PROPOSTA DE

LICENCIAMENTO

DE SOFTWARE

BitDefender

Lnx-IT Informação e Tecnologia
Av. Venâncio Aires, 1137 – Bairro: Bom fim – Porto Alegre – RS – CEP: 90040.193 – Fone: +55 51 3331.1446
E-mail: comercial@lnx-it.inf.br Website: http://www.lnx-it.inf.br

A **Lnx-IT** é uma empresa, fundada no ano de 2003, localizada em Porto Alegre, no Rio Grande do Sul, especializada na distribuição e comercialização de soluções em segurança da informação.

Trabalhamos com grandes fabricantes internacionais de expressão, tais como **BitDefender e Acronis.**

Nossa equipe é certificada diretamente pelos fabricantes das soluções representadas e possui uma vasta experiência em segurança da informação. Oferecemos aos nossos clientes serviços de suporte técnico e de treinamento com alto padrão de qualidade nas soluções comercializadas.

ÁREAS DE ATUAÇÃO:

Revendedor autorizado de produtos **BitDefender**.
Revendedor autorizado de Produtos **Acronis**.

Lnx-IT Informação e Tecnologia
Av. Venâncio Aires, 1137 – Bairro: Bom fim – Porto Alegre – RS – CEP: 90040.193 – Fone: +55 51 3331.1446
E-mail: comercial@lnx-it.inf.br Website: http://www.lnx-it.inf.br

PROPOSTA COMERCIAL

Porto Alegre, 06 de dezembro de 2024.

Empresa: **PREFEITURA MUNICIPAL DE CANELA**

Produto	*Users*	*Vlr.Unit.*	*Total*
BitDefender GravityZone Business Security Enterprise			
- Estações de trabalho Windows/Mac/Linux			
- Servidores Windows			
- EDR			
Licenciamento de 3 anos + 1 ano (Totalizando 48 meses			
de cobertura)	832	R$ 47,00	**R$ 39.104,00**
		TOTAL	**R$ 39.104,00**

Valores em Real (R$), válidos até: Conforme Edital de Pregão Eletrônico 18/2024 Pref. Mun. Canela. 60 dias

Forma de Pagamento

Conforme Edital de Pregão Eletrônico 18/2024 Pref. Mun. Canela e suas atas e correções

Prazo para entrega

Imediato via download – chaves em até 5 dias úteis.

OBS:

Licenças válidas pelo período conforme apresentado acima.

Valores válidos apenas para a condição acima.

Importante: Até 35% do total das licenças poderão ser destinadas a Servidores.

Carlos Bestetti
comercial@lnx-it.inf.br

Produto: BITDEFENDER GRAVITYZONE BUSINESS SECURITY ENTERPRISE

1. Segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.
1.1. Possui console central única de gerenciamento. As configurações do Antivírus, AntiSpyware, Firewall, Detecção de intrusão controle de Dispositivos e Controle de Aplicações são realizadas através da mesma console;
1.2. Capacidade de remoção do software de antivírus já instalado e instalado de forma remota pela console de gerenciamento;
1.3. Possui os seguintes módulos:
1.4. Console de Gerenciamento fornecendo funcionalidades de gestão;
1.5. Módulos para estações físicas, laptops e servidores;
1.6. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;
1.7. Utiliza o conceito de heurística;
1.8. Oferece tecnologia que explora vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);
1.9. Oferece tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;
1.10. Oferece inventário de softwares;
1.11. Oferece tecnologia onde a solução testa arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;
1.12. Oferece proteção por base de assinaturas;

2. Console De Gerenciamento
2.1. Instalação e configuração
2.2. Fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem (Cloud).
2.3. Suporta os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; XenDesktop, VDI-ina-Box;
2.4. Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;
2.5. Fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;
2.6. Permite instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;
2.7. Mecanismo de varredura disponível para download separadamente;
2.8. Permite a inclusão de um modulo de balanceamento para casos em vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);
2.9.Totalmente em português.

3. Características Gerais
3.1. Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem atualizados;
3.2. Permite que o administrador escolha qual o pacote será atualizado;
3.3. Notificações destacadas como item não lido, enviar e-mail para o administrador;
3.4. Notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware,
3.5. Painel para Monitoramento baseado em "portlets" configuráveis com as seguintes especificações:

Nome; Tipo de relatório; Alvo do relatório;
3.6. Disponibiliza "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais;
3.7. Inventário da Rede
3.8. Possui as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;
3.9. Possui possibilidade de definição de sincronização com o Active Directory em horas;
3.10. Compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;
3.11. Descoberta de rede para máquinas em grupo de trabalho;
3.12. Busca em tempo real com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;
3.13. Possibilita a instalação remota e desinstalação remota do antivírus;
3.14. Possibilita a configuração de pacotes de instalação do produto de antivírus;
3.15. Tarefas remotas e configuráveis de Scan;
3.16. Tarefa de reinicialização remota de estação ou servidor;
3.17. Assinar políticas para no mínimo os níveis: Computador, Máquina Virtual ou Possuir a propriedade detalhada de objetos gerenciados para: Nome, IP, Sistema Operacional, Grupo, Política Assinada, ultimo status de malware;

4. Políticas
4.1. Modelo único para todos os equipamentos, seja físico ou virtual;
4.2. Cada serviço de segurança tem seu modelo configurável de política com opções específicas de ativar/desativar;
4.3. Configuração das funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

5. Relatórios
5.1. Relatório para cada serviço de segurança;
5.2. Facilidade de usar e visualização simplificada;
5.3. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;
5.4. Filtros de agendamento de relatórios;
5.5. Arquivo com todas as instâncias de relatório agendados;
5.6. Exporta o relatório nos formatos .pdf e/ou .csv;
5.7. Oferece possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.

6. Quarentena
6.1. Restauração remota, com configuração de localidade e deleção;
6.2. Criação e exclusão para arquivos restaurados;

7. Usuários
7.1. Administração baseada em regras;
7.2. Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador - Gerente dos componentes da solução, Administrador de rede - Gerente dos serviços de segurança;
7.3. Relatório - Monitora e cria relatórios;
7.4. Possível customizar um tipo de usuário;

7.5. Permite a integração do usuário com o Active Directory para autenticação da console de gerenciamento;
7.6. Logs de utilização;
7.7. Registrar as ações do usuário na console de gerenciamento;
7.8. Detalhar cada ação do usuário;
7.9. Permitir busca complexa baseada em ações do usuário, intervalos de tempo;

8. Certificado de Segurança
8.1. Prove o acesso via HTTPS;
8.2. Permiter a importação de certificados digitais;
8.3. O gerenciamento e a comunicação com dispositivos móveis é feito de forma segura utilizando certificados digitais;

9. Proteção Para Estações De Trabalho E Servidores Físicos
9.1. Permite a configuração do scan do antivírus do cliente como: Scan local, Scan Hibrido, Scan Central;
9.2. Permite a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso a internet; (Windows Workstation), Instalar o antivírus sem o módulo de firewall; (Windows Workstation)
9.3. Suporta no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 10 32 e 64 Bits, Windows 7 32 e 64Bits.
9.4. Suporta no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2012R2, Windows Server 2012, Windows Server 2008 R2.
9.5.Suporta no mínimo os seguintes sistemas operacionais para distribuição Linux: Red Hat Enterprise Linux, Cent OS 5.6 ou superior, Ubuntu 10.04 LTS ou superior, SUSE Linux Enterprise Sever 11 ou superior, OpenSUSE 11 ou superior, Fedora 15 ou superior, Debian 5.0 ou superior;

10. Gerenciamento e Instalação Remota
10.1. Permite ao administrador customizar a instalação;
10.2. A instalação executa das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerencia web;
10.3. Relatório com as estações instaladas e as faltantes da instalação;
10.4. A console de gerenciamento inclui informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: Nome, IP, Sistema Operacional, Política Aplicada;
10.5. Através da console, o administrador poderá enviar uma política única para configurar o antivírus;
10.6. A console de gerenciamento inclui sessão de log com as seguintes informações: Login, Edição, Criação, Log-out, com capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits, permitindo ao administrador criar grupos e subgrupos para mover as estações de trabalho;
10.7. O agente utilizado na sincronização é incluído no cliente do antivírus e não é necessário à distribuição em um agente separado;

11. Proteção Para Estações E Servidores Virtuais
11.1. Proteção de antivírus dedicado para ambientes virtuais;
11.2. Disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;
11.3. A console de gerenciamento central da solução tem a possibilidade de integrar com múltiplos vCenters VMWare;

11.4. Protege em tempo real e agendado as máquinas virtuais Linux;
11.5. O produto oferece agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft Hyper-V, Red Hat Virtualization, Oracle KVM, KVM;

12. Funções Gerais
12.1. Métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;
12.2. Reporta o estado atual das VMs no mínimo, protegida/desprotegida;

13. Requisitos Mínimos suportados pelo Sistema.
13.1. Plataformas de Virtualização: VMware vSphere ESX 5.0 ou superior, VMware vCenter Server 4.1 ou superior, VMWare Tools 8.6.0 , Citrix XenDesktop 5.0 ou superior, Xen Server 5.5 ou superior, Citrix VDI-in-a-Box 5, Microsoft Hyper-V Server 2008 R2, 2012, Oracle VM 3.0, Red Hat Enterprise Virtualization 3.0
13.2. Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, Windows 10
13.3. Sistemas Operacionais Servidores: Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Linux Red Hat Enterprise, CentOS 5.6 ou superior, Ubuntu 10.04 LTS ou superior, SUSE Linux Enterprise Server 11 ou superior, OpenSUSE 11 ou superior, Fedora 15 ou superior, Debian 5.0 ou superior.

14. Componentes e Funcionalidade do Antivírus Geral
14.1. Scan em tempo real automático;
14.2. Configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;
14.3. Escaneamento de comportamento heurístico;
14.4. Escaneamento em tempo real, qualquer informação localizada em mídias de armazenamento como: CD/DVD, Discos Externos, Pen-Drivers, permite a escolha e configuração de pastas a serem escaneadas;
14.5. Para melhor proteção, o antivírus tem no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada em Heurística, Baseada em monitoramento contínuo de processos;
14.6. Capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;
14.7. O cliente do antivírus possui módulo de Antiphishing com opção de verificar links pesquisados com os sites de pesquisas Search Advisor na Estações de trabalho;
14.8. Possui módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;
14.9. O módulo de firewall permite configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;
14.10. Permite o envio automático de arquivos da quarentena para o laboratório de vírus;
14.11. Remoção automática de arquivos antigos, pré-definidos pelo administrador;
14.12. Permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
14.13. Cria de forma automática exclusão para arquivos restaurados da quarentena;
14.14. Permite escanear a quarentena após a atualização das atualizações de assinaturas;

15. Controle de Usuário
15.1. Possui módulo de controle de usuário integrando com as seguintes características: Bloqueio de acesso a internet, Bloqueio de acesso a aplicações definidas pelo administrador;

16. Controle do Dispositivo

16.1. Instalação do módulo de controle de dispositivos através da console de gerenciamento;
16.2. Através do módulo de controle de dispositivo é possível controlar: Bluetooth, CDROM/DVDROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;
16.3. Permite regras de definição de bloqueio/desbloqueio;
16.4. Permite regras de exclusão;

17. Atualização
17.1. Após a atualização o administrador tem a capacidade de adiar uma reinicialização;
17.2. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
17.3. Permite atualizações de assinatura de hora em hora;
17.4. Permite motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

18. Proteção para caixa de e-mail:
18.1. Fornece proteção para ambiente Exchange
18.2. Oferece tecnologia para proteção contra spam;
18.3. Oferece análise comportamental e proteção para zero-day;
18.4. Oferece proteção contra vírus e tentativas de phishing;

19. Criptografia
19.1. Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de Criptografia presente na mesma Console do Antivirus (ADQUIRIDO SEPARADAMENTE).
19.2. Utiliza quando necessário serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);
19.3. Solicita autenticação quando iniciado o sistema operacional do equipamento;
19.4. Compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra

20. **Proteção Avançada NGAV**

20.1. Detecta e bloqueia todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como elimina malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detecta e bloqueia ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, sendo detectados e bloqueados antes de serem executados.
20.2. Detecta, para, bloqueia e interrompe malwares sem arquivos.
20.3. Para os ataques com base em macros e scripts. Analisa scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adiciona técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.
20.4. Reparo e resposta automatizada a ameaças
20.5. Quando uma ameaça é detectada, a ferramenta neutraliza imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mau intencionadas. Compartilha as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes.

20.6. Obtem visibilidade e contexto sobre ameaças identificando e reportando atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.
20.7. Opera com um único agente e console integrados bem como personaliza automaticamente o pacote de instalação e minimiza o carregamento do agente.
20.8. Nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também detecta técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web.
Permite que os administradores de segurança ajustem a proteção para combater os riscos.

21. Machine Learning
21.1. As técnicas de Machine Learning utilizam modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados.
21.2. A ferramenta de Machine Learning é baseada em características estáticas e dinâmicas, e se treinam continuamente com bilhões de amostras de arquivos legítimos e maliciosas melhorando significativamente a efetividade da detecção de malware e minimiza os falsos positivos, ações evasivas e conexões a centros de comando e controle.

22. Sandbox
22.1. Sandbox integrado nos terminais que analisa arquivos suspeitos em profundidade, aciona ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas. O Sandbox é integrado com o agente e encaminha automaticamente os arquivos suspeitos para análise. Ao retornar uma análise com resultado "malicioso", o Sandbox bloqueia automaticamente o arquivo malicioso em sistemas em toda rede imediatamente. O recurso de envio automático permite que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecer um contexto claro das ameaças e ajudar a entender o comportamento delas.

23. Antiexploit Avançado
23.1. Contem antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja: Flash ou Java). Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (return oriented programming), etc.

24. Inspetor de processo
24.1. O Inspetor de Processos opera em um modo de confiança zero, monitorando continuamente todos os processos em execução no sistema operacional. Procura atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaço de outro processo (seqüestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem etc. Toma as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Detecta de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.

***25.*Detecção e Resposta - EDR**

25.1. Realiza a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplica funcionalidades de XEDR para detectar ataques avançados em vários terminais em infraestruturas híbridas (estações de trabalho, servidores ou containers, executando vários sistemas operativos)

25.2. Analisa continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus terminais, permitindo ações automáticas de fortalecimento. Identifica ações e comportamentos dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login em sites, gerenciamento de senhas inadequado, uso de USBs comprometidos, infecções recorrentes, etc.