TERMO DE REFERÊNCIA

OBJETO: Suíte de Aplicativo de Segurança (antivírus, antimalware, proteção contra Ransomware) , com módulos de gerenciamento.

DESCRIÇÃO TÉCNICA

1. Módulo de Gerenciamento

Módulo para gerenciamento da solução antivírus:

- A Console de Gerenciamento pode ser disponibilizada em um ambiente em nuvem hospedado pela contratada, com acesso à console via WEB (navegador), através de uma conexão segura e criptografada HTTPS;
- Suportar o gerenciamento de máquinas da rede de dados a partir de um único servidor;
- Permitir o gerenciamento do servidor a partir de console em outra máquina;
- Permitir a instalação do antivírus e demais funcionalidades (firewall, controle de aplicativos, controle de dados, filtro de navegação web e etc) remotamente nos clientes, a partir de uma única console;
- Permitir a alteração das configurações dos antivírus nos clientes de maneira remota e através de regras aplicáveis a uma máquina ou um grupo de máquinas;
- Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local;
- Permitir a criação de tarefas remotamente de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do sistema operacional ou no logon na rede;
- Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado, podendo ele ser local ou em nuvem;
- Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede;
- Permitir diferentes níveis de administração do console de gerenciamento;
- Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;
- Criação de grupos de máquinas baseadas em regras definidas por grupos de máquinas ou usuários;
- Forçar a configuração determinada no console para os clientes:
- A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação SSL.
- Forçar a instalação remota do software antivírus nos clientes:
- Geração de relatórios gráficos;
- Customização dos relatórios gerados;
- Exportação dos relatórios para, no mínimo, um dos seguintes formatos: HTML, XLS, DOC, TXT
- Geração de relatórios que contenham as seguintes informações:
  - Máquinas com a lista de definições de vírus desatualizada;
  - Qual a versão do software instalado em cada máquina;
  - Os vírus que mais foram detectados;
  - As máquinas que mais sofreram infecções em um determinado período de tempo;
  - Os usuários que mais sofreram infecções em um determinado período de tempo;
- Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local, VPN;

- Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;
- Suportar o gerenciamento de no mínimo 1.000 máquinas a partir de um único servidor, sendo ele local ou em nuvem;
- Console de gerenciamento unificada para computadores, servidores e dispositivos móveis, isto é, através de uma única interface, gerenciar a solução em qualquer dispositivo instalado, com aplicações de políticas, controle de atualizações e geração de relatórios;
- Permitir o gerenciamento centralizado da instalação nos clientes a partir de uma única console, com possibilidade de Sincronização com o Active Directory (o active directory não pode ser obrigatório para uso desse recurso), e verificar se possui antivírus instalado;
- Permitir a criação de grupos de máquinas com definições de políticas próprias, isto é, com definições diferentes das demais máquinas da rede e sem a interferência de políticas de outros grupos;
- Permitir a definição, por grupo de máquinas, de horário para a atualização das definições de vírus;
- Notificação automática, por e-mail, ao administrador em caso de epidemia de malwares;

2. Módulo de antimalware (antivírus)

2.1 Sistemas Operacionais Suportados

- Suporte total a todas as versões do Windows Server, no mínimo Windows Server 2008;
- Suporte total a versões do Windows, no mínimo Windows 8.1;

2.2 Características mínimas para computadores (Desktop, Notebook)

- Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções:
    - Negar acesso ao arquivo infectado e prosseguir;
    - Limpar o arquivo;
    - Apagar arquivo infectado;
    - Mover o arquivo infectado para área de segurança (quarentena).
- Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;
- Gerar notificações de eventos de vírus através de alerta na rede;
- Capacidade de instalação remota, através de console, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- Rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados;
- Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem como opção de bloqueio da comunicação via rede;
- Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;
- Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável;
- Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo;
- Detecção de programas maliciosos como programas de propaganda, ferramentas como password crackers, etc;

- Detecção por intermédio de assinaturas, heurísticas, por comportamento e reputação de arquivos.
- Rastreamento manual com interface Windows, customizável, com opção de limpeza;
- Programação de atualizações automáticas das listas de definições de vírus, a partir de locais predefinidos da rede, ou de site Internet, com frequência (no mínimo diária) e horários definidos pelo usuário;
  - Permitir atualização incremental da lista de definições de vírus;
  - Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus;
- Programação de rastreamentos e monitoramento (sob demanda e "on-line/real-time") –automáticos do sistema com as seguintes opções:
  - Escopo: todos os drives locais, drivers específicos ou pastas específicas;
  - Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear ou mover automaticamente para área de segurança (quarentena);
  - Frequência: horária, diária, semanal e mensal;
  - Exclusões: pastas, arquivos e processos que não devem ser rastreados;
  - Definição do usuário ou conta de máquina a ser utilizado durante a verificação.
- Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;
- Permitir proteção das configurações através de senha;
- Rastreamento de arquivos compactados tipo .zip, .rar, .7zip, .gz, entre outros.
- Atualizar a partir de um servidor web externo, servidor web interno e através de servidor de arquivos/pastas compartilhadas;
- Oferecer suporte ao uso de repositórios para atualização do produto e vacinas;
- Possibilitar executar varredura em tempo real: de arquivos (gravação e/ou leitura), de processos em memória;
- Possibilitar executar varredura manual com interface Windows, configurável, com opção de limpeza;
- Possibilitar rastreamento por linha-de-comando, parametrizável, com opção de limpeza;
- Capacidade de detectar vírus de macros;
- Detecção e remoção de programas maliciosos como spyware, adware, trojans, etc.
- Solução única para proteção, em tempo real, contra malwares em geral, incluindo vírus, trojans, adware, rootkits, spywares, ransoware, phishing, spam, worms, aplicações potencialmente indesejadas e outros tipos de códigos maliciosos com opção de customização como, por exemplo, do tipo de varredura;
- Possuir processo para a desinstalação automática do sistema antivírus existente no equipamento;
- O programa deverá enviar os arquivos em quarentena para análise da equipe responsável por criar vacinas do fabricante;
- Gerenciamento integrado à console de gerência da solução;
- 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;
- Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação ou arquivo;
- Manipuladores de agentes permitem o gerenciamento de sistemas de terminais mesmo quando desconectados da rede, ou no Domínio, com gerenciamento de nível de privilégio através de senha;
- Proteção contra desinstalação não autorizada do produto e proteção contra remoção do módulo residente em memória através de senhas distintas;
- "Roll-back" da biblioteca de vírus;

- Instalação sem reinicialização da estação de trabalho;
- Em caso de parada na proteção, o serviço de antivírus deve ser capaz de reiniciar automaticamente após um período definido na política pelo administrador, sem a necessidade de reinicialização da estação;
- Permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias. Com possibilidade de: alerta, bloqueio, lista de exceção (White List/ Black List);

2.3 Características mínimas para Servidores

- Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções:
    - Negar acesso ao arquivo infectado e prosseguir;
    - Limpar o arquivo;
    - Apagar arquivo infectado;
    - Mover o arquivo infectado para área de segurança (quarentena).
- Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;
- Gerar notificações de eventos de vírus através de alerta na rede;
- Capacidade de instalação remota, através de console, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- Rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados;
- Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem como opção de bloqueio da comunicação via rede;
- Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;
- Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável;
- Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo;
- Detecção de programas maliciosos como programas de propaganda, ferramentas como password crackers, etc;
- Detecção por intermédio de assinaturas, heurísticas, por comportamento e reputação de arquivos.
- Rastreamento manual com interface Windows, customizável, com opção de limpeza;
- Programação de atualizações automáticas das listas de definições de vírus, a partir de locais predefinidos da rede, ou de site Internet, com freqüência (no mínimo diária) e horários definidos pelo usuário;
    - Permitir atualização incremental da lista de definições de vírus;
    - Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus;
- Programação de rastreamentos e monitoramento (sob demanda e "on-line/real-time") –automáticos do sistema com as seguintes opções:
    - Escopo: todos os drives locais, drives específicos ou pastas específicas;
    - Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear ou mover automaticamente para área de segurança (quarentena);
    - Frequência: horária, diária, semanal e mensal;
    - Exclusões: pastas, arquivos e processos que não devem ser rastreados;
    - Definição do usuário ou conta de máquina a ser utilizado durante a verificação.

- Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;
- Permitir proteção das configurações através de senha;
- Rastreamento de arquivos compactados tipo .zip, .rar, .7zip, .gz, entre outros.
- Atualizar a partir de um servidor web externo, servidor web interno e através de servidor de arquivos/pastas compartilhadas;
- Oferecer suporte ao uso de repositórios para atualização do produto e vacinas;
- Possibilitar executar varredura em tempo real: de arquivos (gravação e/ou leitura), de processos em memória;
- Possibilitar executar varredura manual com interface Windows, configurável, com opção de limpeza;
- Possibilitar rastreamento por linha-de-comando, parametrizável, com opção de limpeza;
- Capacidade de detectar vírus de macros;
- Detecção e remoção de programas maliciosos como spyware, adware, trojans, etc.
- Solução única para proteção, em tempo real, contra malwares em geral, incluindo vírus, trojans, adware, rootkits, spywares, ransoware, phishing, spam, worms, aplicações potencialmente indesejadas e outros tipos de códigos maliciosos com opção de customização como, por exemplo, do tipo de varredura;
- Possuir processo para a desinstalação automática do sistema antivírus existente no equipamento;
- O programa deverá enviar os arquivos em quarentena para análise da equipe responsável por criar vacinas do fabricante;
- Gerenciamento integrado à console de gerência da solução;
- 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;
- Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação ou arquivo;
- Manipuladores de agentes permitem o gerenciamento de sistemas de terminais mesmo quando desconectados da rede, ou no Domínio, com gerenciamento de nível de privilégio através de senha;
- Proteção contra desinstalação não autorizada do produto e proteção contra remoção do módulo residente em memória através de senhas distintas;
- "Roll-back" da biblioteca de vírus;
- Instalação sem reinicialização da estação de trabalho;
- Possuir capacidade para bloquear acesso às pastas compartilhadas na estação de trabalho, em caso de epidemia, e após o término dessa, restaurar as configurações originais;
- Em caso de parada na proteção, o serviço de antivírus deve ser capaz de reiniciar automaticamente após um período definido na política pelo administrador, sem a necessidade de reinicialização da estação;
- Permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias. Com possibilidade de: alerta, bloqueio, lista de exceção (White List/ Black List);

2.4. Controle de Dispositivo

- Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução/bloqueio do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido.
- Os dispositivos controlados deverão ser no mínimo os descritos a seguir:
    - Armazenamento removível (ex. USB ou HD Externo, pen drives, cartões de memória, etc).
    - Armazenamento removível seguro (ex. tokens ou smart cards).

- Dispositivos de CD e DVD.
- Dispositivos de infravermelho.
- Dispositivos Wi-Fi.
- Interfaces de Bluetooth.
- Modems de acesso via rede celular (3G/4G/etc).
- Dispositivos MTP/PTP (smartphones, câmeras digitais, etc.)

2.5. Controle de acesso Web

- Deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados;
- As listas branca e negra deverão permitir a inserção de nomes de domínio e endereços IP;
- Permitir o bloqueio de acesso à web sites via HTTP e HTTPS;
- Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para o console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

2.6. Proteção contra Ransomware

- Dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
- Capacidade de remediação da ação de criptografia maliciosa dos ransomwares;
- Capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;
- Capacidade de rollback de arquivos que foram criptografados;

3. Suporte Técnico e manutenção oferecidos pelo fabricante do software

- A contratada, caso não seja o próprio fabricante, deve possuir contrato de suporte técnico para atendimento ilimitado junto ao fabricante do produto oferecido, a fim de garantir o serviço prestado;
- Serviços de suporte especializado em segurança da informação para instalação, configuração e suporte ao funcionamento da solução antimalware. O suporte será em regime de, no mínimo, 8 x 5 (dias úteis, horário comercial);
- Suporte técnico telefônico no idioma Português Brasil direto com o fabricante do produto;
- Com direito a atualizações de assinaturas e software, e suporte técnico ilimitado (via e-mail e telefone), sem custo adicional, pelo período de contratação do software antivírus a contar do recebimento das licenças de uso pela Prefeitura;
- O telefonema para o suporte técnico remoto deverá ser atendido por técnico devidamente capacitado para interpretar e, eventualmente resolver ou contatar os recursos necessários para a resolução do problema em regime de, no mínimo, 8 x 5 (dias úteis, horário comercial).
- Fornecimento de vacina para novos vírus no prazo máximo de 48 horas a partir do registro de ocorrência feito pela FUNDHAS.
- O tempo máximo de 3 (três) dias úteis para resolução de suporte técnico, quando não para vacina.

VIGÊNCIA CONTRATO: 24 meses
Licença de uso para 950 Computadores