top infecções, e gráfico do throughput de tráfego monitorado;

1.3.20. Características da funcionalidade de análise de ataques avançados em Rede On-Premises

- 1.3.20.1. A solução deverá prover as funcionalidades de inspeção *inbound de Malware* com filtro de ameaças avançadas e análise de execução em tempo real, inspeção *outbound de call-backs*;
- 1.3.20.2. Deve ter a capacidade para detecção de “Web Exploits” e “Command & Control”;
- 1.3.20.3. A solução deverá suportar no mínimo 14.000 usuários simultâneos;
- 1.3.20.4. Suportar os protocolos HTTP (Inbound), e protocolos TCP e UDP sem exceções (outbound);
- 1.3.20.5. Implementar e identificar existência de Malware em comunicações de entrada e saída;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.20.6. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN;
- 1.3.20.7. Implementar detecção de Malwares que utilizem mecanismo de exploit em arquivos PDF;
- 1.3.20.8. Implementar detecção de Malwares que utilizem mecanismo do tipo zero-day ou semelhante nas seguintes aplicações: Microsoft Internet Explorer, Mozilla FireFox, Adobe Acrobat Reader, Adobe Acrobat, Microsoft Silverlight, SUN Java, RealPlayer, e Apple Quicktime, possibilitando integração com os módulos de Segurança de Endpoint (servidor e cliente), assim como, com o módulo de Segurança Avançada de Endpoint;
- 1.3.20.9. Implementar Rede de Inteligência proprietária do fabricante existente em no mínimo 05 (cinco) localidades de forma a cobrir ataques originados de qualquer localidade global, com mecanismo opcional de retroalimentação de Malwares não identificados;
- 1.3.20.10. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
- 1.3.20.11. Deve ser capaz de utilizar o agente de Endpoint do próprio fabricante como agente de APT, sem a necessidade de implementação de agente exclusivo;
- 1.3.20.12. Deve ser capaz de utilizar, receber e consumir as informações advindas das aplicações Check Point, Palo Alto e SourceFire, para refinar o comportamento local da rede, de forma a personalizar o resultado das inspeções, correlacionando TODAS as informações recebidas internamente com as recebidas através rede mundial de informações do próprio fabricante;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.20.13. Deve ter integrações nativas com as soluções de DLP, criptografia, IPS comportamental, proteção de endpoint e gerenciamento de endpoint;
- 1.3.20.14. Implementar integração com ferramentas de SIEM;
- 1.3.20.15. Implementar mecanismo de integração com servidores Syslog;
- 1.3.20.16. Implementar atualização a base de dados da Rede de Inteligência de forma automática;
- 1.3.20.17. Toda análise deve ser realizada de forma automatizada sem a necessidade de criação de regras específicas ou interação de um operador;
- 1.3.20.18. Todas as máquinas virtuais utilizadas na solução devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema;
- 1.3.20.19. Toda a verificação e a análise de Malwares e códigos maliciosos deve ocorrer em tempo real, não sendo aceitas verificações em cache engine ou batch mode;
- 1.3.20.20. O módulo de rede deve ter a capacidade de analisar a reputação categorizando os arquivos ou aplicações, minimamente em:
 - 1.3.20.20.1. Conhecida ou não no ambiente computacional;
 - 1.3.20.20.2. Indicando a quanto tempo existe na rede mundial de computadores;
 - 1.3.20.20.3. Onde foi detectada sua primeira aparição e sob quais circunstâncias;
 - 1.3.20.20.4. Identificar suas mutações e alvos de ataques;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 1.3.20.21. O módulo de rede deve ter a capacidade de implementar tecnologia de IPS para identificar máquinas comprometidas no possível ataque;
- 1.3.20.22. O módulo de rede deve ter a capacidade de implementar funcionalidades de Antivírus e blacklist para endereços IP's, URL e Domínios;
- 1.3.20.23. O módulo de rede deve ter capacidade de executar o conteúdo suspeito em um ambiente apartado baseado em nuvem, evitando contato com o ambiente de produção, sendo implementado em dois modelos, tanto em ambiente virtual, quanto em ambiente bare-metal, evitando desta forma, o sucesso de ataques que exploram vulnerabilidade em ambientes virtuais;
- 1.3.20.24. O módulo de rede deve ter a capacidade de emular o comportamento humano na utilização de sistemas operacionais e aplicações, onde suas vulnerabilidades são comumente exploradas, correlacionando tais resultados com uma análise comportamental entregue pela rede de inteligência mundial do fabricante;

2. Item 2 - Subscrição Symantec Data Center Security – SKU: DCS-SRVA-SUB

2.1. Características gerais

- 2.1.1. A Subscrição Symantec Data Center Security, deve implementar de forma combinada pelo menos, as seguintes funcionalidades:
- 2.1.1.1. Antivírus com uma prevenção avançada contra ameaças;
- 2.1.1.2. Funcionalidade IPS/IDS de host;
- 2.1.1.3. Firewall de host;
- 2.1.1.4. Análise de reputação de arquivos;
- 2.1.1.5. Proteção contra ameaças de dia zero;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

2.1.1.6. Anti-Malware para máquinas virtuais via Vmware NSX.

2.1.2. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários da console de gerenciamento em ambientes físicos e virtuais:

2.1.2.1. Windows 7;

2.1.2.2. Windows Server 2003 Standard/ Enterprise 32-bit;

2.1.2.3. Windows Server 2003 Standard/ Enterprise 64-bit;

2.1.2.4. Windows Server 2008 e 2008 R2;

2.1.2.5. Windows Server 2012 e 2012 R2;

2.1.2.6. Windows Server 2016; 2019 e posteriores;

2.1.3. A solução deve suportar, no mínimo, os seguintes sistemas de virtualização para a instalação do sistema operacional do servidor de gerenciamento em ambientes virtuais:

2.1.3.1. VMware vSphere e ESXi 6.0;

2.1.3.2. Microsoft Hyper-V Windows Server 2012 R2;

2.1.3.3. Amazon Web Services (AWS);

2.1.3.4. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários do agente:

2.1.3.5. Windows 2000 Professional/Server/Advanced Server;

2.1.3.6. Windows XP Professional;

2.1.3.7. Windows 7;

2.1.3.8. Windows Server 2003 Standard/ Enterprise 32-bit;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 2.1.3.9. Windows Server 2003 Standard/ Enterprise 64-bit;
- 2.1.3.10. Windows 2008 e 2008 R2;
- 2.1.3.11. Windows 2012 e 2012 R2
- 2.1.3.12. Windows 2016 e Windows 2019;
- 2.1.3.13. Red Hat Enterprise Linux 4, 5, 6 e 7;
- 2.1.3.14. Red Hat Enterprise Linux 7 Atomic;
- 2.1.3.15. SUSE Enterprise Linux 9, 10, 11 e 12;
- 2.1.3.16. CentOS 6 e 7;
- 2.1.3.17. Oracle LNX 5, 6 e 7;
- 2.1.3.18. Amazon Linux;
- 2.1.3.19. Ubuntu 12.04, 14.04 e 16.04
- 2.1.4. A solução deve ser suportada, no mínimo, nas seguintes versões de VMware:
 - 2.1.4.1. VMware ESX 4.1;
 - 2.1.4.2. Vmware ESXi 5, 5.1, 5.5, 6 e 7;
- 2.1.5. O software deve suportar os componentes IDS e IPS, para no mínimo os seguintes sistemas operacionais:
 - 2.1.5.1. Red Hat Enterprise Linux 4, 5, 6 e 7;
 - 2.1.5.2. Red Hat Enterprise Linux 7 Atomic;
 - 2.1.5.3. CentOS 6 e 7;
 - 2.1.5.4. Oracle Linux 6 e 7;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 2.1.5.5. Suse Linux Enterprise Server 10, 11 e 12;
- 2.1.5.6. Ubuntu 14.04 e 16.04 LTS;
- 2.1.5.7. Windows 2000 SP4 Professional, Server e Advanced Server;
- 2.1.5.8. Windows XP Professional SP2, SP3;
- 2.1.5.9. Windows 2003 Standard e Enterprise (32 e 64 bits);
- 2.1.5.10. Windows 2008 e 2008 R2 Standard e Enterprise (32 e 64 bits);
- 2.1.5.11. Windows 2012 e 2012 R2;
- 2.1.5.12. Windows 2016 e Windows 2019;
- 2.1.6. O software deve suportar o componente IDS, para no mínimo os seguintes sistemas operacionais:
 - 2.1.6.1. Vmware Server ESXi 6.5 Host;
 - 2.1.6.2. Vmware Server ESXi 6.0 Host;
 - 2.1.6.3. VMWare Server ESXi 5.5 Host;
 - 2.1.6.4. VMWare Server ESXi 5.1 Host;
 - 2.1.6.5. VMWare Server ESXi 5.0 Host;
 - 2.1.6.6. VMWare Server ESX 4.1 Host;
- 2.1.7. O software deve suportar o componente IDS e IPS, em containers Docker, para no mínimo os seguintes sistemas operacionais:
 - 2.1.7.1. Ubuntu 14.04 e 16.04 LTS;
 - 2.1.7.2. Red Hat Enterprise Linux 8
 - 2.1.7.3. Red Hat Enterprise Linux 7;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

2.1.7.4. Red Hat Enterprise Linux 7 Atomic;

2.1.7.5. CentOS 7.

2.1.8. A solução deve possibilitar a expansão futura para atender ambientes em Nuvens Públicas, através de integração nativa com solução dedicada para este fim, sendo compatível no mínimo com AWS, MS Azure e Google Cloud Platform.

2.2. Características específicas

2.2.1. Deve oferecer proteção proativa contra ataques tipo Dia-Zero diretamente no equipamento, para no mínimo:

2.2.2. Impedir a exploração maliciosa de sistemas e aplicações;

2.2.3. Prevenir a entrada e distribuição de códigos maliciosos;

2.2.4. A solução deve conter políticas de “hardening” padrões e nativas, possibilitando a proteção de aplicativos de alto risco e base de dados, contra a execução não permitida;

2.2.5. A solução deve conter políticas de segurança nativas para aplicativos Microsoft;

2.2.6. A solução deve impedir a execução de aplicações não autorizadas;

2.2.7. A solução deve permitir ao Administrador bloquear tráfego por porta, por protocolo, por IP ou por faixa de endereços IP;

2.2.8. A solução deve proteger arquivos e registros do sistema baseado em políticas;

2.2.9. A solução deve monitorar arquivos e registros do sistema baseado em políticas;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 2.2.10. A solução deve permitir a configuração de filtros de eventos no agente, onde somente os eventos filtrados serão encaminhados para o servidor de gerenciamento;
- 2.2.11. A solução deve possuir políticas predefinidas de monitoramento, de no mínimo os seguintes recursos:
- 2.2.11.1. Falha de acesso;
 - 2.2.11.2. Logon com sucesso;
 - 2.2.11.3. Detecção de logoff remoto;
 - 2.2.11.4. Alteração de configuração pelo Usuário;
 - 2.2.11.5. Alteração no grupo de gerenciamento.
- 2.2.12. A solução deve possuir recurso de prevenção contra acesso indevido de usuários e de aplicações a outros recursos do sistema, como arquivos, processos, bibliotecas e registros;
- 2.2.13. A solução deve implementar a capacidade de prevenção contra ataques de exploração, com regras pré-definidas baseadas no comportamento padrão das aplicações do servidor;
- 2.2.14. A solução deve implementar a capacidade de prevenção de intrusão baseado no comportamento das aplicações;
- 2.2.15. A solução deve possuir recurso nativo de firewall, restringindo atividades de rede por IP e Porta nos sentidos de entrada e saída;
- 2.2.16. A solução deve possuir a capacidade de prevenção contra alteração de privilégios do servidor;
- 2.2.17. A solução deve possuir a capacidade de prevenir contra alterações em arquivos e registros do servidor;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 2.2.18. A solução deve possuir a capacidade de proteção contra execução de instalações e operações não autorizadas no servidor;
- 2.2.19. A solução deve monitorar de forma granular arquivos e diretórios dos equipamentos protegidos;
- 2.2.20. A solução deve possuir a capacidade de prevenir a injeção de códigos em processos em memória para servidores Windows (memory injection protection);
- 2.2.21. A solução deve implementar o conceito de “sandbox” para as aplicações conhecidos do administrador, independentemente se são aplicações de mercado ou proprietárias;
- 2.2.22. A solução deve ter a capacidade de no mínimo:
- 2.2.22.1. Bloquear instalações de aplicações indevidas;
 - 2.2.22.2. Proteger o “core” do sistema operacional;
 - 2.2.22.3. Proteger as áreas “RAW” dos discos locais;
- 2.2.23. A solução deve possuir a capacidade de implementar listas de aplicações autorizadas a serem executadas, através da utilização de pelo menos, os seguintes parâmetros:
- 2.2.23.1. Hash do arquivo executável para o processo específico (MD5 e SHA256);
 - 2.2.23.2. Nome como é publicado, conforme é descrito no certificado emitido pelo fabricante da aplicação;
 - 2.2.23.3. Assinatura digital das aplicações e aplicativos, incluindo componentes de sistema operacional, assinaturas Microsoft, assinaturas confiáveis, serviços e processos interativos;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 2.2.24. A solução deve ter a capacidade de implementar auditoria no Microsoft Active Directory, possibilitando elaborar relatórios com a periodicidade diária, semanal e mensal, para no mínimo:
- 2.2.24.1. Eventos de reset de senha de usuários;
 - 2.2.24.2. Eventos de alteração de Permissionamento;
 - 2.2.24.3. Eventos de manipulação de grupos de alto privilégio.
- 2.2.25. A solução deve realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;
- 2.2.26. A capacidade de verificar a reputação de arquivos, deve correlacionar no mínimo as seguintes características:
- 2.2.26.1. Origem confiável;
 - 2.2.26.2. Origem não confiável;
 - 2.2.26.3. Tempo de existência do arquivo na internet;
 - 2.2.26.4. Comportamento do arquivo;
 - 2.2.26.5. Quantidade mínima de usuários que baixaram o arquivo da internet.
 - 2.2.26.6. Deve ter a capacidade de integração nativa com a tecnologia VMWare NSX, movendo de forma automática um determinado equipamento infectado para uma área de quarentena;
 - 2.2.26.7. Deve ter a capacidade de liberar alguns serviços mesmo em área de quarentena, ao mover o equipamento identificado como infectado dentro do VMWare NSX;
- 2.2.27. A solução deve efetuar "hardening" de sistemas operacionais, aplicações e bancos de dados;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

2.2.28. A solução deve ter a capacidade de implementar, em uma infraestrutura virtual, serviço de antivírus, funcionalidade de reputação de arquivos, funcionalidades de IDS/IPS para no mínimo:

2.2.28.1. VMware ESXi 6.0 ou superior;

2.2.28.2. VMware vCenter 6.0 ou superior;

2.2.28.3. VMware NSX 6.1.3 e superior, nas versões Advanced e Enterprise;

2.2.28.4. Windows Server 2019, 64 bits

2.2.28.5. Windows Server 2016, 64 bits;

2.2.28.6. Windows 10, 64 bits;

2.2.28.7. Windows 8/8.1, 32/64 bits;

2.2.28.8. Windows 7, 32/64 bits;

2.2.28.9. Windows 2012 e 2012 R2;

2.2.28.10. Windows Server 2008 e 2008 R2, 32 e 64 bits;

2.2.29. A solução deve ter a capacidade de implementar, em uma infraestrutura do VMware vSphere, funcionalidade de no mínimo:

2.2.29.1. Bloqueio a acesso não autorizado a Chaves SSL;

2.2.29.2. Bloqueio a acesso não autorizado a arquivos de configurações;

2.2.29.3. Bloqueio a acesso não autorizado a chaves de registro;

2.2.29.4. Bloqueio a acesso não autorizado a arquivos de Logs;

2.2.29.5. Controle sobre privilégios de usuários e processos;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 2.2.29.6. Monitoração da Integridade dos arquivos de vCenter;
- 2.2.29.7. Monitoração da Integridade dos arquivos dos Servidores ESXi 5.1 e superiores;
- 2.2.29.8. Monitoração da Integridade dos arquivos de configurações das VM Guest;
- 2.2.29.9. Monitoração direta dos LOGs nos servidores ESX, ESXi e vCenter;
- 2.2.30. A solução deve ter a capacidade de implementar as funcionalidades de controle de dispositivos e aplicações;
- 2.2.31. A solução deve ter a capacidade de implementar a funcionalidade de "File and Configuration Lock Down";
- 2.2.32. A solução deve implementar em um único agente as funcionalidades de HIPS, HIDS, Host Firewall, Application e Device Control;
- 2.2.33. A solução deve ser capaz de identificar as aplicações instaladas nos servidores, após a instalação do agente, em MS Windows e Linux;
- 2.2.34. A solução deve implementar funcionalidades de Anti-malware, através do uso de agentes, em servidores Linux físicos ou virtualizados, no mínimo para:
 - 2.2.34.1. Red Hat Enterprise Linux;
 - 2.2.34.2. Ubuntu 14 e 16;

3. Item 3 - Subscrição Symantec It Management Suíte (Symantec Altiris) – SKU: ALT-SUB

3.1. Características Gerais



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

3.1.1. A Solução de gerenciamento de conformidade de endpoints deve permitir o acompanhamento de todo o ciclo de vida do ativo, incluindo licenciamento, serviços de instalação, configuração e suporte técnico, conforme especificações a seguir:

- 3.1.1.1. Criação de políticas e tarefas de conformidade;
- 3.1.1.2. Descoberta e inventário completo de estações de trabalho e servidores;
- 3.1.1.3. Gerenciamento de softwares e aplicações;
- 3.1.1.4. Monitoramento de utilização de softwares e aplicações;
- 3.1.1.5. Gerenciamento de atualizações de segurança;
- 3.1.1.6. Medição e bloqueio de software;
- 3.1.1.7. Gerenciamento de imagens de sistemas operacionais.

3.2. Características específicas

3.2.1. Criação de tarefas e políticas de conformidade.

- 3.2.1.1. Deve permitir a criação de tarefas ou scripts em máquinas com os agentes instalados, permitindo interação com qualquer característica da estação ou servidor de forma remota;
- 3.2.1.2. A tarefa deve representar uma execução pontual ou programada, permitindo controle granular sobre a escolha do período de sua execução;
- 3.2.1.3. Os agendamentos de execução de tarefas devem poder ser programados minimamente, por:
 - 3.2.1.3.1. Horário agendado;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 3.2.1.3.2. Janela de execução, permitindo repetição diariamente, semanalmente, anualmente, ou até mesmo através de escolha de quais dias exatos da semana deve ser executada;
- 3.2.1.3.3. Durante o login do usuário;
- 3.2.1.3.4. Durante a inicialização do equipamento.
- 3.2.1.4. Deve ser possível escolher qual usuário será utilizado para execução da tarefa nas máquinas alvo;
- 3.2.1.5. Deve ser possível salvar a saída da execução de comandos para análise do administrador do sistema;
- 3.2.1.6. A Solução deve possibilitar a implementação de políticas de conformidade de softwares ou configurações, atendendo minimamente, os critérios abaixo:
 - 3.2.1.6.1. Instalar um software em um endpoint, sempre que este não for encontrado;
 - 3.2.1.6.2. Impor configurações em um endpoint, corrigindo sempre que ela for alterada ou não encontrada;
 - 3.2.1.6.3. Deve permitir execução de scripts em pelo menos, as seguintes linguagens:
 - 3.2.1.6.4. Apple script;
 - 3.2.1.6.5. Command script;
 - 3.2.1.6.6. Javascript;
 - 3.2.1.6.7. Perl;
 - 3.2.1.6.8. Powershell;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

3.2.1.6.9. Python;

3.2.1.6.10. Unix script;

3.2.1.6.11. VBScript.

3.2.1.7. A solução deve permitir que muitas tarefas sejam concatenadas em uma apenas, possibilitando a execução em sequência de muitas atividades a partir de uma única instância de execução.

3.2.2. Descoberta e inventário completo de estações de trabalho e servidores;

3.2.2.1. A solução deve ser capaz de descobrir qualquer dispositivo que possua um endereço IP atribuído (computador, servidor, impressora, roteador, switch, hub e outros) independente de fabricante ou fornecedor;

3.2.2.2. Deve ser capaz de descobrir dispositivos por meio do protocolo SNMP (Simple Network Management Protocol);

3.2.2.3. A solução deve permitir a descoberta de ativos pelos seguintes meios:

3.2.2.3.1. Análise de redes ou ranges de IP;

3.2.2.3.2. Integração com domínio, Active Directory;

3.2.2.4. Deve permitir a execução do inventário através de políticas definidas na console central para dispositivos com agente;

3.2.2.5. Deve permitir verificações incrementais, apenas em características novas e alteradas;

3.2.2.6. Permitir a realização de inventário e descoberta de forma esporádica pelo administrador e/ou automática por meio de



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

agendamentos flexíveis, possibilitando definir frequência e horário para pelo menos, os seguintes filtros:

- 3.2.2.6.1. IP e range de IP;
- 3.2.2.6.2. Comunidade SNMP;
- 3.2.2.7. Deve realizar a captura de inventário básico, executado com periodicidade inferior aos inventários completos, contendo informações gerais dos clientes, como:
 - 3.2.2.7.1. Hostname e domínio;
 - 3.2.2.7.2. Sistema operacional, idioma, diretório de instalação e sistema de arquivos;
 - 3.2.2.7.3. Versão do sistema operacional e Service Pack;
 - 3.2.2.7.4. Tipo do dispositivo (computador, móvel, dispositivo de rede);
 - 3.2.2.7.5. Endereço Mac;
 - 3.2.2.7.6. Configurações TCP/IP de todas as placas de rede incluindo virtuais;
 - 3.2.2.7.7. Indicação de endereçamento: IP fixo ou dinâmico;
- 3.2.2.8. Captura de eventos de logon e logoff identificando usuário, domínio, data de logon e logoff e tempo total logado, independente se o computador estiver no domínio e se o logon for em domínio ou local, permitindo ao administrador identificar os usuários que estavam conectados no computador em determinado horário;
- 3.2.2.9. Executar o inventário mesmo em computadores desligados, desde que estejam com alimentação de energia na fonte (cabo ligado na tomada) e conectados à rede, no mínimo das seguintes formas:



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 3.2.2.10. Ligar o computador, inicializar o sistema operacional e executar o inventário em computadores cuja placa de rede e BIOS suportem a tecnologia wake-on-lan;
- 3.2.2.11. Ligar o computador, inicializar o sistema operacional e executar o inventário em computadores que suportem a tecnologia vPro, desde que o seu processador seja compatível com a tecnologia vPro;
- 3.2.2.12. Deve suportar à definição de limite de tempo máximo para execução do inventário, provocando a interrupção do processo caso leve mais tempo que o limite definido;
- 3.2.2.13. Deve executar o inventário de forma silenciosa sem exibição de janela e sem requerer nenhuma ação para o usuário;
- 3.2.2.14. Deve possuir inventário de pelo menos os seguintes tipos de informação de computadores Windows:
 - 3.2.2.14.1. Processador, quantidade, velocidade e tipo/marca;
 - 3.2.2.14.2. Tipo de computador: desktop, laptop, servidor ou outra classificação do fabricante;
 - 3.2.2.14.3. Fabricante do hardware, modelo, número de série;
 - 3.2.2.14.4. Código de patrimônio se estiver cadastrado no BIOS;
 - 3.2.2.14.5. Fabricante, versão e data da BIOS e informações da SMBIOS;
 - 3.2.2.14.6. Slots de memória disponíveis;
 - 3.2.2.14.7. Sistema operacional, pasta de instalação, service pack, versão, idioma, fuso horário;
 - 3.2.2.14.8. Patches e hotfixes do sistema operacional e softwares;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 3.2.2.14.9. Dispositivos configurados e respectivas configurações;
- 3.2.2.14.10. Drivers;
- 3.2.2.14.11. Endereço Mac;
- 3.2.2.14.12. Configurações TCP/IP de todas as placas de rede incluindo virtuais;
- 3.2.2.14.13. Indicação de endereço IP: fixo ou dinâmico;
- 3.2.2.14.14. Discos e pastas da rede mapeados;
- 3.2.2.14.15. Impressoras instaladas, compartilhadas e mapeadas pela rede;
- 3.2.2.14.16. Discos físicos e lógicos incluindo letras atribuídas, tamanho e propriedades;
- 3.2.2.14.17. Tamanho total em disco, total livre, na lixeira, em pastas temporárias e cache;
- 3.2.2.14.18. Particionamento dos discos e formato FAT ou NTFS;
- 3.2.2.14.19. Discos e pastas compartilhadas e respectivo acessos;
- 3.2.2.14.20. Status de compartilhamento administrativo;
- 3.2.2.14.21. Membros do grupo administração local;
- 3.2.2.14.22. Perfis de usuários existentes no computador;
- 3.2.2.14.23. Verificar grupos locais no computador;
- 3.2.2.14.24. Tarefas agendadas no sistema operacional;
- 3.2.2.14.25. Histórico de conexões à porta USB a qualquer horário;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 3.2.2.14.26. Softwares registrados no Painel de Controle, incluindo ocultos;
- 3.2.2.14.27. Softwares residentes no computador independentemente de estarem instalados ou presentes no Painel de Controle;
- 3.2.2.14.28. Conexões ODBC de sistema;
- 3.2.2.14.29. Inventário de pelo menos os seguintes tipos de informação de computadores Mac:
- 3.2.2.14.30. Processador, quantidade, velocidade, tipo e marca;
- 3.2.2.14.31. Fabricante do hardware, modelo, número de série;
- 3.2.2.14.32. Código de patrimônio se estiver cadastrado no equivalente à BIOS;
- 3.2.2.14.33. Impressoras instaladas, compartilhadas e mapeadas pela rede;
- 3.2.2.14.34. Discos físicos e lógicos, tamanho e propriedades;
- 3.2.2.14.35. Tamanho total em disco, total livre, na lixeira, em pastas temporárias e cache;
- 3.2.2.14.36. Discos e pastas compartilhadas e respectivo acessos;
- 3.2.2.14.37. Status de compartilhamento administrativo;
- 3.2.2.14.38. Membros do grupo administração local;
- 3.2.2.14.39. Perfis de usuários existentes no computador;
- 3.2.2.14.40. Verificar grupos locais no computador;
- 3.2.2.14.41. Tarefas agendadas no sistema operacional;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

3.2.2.14.42. Histórico de conexões à porta USB a qualquer horário;

3.2.2.14.43. Softwares instalados no computador, incluindo ocultos;

3.2.2.14.44. Softwares residentes no computador.

3.2.2.15. O inventário deve fornecer informações sobre as mudanças que ocorrem em todas as estações de trabalho e servidores;

3.2.2.16. O inventário deve manter histórico sobre quaisquer instalações e desinstalações de software, bem como sobre adições e remoções de hardware que ocorreram nas estações de trabalho e servidores.

3.2.3. Gerenciamento de softwares e aplicações

3.2.3.1. Deve possibilitar a distribuição e instalação de softwares, automatizar procedimentos de configuração ou manutenções rotineiras;

3.2.3.2. A distribuição de softwares deve ocorrer de forma remota e desassistida, ou seja, o usuário final não deve perceber ou interagir nesta instalação;

3.2.3.3. A solução deve possuir um ponto central de instalação, atualização e desinstalação de software;

3.2.3.4. Deve possibilitar o acompanhamento em tempo real do status da distribuição do software;

3.2.3.5. Deve possuir suporte a computadores Windows, MacOS e Linux;

3.2.3.6. Deve instalar automaticamente as aplicações ou componentes requeridos de uma aplicação principal que for instalada pela solução;

3.2.3.7. Deve possuir controle centralizado do status de distribuição do pacote;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 3.2.3.8. Através do módulo de criação de políticas, deve possibilitar a criação de políticas de distribuição de software com definição de data de início e término da validade da política, utilizando o horário do servidor de gerenciamento;
- 3.2.3.9. Deve possuir flexibilidade no agendamento da política com possibilidade de combinação de qualquer uma das regras a seguir isoladas ou simultaneamente:
- 3.2.3.9.1. Assim que o computador se comunicar com servidor;
 - 3.2.3.9.2. Somente em um determinado dia e horário;
 - 3.2.3.9.3. Assim que possível após o horário agendado.
- 3.2.3.10. A solução deve ter a capacidade de verificar previamente a necessidade de instalação das dependências, sejam elas, patches de segurança, patches de atualização, instalação de outros softwares entre outros e dentro da mesma tarefa sanar todas as dependências, para só então executar a instalação de fato do software desejado;
- 3.2.3.11. A solução deve ter a capacidade de emitir relatórios de distribuição de software, incluindo entrega, instalação e funcionalidades bem-sucedidas, identificação de máquinas off-line e instalações com falha;
- 3.2.3.12. A solução deve ter a capacidade de agrupar pacotes de aplicativos de software ou alterações e estabelecer pré-requisitos para pacotes, de modo que as alterações que exijam modificações no sistema, antes de sua implantação, sejam empacotadas, contabilizadas e com garantia de execução em uma ordem estabelecida;
- 3.2.3.13. A funcionalidade de catálogo de software deve ser organizada conforme descrição na metodologia ITIL, possibilitando o cadastro de:



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 3.2.3.13.1. Pacotes de softwares instalados;
- 3.2.3.13.2. Pacotes passíveis de distribuição pela ferramenta;
- 3.2.3.13.3. Dependência e substituição de pacotes;
- 3.2.3.13.4. Mecanismo de detecção da instalação do software;
- 3.2.3.13.5. Tarefas de instalação e remoção.

3.2.3.14. Deve permitir a implantação de um portal de software, criando uma espécie de self-service de softwares, para que os usuários possam realizar a instalação sem a necessidade de privilégios administrativos ou chamados à equipes de service desk.

3.2.4. Gerenciamento de atualizações de segurança;

- 3.2.4.1. Deve possuir suporte a computadores Windows, MacOS e Linux;
- 3.2.4.2. Deve realizar o download de atualizações de repositórios oficiais na internet, para que a distribuição interna seja planejada e tenha o controle de banda otimizado;
- 3.2.4.3. Deve executar verificação remota de vulnerabilidades e necessidades de updates, correlacionando os updates baixados com aqueles são necessários pelos agentes instalados;
- 3.2.4.4. Deve possuir relatórios gerenciais sobre vulnerabilidades e status dos patches;
- 3.2.4.5. Após a instalação de uma atualização, deve ser possível emitir notificações para usuários finais, permitindo que eles posterguem a reinicialização por um período definido na política central;
- 3.2.4.6. A solução deve ter a capacidade de importar a partir da console de gerenciamento, os resultados das varreduras contra vulnerabilidade e distribuir automaticamente os patches de correção;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

3.2.4.7. A solução deve implementar a capacidade de multicast para distribuição de atualizações de segurança, permitindo que apenas um agente faça o download do servidor central e faça a entrega para as máquinas mais próximas ou conectadas no mesmo switch;

3.2.4.8. Deve permitir a realização de gerenciamento de atualizações para soluções de pelo menos, os seguintes fabricantes:

- 3.2.4.8.1. 7-Zip;
- 3.2.4.8.2. Acro Software;
- 3.2.4.8.3. Adobe;
- 3.2.4.8.4. Amazon Services LLC;
- 3.2.4.8.5. AOL Inc;
- 3.2.4.8.6. Apache Software Foundation;
- 3.2.4.8.7. Apple;
- 3.2.4.8.8. Atlassian;
- 3.2.4.8.9. Autodesk;
- 3.2.4.8.10. Box.com;
- 3.2.4.8.11. Cisco;
- 3.2.4.8.12. Citrix;
- 3.2.4.8.13. Dropbox;
- 3.2.4.8.14. EMC;
- 3.2.4.8.15. Evernote Corporation;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 3.2.4.8.16. Foxit Corporation;
- 3.2.4.8.17. Gimp.org;
- 3.2.4.8.18. Google;
- 3.2.4.8.19. Hewlett-Packard;
- 3.2.4.8.20. LibreOffice;
- 3.2.4.8.21. Microsoft;
- 3.2.4.8.22. Mozilla Foundation;
- 3.2.4.8.23. Nitro Software, Inc.;
- 3.2.4.8.24. Notepad++;
- 3.2.4.8.25. Nullsoft;
- 3.2.4.8.26. Opera Software ASA;
- 3.2.4.8.27. Oracle;
- 3.2.4.8.28. Pidgin;
- 3.2.4.8.29. Rarlab;
- 3.2.4.8.30. Real;
- 3.2.4.8.31. RealVNC;
- 3.2.4.8.32. Research In Motion;
- 3.2.4.8.33. Simon Tatham;
- 3.2.4.8.34. Skype Technologies S.A.;
- 3.2.4.8.35. Sourceforge.Net;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 3.2.4.8.36. Splunk;
- 3.2.4.8.37. Sun Microsystems;
- 3.2.4.8.38. TeamViewer GmbH;
- 3.2.4.8.39. TechSmith;
- 3.2.4.8.40. TortoiseSVN;
- 3.2.4.8.41. UltraVNC;
- 3.2.4.8.42. VideoLAN;
- 3.2.4.8.43. VMware;
- 3.2.4.8.44. WinZip;
- 3.2.4.8.45. Wireshark Foundation;
- 3.2.4.8.46. Zoom Video Communications.

3.2.5. Medição e bloqueio de software

- 3.2.5.1. A solução deve permitir a medição e remoção de software não permitido;
- 3.2.5.2. A solução deve permitir a medição do uso de aplicações em computadores, sendo aplicativos compostos de vários arquivos ou executáveis simples;
- 3.2.5.3. Deve coletar e armazenar informações gerais sobre a utilização de aplicações, como: nome do arquivo, usuário, computador onde foi executado, data e hora;
- 3.2.5.4. Deve implementar políticas diferenciadas de medição do uso e remoção de software para grupos de computadores, permitindo que



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

um mesmo software seja executado em um computador, mas negado em outro;

3.2.5.5. Deve possibilitar o envio de alertas ao administrador quando um aplicativo é bloqueado;

3.2.5.6. Deve identificar softwares executados mesmo que não instalados;

3.2.6. A definição de lista de softwares não autorizados, deve ser baseada em nome de arquivo ou informações do cabeçalho do programa, permitindo que o bloqueio seja efetivo mesmo que o usuário modifique o nome do arquivo;

3.2.7. O bloqueio de utilização de software deve ocorrer de acordo com os seguintes critérios: Indefinidamente (sempre), somente em determinados horários ou somente em determinados dias e horários;

3.2.8. Gerenciamento de imagens de sistemas operacionais

3.2.8.1. Deve permitir a captura e distribuição de sistema operacional;

3.2.8.2. Deve provisionar dinamicamente uma imagem, contendo suas configurações e software para os computadores que se conectarem à rede usando regras por MAC Address, tipo de hardware, rede local, e outros dados;

3.2.8.3. Deve possuir a capacidade de transmitir pacotes via multicast, o cliente deve receber a imagem e depois enviar via multicast para o resto dos clientes que irão receber a imagem;

3.2.8.4. A solução deve permitir a utilização de PXE;

3.2.8.5. Deve possuir meios para realização das tarefas de imagem, mesmo quando PXE não estiver disponível;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

3.2.8.6. O processo de disponibilização da imagem em uma estação de trabalho deve seguir o fluxo completo, entregando não apenas o sistema no destino, mas também todas as configurações, drivers e softwares desejáveis para funcionamento mínimo do equipamento.

3.2.8.7. Para entregar drivers, não deve ser necessário a customização de imagens para sua inserção. A solução deve possuir um banco de drivers a ser consultado durante o processo para instalação apenas aqueles designados para o equipamento destino.

4. Item 4 - Subscrição Symantec Messaging Gateway Hybrid – SKU: SMG-HYB-SUB

4.1. Características Gerais

4.1.1. A solução deverá ser ofertada na modalidade de serviço (SaaS);

4.1.2. Deve funcionar como SMTP Mail sendo compatível no mínimo com os seguintes serviços de correio eletrônico: Microsoft Exchange, Microsoft Office 365 e Google Apps;

4.1.3. Deve contemplar, no mínimo, as funcionalidades de antivírus, AntiSpam, anti-spyware, anti-phishing, anti-ransomware, controle de worms, filtro de conteúdo, controle de arquivos de imagem, filtro contra novos vírus sem assinatura e criptografia;

4.1.4. A solução deve apresentar no mínimo 95% de precisão na detecção de uma ameaça, ou seja, 5% no máximo de falso -positivo; e falso-negativo;

4.1.5. A solução deverá conter filtros para análise de imagem, e estes filtros deverão possuir no mínimo controles tipo:

4.1.5.1. Exposição de pele, a fim de detectar possíveis imagens de pornografia;

4.1.5.2. Controle granular de imagem;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 4.1.5.3. Possuir lista branca/lista negra para envio e recebimento de imagens;
- 4.1.5.4. Detecção de links maliciosos através de imagens;
- 4.1.5.5. Detecção de Spam/ameaças através de imagens no corpo do e-mail;
- 4.1.5.6. Detectar e verificar imagens em arquivos office da Microsoft;
- 4.1.6. A solução deverá conter uma base de reputação global de imagens.
- 4.1.7. A solução deverá nativamente ser capaz de detectar links maliciosos no corpo do e-mail e testar todos os pontos de conexão até seu último destino, a fim de detectar possíveis malwares provenientes de um phishing;
- 4.1.8. A solução deverá prover relatório sobre bloqueio de links maliciosos;

4.2. Características específicas

4.2.1. Gerenciamento

- 4.2.1.1. Permitir gerenciamento unificado, contemplando todas as funcionalidades da solução, via web HTTP e HTTPS;
- 4.2.1.2. Possuir console de gerenciamento, no mínimo, nas linguagens Inglês e Português do Brasil;
- 4.2.1.3. Deve possuir a capacidade de enviar alertas via SMS, para telefones dos administradores cadastrados na console de gerenciamento;
- 4.2.1.4. Deve ser possível integrar com o Active Directory para manter sincronizado a lista de usuários do Órgão;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 4.2.1.5. Deve ser possível cadastrar diversos administradores com perfis diferentes;
- 4.2.1.6. Deve ser possível configurar os perfis de administração com funções específicas;
- 4.2.1.7. Deve suportar múltiplos domínios (registros MX), para no mínimo 200 domínios;
- 4.2.1.8. A solução deve ser multitenant, na qual as regras de detecção serão exclusivas para cada domínio, não sendo possível que uma regra seja lida para um domínio mesmo que não se aplique, otimizando assim o processamento da solução e garantindo sigilo;
- 4.2.1.9. A solução deve ter a capacidade de implementar um conjunto políticas globais, assim como, políticas específicas para cada domínio administrado pela solução;

4.2.2. Características de varredura de mensagens:

- 4.2.2.1. Deve processar o fluxo de entrada e de saída de mensagens de correio eletrônico, possibilitando a customização de políticas;
- 4.2.2.2. Prover a funcionalidade de incluir “disclaimers”, em formato html e texto, tanto no início quanto no rodapé das mensagens enviadas;
- 4.2.2.3. Deve ser possível configurar o tamanho máximo da mensagem a ser analisada.

4.2.3. Características do módulo antivírus:

- 4.2.3.1. Deve suportar a detecção heurística de vírus;
- 4.2.3.2. Deve reconhecer, detectar e bloquear spywares, adwares, worms e Trojan;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 4.2.3.3. Deve reconhecer, detectar e bloquear ameaças via análise de comportamento;
- 4.2.3.4. Deve ser capaz de realizar o filtro de malwares na entrada e na saída de e-mails;
- 4.2.3.5. Deve possuir notificação de e-mails bloqueados pelo módulo antivírus, podendo ser customizado pelo administrador da solução, podendo ser enviada para o administrador da solução e destinatário/remetente;
- 4.2.3.6. A solução deve ter integração nativa com a solução contra ataques de APT em e-mail do mesmo fabricante;
- 4.2.3.7. A solução deve prover tecnologia de detecção em múltiplas camadas, para no mínimo:
 - 4.2.3.7.1. Heurística;
 - 4.2.3.7.2. Scan dos hyperlinks (curtos e normais) para validar se são maliciosos ou não, verificando se são utilizados para spam, phishing entre outras finalidades, executando o bloqueio da mensagem em tempo real;
 - 4.2.3.7.3. Verificação de ameaças utilizando tecnologia de Sandbox em nuvem do fabricante.
- 4.2.3.8. A solução deve prover proteção contra “spear phishing” utilizando a verificação de hyperlinks (curtos e normais) independentemente da quantidade de redirecionamentos existentes nestes links, através de no mínimo duas técnicas:
- 4.2.3.9. Utilizando a verificação do hyperlink no momento que a solução recebe a mensagens;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 4.2.3.10. Utilizando a verificação quando o usuário acessa o hyperlink, evitando desta forma que, manipulações posteriores as verificações por parte da solução sejam capazes de serem efetivas.
- 4.2.3.11. A solução deve proteger contra os ataques avançados de “Stealthy”, através de técnicas de machine learning utilizadas pela estrutura de sandbox da solução, executando arquivos tanto em ambiente virtual como físico possibilitando o bloqueio de ataques de “Targeted” e “Advanced Threats”;
- 4.2.3.12. A solução deve ter a capacidade de integração com soluções de SIEM – Security Information and Event Management;
- 4.2.3.13. A solução deve ter integração nativa com soluções de DLP de e-mail;
- 4.2.3.14. A solução deve suportar de forma automática a criptografia de e-mails de saída a partir de políticas de detecção pré-definidas pelo administrador da ferramenta;
- 4.2.3.15. A solução deve ter a capacidade de proteger contra ataques de dia zero.

4.2.4. Características do módulo AntiSpam:

- 4.2.4.1. Deve permitir configurar regras de AntiSpam exclusivas para domínios diferentes;
- 4.2.4.2. Deve utilizar, pelo menos, as seguintes tecnologias de detecção de spams: assinaturas para corpo da mensagem e anexos, análise heurística (análise de cabeçalho, conteúdo e estrutura da mensagem), filtro de URLs, filtro anti-phishing e proteção contra ataques direcionados;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 4.2.4.3. Deve possuir recurso de detecção de ataques de diretório, sendo capaz de recusar a mensagem caso o usuário destinatário seja inválido;
- 4.2.4.4. Deve permitir gerenciar política de análise de spam por regra de entrada e por grupo de usuários com opções de ação como quarentenar, negar entrega e marcar assunto com tag de acordo com a probabilidade de a mensagem ser spam;
- 4.2.4.5. Deve possuir recurso de lista de bloqueio personalizada, onde os endereços cadastrados nesta serão bloqueados pela solução. Esta lista pode ser preenchida por endereços IP, domínios ou endereços de email;
- 4.2.4.6. Deve possibilitar a utilização de funcionalidades como DMARC e SPF;
- 4.2.4.7. Deve permitir gerenciar política de análise de spam pelo uso de RBLs (Realtime Blackhole List), ou seja, lista dinâmica de endereços IPs que comprovadamente enviam spams;
- 4.2.4.8. Deve permitir gerenciar política de análise de spam pelo bloqueio de backscatter, ou seja, mensagens de retorno automatizadas.

4.2.5. Saída de e-mails (outbound)

- 4.2.5.1. Deve possuir mecanismos de proteção, que identifiquem spam e vírus na saída de e-mails do Órgão, bloqueando a mensagem, prevenindo a inclusão do domínio do Órgão em listas de bloqueio de spams e evitando ataques oriundos da rede interna do Órgão;
- 4.2.5.2. Deve realizar a análise de malwares, bloqueando automaticamente caso o e-mail possua alguma ameaça;

4.2.6. Filtro de conteúdo



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 4.2.6.1. Deve verificar o envelope da mensagem: remetente, destinatário, assunto, cabeçalho, anexos e corpo da mensagem;
- 4.2.6.2. Deve possibilitar filtragem baseada no cabeçalho da mensagem, dicionário predefinido e customizado com palavras-chave e expressões regulares;
- 4.2.6.3. Deve possuir modelos pré-definidos de políticas atendendo a padrões de mercado, como PCI e HIPAA;
- 4.2.6.4. Deve permitir gerenciamento de política de filtro de conteúdo (palavras-chave) por entrada e por grupo de usuários com opções de ações como: negar entrega, comprimir os anexos, redirecionar para o administrador, marcar assunto com tag e notificação de envio de e-mail para remetente e destinatário;
- 4.2.6.5. Deve permitir gerenciar política de filtro de anexos por domínio de entrada e saída, bem como por grupo de usuários com opções para, no mínimo, os tipos de anexo compactados, executáveis e scripts, com opções de ação como negar entrega, remover o anexo e notificação de envio de e-mail para remetente e destinatário;

4.2.7. Quarentena

- 4.2.7.1. Deve possuir a capacidade de colocar mensagens suspeitas em quarentena;
- 4.2.7.2. Deve enviar notificações aos usuários com informações sobre a quarentena pessoal.
- 4.2.7.3. Deve ser possível configurar a periodicidade de envio de notificações da quarentena pessoal;
- 4.2.7.4. Deve ser possível escolher a linguagem para as notificações enviadas aos usuários, possuindo no mínimo Português do Brasil e Inglês;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

4.2.7.5. Deve permitir que o acesso a quarentena seja feito pelo próprio usuário, ou pelo administrador(es) da solução;

4.2.7.6. Deve permitir a liberação ou exclusão de mensagens.

4.2.8. Relatórios e auditoria

4.2.8.1. Deve possuir dashboard contendo informações de quantidade de e-mails analisados, tanto na entrada quanto na saída, bem como informações de filtros de AntiSpam e anti-malware;

4.2.8.2. Deve disponibilizar relatórios com opção separada para tráfego por domínio de mensagens;

4.2.8.3. Deve disponibilizar relatórios de visão geral do tráfego, quantidade de e-mails com vírus, spam e filtro de conteúdo;

4.2.8.4. Deve disponibilizar relatório específico de incidentes de ataques direcionados e persistentes;

4.2.8.5. Deve disponibilizar rastreamento dos e-mails através de ferramenta integrada no próprio portal, permitindo ao administrador da solução realizar buscas dessas mensagens através do remetente, destinatário, data e assunto, bem como ter o status atual da mensagem (entregue, fila de entrega, tipo de filtro aplicado e ação executada);

4.2.8.6. Deve possibilitar agendamento e envio de relatórios por e-mail;

5. Item 5 - Subscrição Symantec Data Loss Prevention – SKU: DLP-ES-SUB

5.1. Características Gerais

5.1.1. Deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações confidenciais detectadas;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.1.2. O licenciamento da solução proposta deve contemplar todas as funcionalidades descritas para este software.
- 5.1.3. Deve ter console de gerenciamento via tecnologia Web (HTTP e HTTPS).
- 5.1.4. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais abaixo:
- 5.1.4.1. Microsoft Windows Server;
 - 5.1.4.2. Red Hat Enterprise Linux;
 - 5.1.4.3. Suportar hardware x86_x64, e o sistema operacional Windows Server 2012 R2 e Linux RedHat Enterprise Versão 5, ou superiores.
- 5.1.5. Suportar funcionamento em sistemas de virtualização.
- 5.1.6. Envio de alertas em tempo real, por e-mail, sobre as condições gerais de saúde e estabilidade do sistema.
- 5.1.7. Suportar funcionamento em plataformas de Single Sign-On (SSO).
- 5.1.8. A solução deverá criptografar toda a comunicação que ocorre entre os servidores de gerenciamento e os agentes instalados em terminais.
- 5.1.9. A solução deverá criptografar a comunicação entre o servidor principal e os servidores adicionais da plataforma.
- 5.1.10. Possuir registros detalhados de auditoria de atividades de sistema.
- 5.1.11. Os dados de auditoria de sistema devem fornecer todas as informações necessárias para acompanhamento de saúde dos servidores que contemplam a plataforma, e também para cada agente instalado.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.1.12. A plataforma deve permitir a criação de relatórios e alertas (Enviados por email periodicamente) para critérios que envolvam o monitoramento de saúde da solução.
- 5.1.13. Permitir a instalação em Sistema Operacional restrito, com serviços e configurações de portas limitados (Hardening).
- 5.1.14. Deve possuir módulos de detecção distintos, gerenciados por console único, para:
- 5.1.15. Localizar dados confidenciais armazenados em servidores de arquivos, intranet, bancos de dados e servidores de e-mail;
- 5.1.16. Localizar dados confidenciais armazenados em desktops e laptops;
- 5.1.17. Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP, permitindo customização de protocolos que não são cadastrados na plataforma por padrão;
- 5.1.18. Detectar vazamento de dados a partir de conexão direta com servidores de e-mail;
- 5.1.19. Detectar vazamento de dados a partir de conexão direta com appliances responsáveis pelo processamento de tráfego WEB (Proxy ou UTM);
- 5.1.20. Capacidade de obter a “impressão digital” de dados estruturados e não estruturados (MS Office docs, PDFs, EMC Documentum, diagramas CAD/CAM, código-fonte, etc.).
- 5.1.21. Capacidade para detectar, utilizando fontes não estruturadas, o vazamento de informações em canais de monitoramento, a partir de um percentual de similaridade definido entre as fontes de dados armazenadas e a informação em circulação.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.1.22. A detecção por nível de similaridade deve ter seu percentual configurado no console, durante a criação da política, permitindo minimamente:
- 5.1.22.1. Criação de um incidente sempre que for detectado um vazamento de um documento monitorado em um percentual pré-definido.
- 5.1.22.2. O percentual definido deve ser customizado a nível de política, permitindo a utilização de valores diferentes para cada tipo de informação monitorada.
- 5.1.23. Capacidade de normalizar variações comuns de apresentação de dados para aprimorar a precisão de políticas de monitoramento.
- 5.1.24. Capacidade de identificar dados estruturados e não estruturados, sem necessidade de utilização de servidores adicionais ou dedicados para este fim.
- 5.1.25. Detectar documentos não estruturados, após usar capacidades nativas de aprendizado automático para analisar um conjunto de amostras.
- 5.1.26. Permitir detectar documentos não estruturados sem a necessidade de “impressões digitais”.
- 5.1.27. Permitir a criação de padrão de identificação utilizando dados internos da instituição de modo a customizar a ferramenta.
- 5.1.28. Permitir personalizar padrões pré-configurados de identificação de dados.
- 5.1.29. Permitir detecção de acordo com expressões regulares configuráveis.
- 5.1.30. Permitir detecção por tipo de arquivo, por nome e extensão de arquivo, remetente/destinatário e protocolo de transmissão.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.1.31. Capacidade de criar política em uma única interface que pode ser implementada em todos os componentes da rede, endpoint e storage.
- 5.1.32. Capacidade de integração direta com LDAP e MS Active Directory para criar regras de detecção baseadas em usuário ou grupo.
- 5.1.33. Permitir a exportação e importação das regras de detecção existentes através da console de gerenciamento.
- 5.1.34. Possuir mecanismo de envio de notificações personalizadas por e-mail aos administradores.
- 5.1.35. Permitir a criação de perfis para administração de servidores, administração de usuário, criação e edição de política.
- 5.1.36. Permitir o envio manual ou automatizado de listas de incidentes personalizadas para os respectivos proprietários.
- 5.1.37. Armazenar e exibir a mensagem original ou arquivo que gerou o incidente.
- 5.1.38. Em um determinado incidente, permitir a verificação do mesmo por assunto, remetente, destinatário, nome de arquivo, proprietário do arquivo, nome de usuário e política.
- 5.1.39. Exibir todo o histórico, inclusive as alterações e edições, referentes ao incidente.
- 5.1.40. Permitir a exportação da lista de incidentes no formato XML e CSV.
- 5.1.41. Possuir interface WEB, compatível, no mínimo, com os navegadores Internet Explorer, Mozilla Firefox e Google Chrome.
- 5.1.42. Permitir a configuração de respostas automáticas com base na severidade, contagem de combinações e política.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.1.43. Capacidade de indicar, automaticamente, o status de incidente, com base em regras acionadas e contagem de combinações.
- 5.1.44. Deve possuir integração com LDAP e MS Active Directory, para obter detalhes e informações adicionais dos usuários envolvidos num incidente detectado.
- 5.1.45. Deve possuir integração com LDAP e MS Active Directory, para autenticação de usuários da solução.
- 5.1.46. Deve manter um histórico de alterações de sistema e acompanhamentos de incidentes.
- 5.1.47. Deve possuir logs detalhados de auditoria de alterações de políticas.
- 5.1.48. A solução deve ter capacidade de descoberta de vazamento de dados nos seguintes canais:
 - 5.1.48.1. Nuvem;
 - 5.1.48.2. E-mail;
 - 5.1.48.3. Web;
 - 5.1.48.4. endpoint;
 - 5.1.48.5. Plataforma de armazenamento de dados.
- 5.1.49. Monitorar como os dados estão sendo usados dentro e fora da rede corporativa.
- 5.1.50. Proteger os dados contra exposição ou roubo em tempo real.
- 5.1.51. A atividade de detecção deve ser realizada de forma distribuída.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.1.52. Deve permitir ocultar certos dados, como informações de identidade do remetente, durante a visualização do Incidente na tela do Console, dependendo do nível de acesso dado ao operador da ferramenta, para no mínimo, os seguintes tópicos:

5.1.52.1. Endereço de e-mail;

5.1.52.2. Nome de usuário;

5.1.52.3. Proprietário do arquivo.

5.1.53. Deve suportar a verificação de arquivos compactados recursivos (exemplos .zip, .rar dentro de .zip, .rar).

5.1.54. Deve suportar de forma comprovada a detecção de dados no idioma português brasileiro.

5.1.55. Deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails.

5.1.56. Deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem.

5.1.57. Deve identificar conteúdo armazenados em colunas específicas de planilhas eletrônicas e em bancos de dados.

5.1.58. Deve possuir capacidade para identificar conteúdo específicos com base em um padrão pré-determinado, para no mínimo:

5.1.58.1. CPF;

5.1.58.2. CNPJ;

5.1.58.3. Número do título de eleitor;

5.1.58.4. RG;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.1.58.5. Dados de tecnologia com o IP Address e IMEI de telefones.

5.1.59. Deve ter a capacidade de detectar presença de conteúdo cifrado/criptografado.

5.1.60. Deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo.

5.1.61. A solução deve possuir, integrada na console, a funcionalidade de workflow para tratamento e escalonamento dos incidentes (Regras a serem acionadas após a detecção de um incidente, podendo contar com regras manuais e automáticas).

5.1.62. Deve ser possível utilizar no workflow, de forma manual ou automática, as seguintes características, para manipulação do incidente:

5.1.62.1. Severidade;

5.1.62.2. Protocolo;

5.1.62.3. Identificação do endpoint;

5.1.62.4. Quantidade de dados confidenciais expostos;

5.1.62.5. Tipo de incidente;

5.1.62.6. Informações provenientes de Antivirus que indiquem a reputação do arquivo que transferiu a informação sigilosa;

5.1.62.7. A localidade do endpoint.

5.1.63. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente para, no mínimo:

5.1.63.1. Data e hora da violação da regra;

5.1.63.2. Status do incidente;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.1.63.3. Severidade do incidente;
 - 5.1.63.4. Política que foi acionada;
 - 5.1.63.5. Técnica de detecção utilizada;
 - 5.1.63.6. Equipamento Servidor que detectou o incidente;
 - 5.1.63.7. Ações automáticas ou manuais que foram realizadas;
 - 5.1.63.8. Histórico completo dos incidentes;
 - 5.1.63.9. Usuário que infligiu a política;
 - 5.1.63.10. Nome endpoint ou endereço IP;
 - 5.1.63.11. Amostra dos dados detectados;
 - 5.1.63.12. Atributos customizados ou padrão.
- 5.1.64. A plataforma deve relacionar os incidentes, proporcionando visões que facilitem a descoberta de possíveis reincidências.
- 5.1.65. Deve possuir informações detalhadas a respeito do banco de dados da ferramenta, para acompanhamento da saúde e utilização de todas as tabelas.
- 5.1.66. Deve possuir a capacidade de exclusão de incidentes em massa, com periodicidade definida pelo administrador e obedecendo critérios específicos.

5.2. Características específicas

- 5.2.1. Criação de Políticas e Detecção de Conteúdo Confidencial
- 5.2.2. Toda política criada na solução deve ser única, compatível e válida para aplicação em qualquer um dos módulos existentes, endpoint, rede, e-mail ou storage, sem a necessidade de duplicação ou recriação.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.2.3. Deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:

- 5.2.3.1. Palavra ou conjunto de palavras-chave;
- 5.2.3.2. Identificadores pré-existentes ou customizados (CPF, CNPJ, Cartão de crédito, etc.);
- 5.2.3.3. Expressões regulares com possibilidade de adaptação para qualquer padrão de dados existentes;
- 5.2.3.4. Conteúdo detectado em arquivos;
- 5.2.3.5. Protocolos de comunicação;
- 5.2.3.6. Nome, tipo, extensão ou tamanho de arquivos;
- 5.2.3.7. Remetente e destinatário de e-mails;
- 5.2.3.8. Conjunto de dados estruturados ou não estruturados;
- 5.2.3.9. Usuários ou grupos de Active directory;
- 5.2.3.10. Cópias para dispositivos USB;
- 5.2.3.11. Dados enviados para fila de impressão;
- 5.2.3.12. Dados copiados para o clipboard;
- 5.2.3.13. Dados copiados para compartilhamentos de rede;
- 5.2.3.14. Aplicativos pré-existentes ou customizados que trafegam informações;
- 5.2.3.15. Cópia para armazenamento em nuvem.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.2.4. Deve permitir alterar a criticidade do incidente, seja por meio de políticas diferentes ou meios automáticos, baseado em valores de referência e limites configuráveis para, no mínimo:

- 5.2.4.1. Quantidade de dados expostos;
- 5.2.4.2. Dados específicos expostos;
- 5.2.4.3. Arquivos específicos expostos;
- 5.2.4.4. Remetente de correio específico;
- 5.2.4.5. Destinatário de correio específico;
- 5.2.4.6. Protocolo de comunicação utilizado.

5.2.5. Deve possibilitar criação de regras de exclusões para as políticas de acordo com grupos de usuários fornecidos pelo LDAP ou MS Active Directory.

5.2.6. O produto deve possuir modelos de políticas de detecção com base em regulamentações e melhores práticas de mercado, para no mínimo:

- 5.2.6.1. PCI;
- 5.2.6.2. HIPAA;
- 5.2.6.3. GDPR.

5.2.7. A solução deve possibilitar a criação de regras para adequação à Lei Geral de Proteção de Dados - LGPD.

5.2.8. A solução deve possuir modelos de políticas de detecção, para no mínimo os seguintes temas:

- 5.2.8.1. Proteção de dados de usuários e funcionários;
- 5.2.8.2. Dados que envolvem segurança de redes;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.2.9. Deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:

5.2.9.1. Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);

5.2.9.2. Compactados (ZIP, RAR, GZ, LHA, HQX, JAR, 7z);

5.2.9.3. CAD (DWG, DXF, VSD, DGN);

5.2.9.4. Planilhas (XLS, XLSX, 123, SXC, ODS, CSV);

5.2.9.5. Apresentações (PPT, PPTX, SXI, SXP, ODP);

5.2.9.6. Outros (PDF, MDB).

5.2.10. As políticas de detecção devem ter a capacidade de definir um percentual do documento indexado para detectar um incidente;

5.2.11. Deve permitir criar políticas que combinem várias tecnologias e regras de detecção com operadores lógicos (E, OU) e de exceção.

5.2.12. Deve ter a capacidade de exportar e importar as políticas existentes, pela interface gráfica do console.

5.2.13. Deve ter a capacidade de detecção utilizando combinações de palavras, possibilitando ignorar a regra caso a detecção das palavras ultrapasse a distância (em quantidade de palavras) configurada na política.

5.2.14. Deve ter a capacidade de construir políticas de detecção, configurando-se o grau de severidade adotado para cada regra criada, conforme o número de correspondências que se deseja encontrar em cada possível violação.

5.2.15. As políticas de detecção devem possuir, no mínimo:

5.2.15.1. A capacidade de normalização de todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

contiver "123456789", deverá ter como correspondente "123-45-6789", "123456789", "123.45.6789", etc.);

5.2.15.2. A capacidade de detecção usando palavras e frases-chave totalmente configuráveis;

5.2.15.3. A capacidade de colocar múltiplas palavras/frases em uma única regra de detecção.

5.2.15.4. A capacidade de detectar faixas de números válidos para determinados tipos de dados, tal como no mínimo, número de cartão nacional de saúde válido.

5.2.16. Resposta a incidentes

5.2.16.1. Deve possuir notificações personalizáveis através de e-mail em caso de violação de política.

5.2.16.2. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações.

5.2.16.3. Deve ser possível notificar automaticamente o remetente, gerente e/ou superior hierárquico do usuário envolvido no incidente.

5.2.16.4. Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, ou seja, execução programada logo após o registro do incidente, iniciando automaticamente o processo de resposta, para no mínimo:

5.2.16.4.1. Adicionar um comentário no incidente;

5.2.16.4.2. Enviar e-mails de notificação;

5.2.16.4.3. Adicionar atributos no incidente;

5.2.16.4.4. Alterar status do incidente;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.16.4.5. Quarentenar arquivos descobertos;
- 5.2.16.4.6. Bloqueio de transferência de arquivos para compartilhamento de rede;
- 5.2.16.4.7. Bloqueio de Impressão;
- 5.2.16.5. Bloqueio de gravação de CD/DVD;
- 5.2.16.6. Bloqueio de cópias para dispositivos USB;
- 5.2.16.7. Bloqueio em aplicações pré-cadastradas;
- 5.2.16.8. Bloqueio para comunicações FTP, HTTP, HTTPS ou SMTP;
- 5.2.16.9. Modificar o cabeçalho SMTP quando o incidente ocorrer via e-mail;
- 5.2.16.10. Enviar incidente via syslog;
- 5.2.16.11. Notificação para o usuário.
- 5.2.17. As ações listadas nos tópicos acima devem ser apresentadas de forma nativa, sem necessidade de customização de scripts ou rotinas para efetivação das funcionalidades requeridas.
- 5.2.18. Deve disponibilizar interface de resposta totalmente personalizável que permita combinações de várias ações de reparo e reação, através da interface gráfica do Incidente.
- 5.2.19. A interface gráfica de ser customizada para possibilitar no mínimo:
 - 5.2.19.1. Adicionar um comentário no incidente;
 - 5.2.19.2. Enviar um log do incidente para syslog;
 - 5.2.19.3. Enviar uma notificação por e-mail;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.19.4. Criação de ações customizadas;
- 5.2.19.5. Adicionar atributos nos incidentes;
- 5.2.19.6. Alterar o status dos incidentes;
- 5.2.19.7. Manipular arquivos no Sharepoint.
- 5.2.20. Deve exibir todos os detalhes do incidente em uma única página.
- 5.2.21. Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo.
- 5.2.22. Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente.
- 5.2.23. Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente.
- 5.2.24. Relatórios**
 - 5.2.24.1. Deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:
 - 5.2.24.1.1. ID do incidente;
 - 5.2.24.1.2. Resposta do agente;
 - 5.2.24.1.3. Hash ou nome da aplicação;
 - 5.2.24.1.4. Dono da informação;
 - 5.2.24.1.5. IP de destino;
 - 5.2.24.1.6. Nome, tamanho e localização do arquivo;
 - 5.2.24.1.7. Quantidade de dados expostos;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.24.1.8. Comentários do incidente;
- 5.2.24.1.9. Localização do endpoint;
- 5.2.24.1.10. Endereço IP do endpoint;
- 5.2.24.1.11. Nome do endpoint;
- 5.2.24.1.12. Usuário;
- 5.2.24.1.13. Política acionada;
- 5.2.24.1.14. Protocolos ou canais de detecção do agente;
- 5.2.24.1.15. Remetente/destinatário;
- 5.2.24.1.16. Servidor de detecção;
- 5.2.24.1.17. Reputação de arquivo proveniente de software de antivírus;
- 5.2.24.1.18. Atributos customizados;
- 5.2.24.1.19. Justificativa de usuário;
- 5.2.24.1.20. Domínio/URL.
- 5.2.24.2. Deve permitir gerar relatórios resumidos por níveis, agrupados, sumarizados e com capacidade de detalhamento;
- 5.2.24.3. O agrupamento dos relatórios deve permitir utilização de filtros para no mínimo os seguintes parâmetros:
 - 5.2.24.3.1. Hash do arquivo;
 - 5.2.24.3.2. Dono da informação;
 - 5.2.24.3.3. IP de destino;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.24.3.4. Domínio;
 - 5.2.24.3.5. Políticas de detecção;
 - 5.2.24.3.6. Localização do endpoint;
 - 5.2.24.3.7. Nome do arquivo;
 - 5.2.24.3.8. Protocolo ou canal de detecção do endpoint;
 - 5.2.24.3.9. Endereço IP ou nome de endpoint;
 - 5.2.24.3.10. Remetente ou destinatário;
 - 5.2.24.3.11. Servidor de detecção;
 - 5.2.24.3.12. Status do incidente;
 - 5.2.24.3.13. Usuário;
 - 5.2.24.3.14. Atributos customizados do incidente.
- 5.2.24.4. Deve fornecer relatórios de tendências com gráficos distribuídos em uma linha de tempo.
- 5.2.24.5. Deve exportar relatórios para formato XML e CSV.
- 5.2.24.6. Deve agendar relatórios para envio automático através de e-mail (datas específicas e periodicamente).
- 5.2.24.7. Deve apresentar um painel para visualização dos relatórios.
- 5.2.24.8. Deve possuir API para permitir que aplicações de terceiros extraiam dados de incidentes da base de dados do DLP.
- 5.2.24.9. Deve ter a capacidade para configurar, salvar relatórios e painéis personalizados por usuário.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.2.24.10. Deve possuir painéis (Dashboards) para, no mínimo os seguintes itens:

5.2.24.10.1. Sumário de políticas mais acionadas durante o monitoramento de vazamento de informações;

5.2.24.10.2. Usuários que mais violaram políticas de segurança;

5.2.24.10.3. Tipos de incidentes que mais ocorreram.

5.2.25. Módulo de descoberta e armazenamento

5.2.25.1. Deve verificar existência de conteúdo confidencial em file systems sem a necessidade de agentes de coleta (agentless) para no mínimo CIFS, NFS, SMB e NTFS.

5.2.25.2. Deve permitir a análise dos file systems através de agentes ou sem agente em sistemas operacionais, para no mínimo:

5.2.25.2.1. Windows Server 2008 R2;

5.2.25.2.2. Windows Server 2012;

5.2.25.2.3. Windows Server 2016;

5.2.25.2.4. Red Hat Enterprise Linux 6 e demais releases da versão;

5.2.25.2.5. Red Hat Enterprise Linux 7 e demais releases da versão.

5.2.25.3. Deve analisar conteúdo sigiloso armazenado em ambientes complexos, para no mínimo:

5.2.25.3.1. Microsoft Sharepoint;

5.2.25.3.2. Microsoft SQL Server;

5.2.25.3.3. Oracle;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.25.3.4. Microsoft Exchange;
- 5.2.25.3.5. Web servers;
- 5.2.25.3.6. Live Link.
- 5.2.25.4. Deve possuir a capacidade de verificar arquivos Microsoft "PST", possibilitando executar varreduras nas mensagens, assim como, nos arquivos anexos as mensagens.
- 5.2.25.5. Possibilidade de mover para quarentena arquivos que violam políticas de segurança.
- 5.2.25.6. Deve manter o arquivo no local original, substituindo seu conteúdo por uma mensagem customizável, como aviso e orientação para o usuário.
- 5.2.25.7. Permitir a remoção do arquivo que está em quarentena e restaurá-lo de volta ao local original.
- 5.2.25.8. Permitir a criptografia de arquivos definidos como confidenciais, utilizando ferramenta de terceiros, e completamente integrado a solução fornecida.
- 5.2.25.9. Deve permitir coleta automática de evidências de violações das políticas para análise legal.
- 5.2.25.10. Permitir a criação de respostas personalizadas para incidentes.
- 5.2.25.11. Exibir detalhes, no incidente, dos arquivos que tiveram as políticas violadas.
- 5.2.25.12. Exibir no incidente o local e as informações do proprietário dos arquivos que tiveram as políticas violadas.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.25.13. Permitir a emissão de relatórios de usuários que mais editaram arquivos e que tiveram as políticas violadas.
- 5.2.25.14. Permitir a emissão de relatórios baseado em dados de acesso e modificação de arquivos que tiveram as políticas violadas.
- 5.2.25.15. Permitir a visualização das permissões efetivas do arquivo. Estas informações devem ser coletadas automaticamente do módulo de visibilidade e auditoria de dados em repouso.
- 5.2.25.16. Deve possibilitar notificação através de e-mail e alerta Syslog em caso de violação de política.
- 5.2.25.17. Deve permitir agendamento de varreduras automáticas.
- 5.2.25.18. Possuir mecanismo de verificação incremental, na qual apenas arquivos novos, ou alterados, sejam verificados.
- 5.2.25.19. Deve permitir configurar janelas de tempo para verificações, interrompendo o processo automaticamente ao fim do período configurado.
- 5.2.25.20. Deve ter a capacidade de definir número limite de incidentes para interromper varreduras.
- 5.2.25.21. Preservar os atributos originais do arquivo, inclusive o atributo "Acessado em", enquanto realiza a verificação.
- 5.2.25.22. Possuir capacidade de pausar, manualmente, a verificação.
- 5.2.25.23. Deve utilizar técnicas de paralelismo e controle de banda.
- 5.2.25.24. Permitir o controle da velocidade das verificações para limitar o uso da largura de banda da rede.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.25.25. Deve ter a capacidade de reutilizar uma única credencial (usuário/senha) em múltiplos alvos a serem verificados.
- 5.2.25.26. Permitir a verificação simultânea em vários alvos distintos.
- 5.2.25.27. Permitir limitar quais portas de comunicação serão utilizadas entre o sistema-alvo e o servidor que faz a verificação.
- 5.2.25.28. Deve permitir filtros por diretório e tipo de arquivo para a varredura de verificação.
- 5.2.25.29. Deve permitir filtros por diretório e tipo de arquivo para ignorar a varredura de verificação.
- 5.2.25.30. Deve permitir aplicar filtros para verificar arquivos adicionados, acessados e modificados entre determinadas datas.

5.2.26. Módulo de endpoint

- 5.2.26.1. Capacidade de descobrir fuga de informações sensíveis, por meio de agente.
- 5.2.26.2. Possibilidade de aplicação de políticas mesmo quando o agente não tem comunicação com o servidor de gerenciamento.
- 5.2.26.3. Possibilidade de armazenamento em cache, dos arquivos que causaram o incidente até que o usuário se conecte, novamente, à rede corporativa.
- 5.2.26.4. Monitorar e bloquear a cópia de dados não permitidos para dispositivos de armazenamento removível (USB).
- 5.2.26.5. Monitorar e bloquear a cópia de dados não permitidos para dispositivos CD/DVD.
- 5.2.26.6. Monitorar e bloquear a cópia de dados não permitidos em unidades de armazenamento local.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.2.26.7. Monitorar e bloquear dados não permitidos enviados a qualquer tipo de impressora local e de rede.

5.2.26.8. Monitorar e bloquear ações de copiar e colar feitas através da área de transferência do Windows.

5.2.26.9. Monitorar e bloquear e-mail corporativo no uso do Microsoft Outlook durante o envio de dados não permitidos.

5.2.26.10. Monitorar e bloquear transmissões HTTP e HTTPS pelo menos nos seguintes navegadores:

5.2.26.10.1. Internet Explorer;

5.2.26.10.2. Microsoft Edge;

5.2.26.10.3. Mozilla Firefox;

5.2.26.10.4. Google Chrome;

5.2.26.10.5. Safari.

5.2.26.11. Monitorar e bloquear transmissões via FTP.

5.2.26.12. Monitorar e bloquear o uso de dados confidenciais por qualquer aplicativo, incluindo programas de criptografia não autorizados.

5.2.26.13. Monitorar e bloquear a cópia de dados nos compartilhamentos de rede pelo Windows Explorer.

5.2.26.14. Deve fornecer integração com agentes de antivírus, obtendo informações de reputação dos arquivos, para impedir dinamicamente que aplicativos potencialmente perigosos acessem arquivos confidenciais em endpoints.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.2.26.15. A Solução deve possuir monitoramento, para no mínimo os seguintes aplicativos:

- 5.2.26.15.1. Adobe Flash Player;
- 5.2.26.15.2. Adobe Reader;
- 5.2.26.15.3. AIM;
- 5.2.26.15.4. Apple iTunes;
- 5.2.26.15.5. Box;
- 5.2.26.15.6. Box Edit;
- 5.2.26.15.7. Bs Recoder GOLD;
- 5.2.26.15.8. BsCLIP;
- 5.2.26.15.9. BurnAware;
- 5.2.26.15.10. Cisco Jabber;
- 5.2.26.15.11. CommandBurner;
- 5.2.26.15.12. CopyToDVD;
- 5.2.26.15.13. CopyToDVD DVD;
- 5.2.26.15.14. Creator10;
- 5.2.26.15.15. DeepBurner;
- 5.2.26.15.16. Dropbox;
- 5.2.26.15.17. Google Chrome;
- 5.2.26.15.18. Google Drive;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.2.26.15.19.	Google Talk;
5.2.26.15.20.	iCloud;
5.2.26.15.21.	Java (TM) Web Launcher;
5.2.26.15.22.	Lotus Notes;
5.2.26.15.23.	Microsoft Edge;
5.2.26.15.24.	Microsoft Internet Explorer;
5.2.26.15.25.	Microsoft Lync;
5.2.26.15.26.	Microsoft Office Excel;
5.2.26.15.27.	Microsoft Office Powerpoint;
5.2.26.15.28.	Microsoft Office Word;
5.2.26.15.29.	Microsoft OneDrive;
5.2.26.15.30.	Microsoft Outlook;
5.2.26.15.31.	Microsoft PowerShell;
5.2.26.15.32.	Microsoft SkyDrive;
5.2.26.15.33.	Microsoft Windows Bluetooth;
5.2.26.15.34.	Mozilla Firefox;
5.2.26.15.35.	Nero;
5.2.26.15.36.	NeroStartSmart;
5.2.26.15.37.	Roxio;
5.2.26.15.38.	Safari;



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.26.15.39. SilentNight Microburner;
- 5.2.26.15.40. Skype;
- 5.2.26.15.41. WebEx Communication Module.
- 5.2.26.16. A solução deve permitir a inclusão de qualquer aplicativo existente que não venha cadastrado por default.
- 5.2.26.17. Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceções de políticas para esses dispositivos.
- 5.2.26.18. O agente deverá suportar, no mínimo, Windows 7 (32 e 64 bits), Windows 2008 R2 Enterprise (64bit), Windows 10, Windows Server 2012, Windows Server 2016 e Apple MacOS.
- 5.2.26.19. Todas as funções devem ser executadas por um único agente.
- 5.2.26.20. Permitir a partir do console central, a reinicialização e desligamento do host gerenciado, assim como a ativação e desativação do agente.
- 5.2.26.21. Possuir mecanismo que reinicie o agente caso o usuário tente interromper o serviço.
- 5.2.26.22. Possuir proteção contra desinstalação do agente.
- 5.2.26.23. O agente não deve ser exibido na lista "Adicionar ou remover programas".
- 5.2.26.24. Capacidade de apresentar as mensagens de notificações em português.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.26.25. Possuir a capacidade de envio de notificação automática, por e-mail, para o usuário e administrador durante a ocorrência de um incidente.
- 5.2.26.26. Possuir a capacidade de gerenciamento da saúde dos agentes.
- 5.2.26.27. Possuir ferramenta para recuperação de agentes com mau funcionamento por meio de scripts, para completa remoção e permitir que seja feita uma nova instalação padrão remota e automatizada dos agentes. A operação não deixará na console quaisquer resquícios como licenças perdidas, duplicadas, lista de clientes pendentes, etc.
- 5.2.26.28. Deve permitir a distribuição do agente através de GPO ou por ferramenta de terceiros.
- 5.2.26.29. Deve ser integrável com ferramentas de criptografia, a fim de criptografar apenas o conteúdo confidencial enviado para um dispositivo USB.
- 5.2.26.30. Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em “pop-up”, escolhendo opções de justificativa configuráveis pelo administrador da ferramenta, reportando para a console de gerenciamento, categorizadas no console para posterior geração de relatórios por categoria de justificativa.
- 5.2.26.31. Deve permitir definir limites em percentual da CPU, disco, e a largura de banda utilizada pelo agente.
- 5.2.26.32. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial.
- 5.2.26.33. A varredura de informações sensíveis executadas nos agentes, deve possibilitar, no mínimo:



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

- 5.2.26.33.1. Iniciar, parar e pausar as verificações;
- 5.2.26.33.2. Monitorar o status à medida que as verificações são executadas;
- 5.2.26.33.3. Classificar e filtrar alvos para facilitar o gerenciamento.
- 5.2.26.34. Permitir a revisão do status das verificações para, no mínimo, os seguintes estados:
 - 5.2.26.34.1. Concluído - indica que todos os agentes DLP concluíram a verificação com êxito;
 - 5.2.26.34.2. Tempo limite - indica que um ou mais agentes DLP incluídos na varredura não se reportaram ao Endpoint Server com um status de varredura dentro de um período configurado.
 - 5.2.26.34.3. Parado - indica que o administrador interrompeu a verificação.
 - 5.2.26.34.4. Em execução - indica que pelo menos um agente DLP começou a executar a verificação.
 - 5.2.26.34.5. Pronto - indica que uma verificação do Endpoint Discover Target está configurada e pronta para execução.
 - 5.2.26.34.6. Em fila - indica que o servidor de gerenciamento de agentes está inoperante e a varredura continua no estado em fila até que esse servidor esteja disponível.
- 5.2.26.35. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados.
- 5.2.26.36. Deve ter a capacidade de monitorar e bloquear dados não permitidos apenas as páginas que são enviadas para impressão ou o documento como um todo.



Ministério da Saúde
Secretaria de Informação e Saúde Digital
Departamento de Informação e Informática do Sistema Único de Saúde
Coordenação de Monitoramento e Avaliação de Contratos de Tecnologia da Informação e Comunicação

5.2.26.37. O agente deve funcionar em modo oculto ao usuário, sem que sua presença seja notada e mesmo assim permitir que avisos e pop-ups sejam entregues aos usuários, quando requerido.

5.2.27. Módulo de rede

5.2.27.1. Permitir a monitoração e bloqueio do e-mail corporativo, evitando que e-mails com dados sigilosos sejam enviados para fora da organização, inclusive em smartphones e tablets.

5.2.27.2. Possibilidade de colocar mensagens de correio eletrônico em quarentena para análise.

5.2.27.3. Permitir a monitoração e bloqueio de tráfego WEB, evitando que dados sigilosos saiam da organização por este canal, inclusive em smartphones e tablets.

5.2.27.4. Capacidade de monitorar e bloquear o tráfego de informações sensíveis em posts de redes sociais.

5.2.27.5. Permitir a monitoração de qualquer serviço baseado em TCP: SMTP incluindo seus anexos, HTTP incluindo arquivos de upload, FTP ativo e passivo.

5.2.27.6. Capacidade de monitorar o vazamento de dados por meio de softwares de Mensagens Instantâneas.

5.2.27.7. Permitir a classificação dos protocolos, mesmo quando executados em portas que não são padrão.

5.2.27.8. Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP e remetente e destinatário de e-mail.