DEFINIÇÃO DO OBJETO

Contratação de empresa (Revenda) para fornecimento de licenças de software de antivírus e suporte pelo período de 12 meses.

1. ESPECIFICAÇÕES GERAIS DO OBJETO

ITEM	DESCRIÇÃO	VALOR	QTDE	VALOR TOTAL
01	Aquisição de Licenças e Atualização do Antivírus	R$	450	R$

Contratação de empresa (Revenda) para fornecimento de licenças de software de antivírus e suporte pelo período de 12 meses

1. Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.
1.1. Possuir console central única de gerenciamento. As configurações do Antivírus, AntiSpyware, Firewall, Detecção
de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;
1.2. O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;
1.3.O produto deverá possuir no mínimo 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. Utilizar o conceito de heurística;
1.8. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);
1.9. Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;
1.10. Oferecer inventário de softwares;
1.11 .Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;
1.12. Oferecer proteção por base de assinaturas;

2. Console De Gerenciamento
2.1. Instalação e configuração
2.2. Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem (Cloud).
2.3. Deverá suportar no mínimos os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; XenDesktop, VDI-ina-Box;

Rua Siqueira Campos, S-64 – Centro – CEP 17280-000 – Pederneiras/SP
Tel.: (14) 3283 9570 – Fax: (14) 3284 1764 – www.pederneiras.sp.gov.br

2.4. Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;
2.5. Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;
2.6. Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;
2.7. O mecanismo de varredura deverá estar disponível para download separadamente;
2.8. A solução deverá permitir 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. Deve ser 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. Permitir que o administrador escolha qual o pacote será atualizado;
3.3. As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;
3.4. No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware,
3.5. Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações: Nome; Tipo de relatório; Alvo do relatório;
3.6. Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;
3.7. Inventário da Rede
3.8. Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;
3.9. Possuir a possibilidade de definição de sincronização com o Active Directory em horas;
3.10. Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;
3.11. Descoberta de rede para máquinas em grupo de trabalho;
3.12. Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;
3.13. Possibilitar a instalação remota e desinstalação remota do antivírus;
3.14. Possibilitar a configuração de pacotes de instalação do produto de antivírus;
3.15. Possuir tarefas remotas e configuráveis de Scan;
3.16. Possuir 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 deve ter seu modelo configurável de política com opções específicas de ativar/desativar;
4.3. Deverá configurar as 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;

Rua Siqueira Campos, S-64 – Centro – CEP 17280-000 – Pederneiras/SP
Tel.: (14) 3283 9570 – Fax: (14) 3284 1764 – www.pederneiras.sp.gov.br

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. Exportar o relatório nos formatos .pdf e/ou .csv;
5.7. Oferecer 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. Deverá ser possível customizar um tipo de usuário;
7.5. Deverá permitir 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. Deverá prover o acesso via HTTPS;
8.2. Deverá permitir a importação de certificados digitais;
8.3. O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais;

9. Proteção Para Estações De Trabalho E Servidores Físicos
9.1. Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Hibrido, Scan Central;
9.2. Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso à internet; (Windows Workstation), Instalar o antivírus sem o módulo de firewall; (Windows Workstation)
9.3. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 11 32 e 64Bits, Windows 10 32 e 64Bits.
9.4. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2019, Windows Server 2012R2, Windows Server 2008 R2.

Rua Siqueira Campos, S-64 – Centro – CEP 17280-000 – Pederneiras/SP
Tel.: (14) 3283 9570 – Fax: (14) 3284 1764 – www.pederneiras.sp.gov.br

9.5. Deverá suportar 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. Deverá permitir ao administrador customizar a instalação;
10.2. A instalação deverá ser possível executar com no mínimo das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerencia web;
10.3. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;
10.4 .A console de gerenciamento deve incluir 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 deverá incluir sessão de log com as seguintes informações: Login, Edição, Criação, Log-out, ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits, deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;
10.7. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser 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. Deverá ter a 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 deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;
11.4. Deverá proteger em tempo real e agendado as máquinas virtuais Linux;
11.5. O produto deverá oferecer agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft Hyper-V, Red Hat Virtualization, Oracle KVM, KVM;

12. Funções Gerais
12.1. Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;
12.2. Deverá reportar 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 10, Windows 11
13.3. Sistemas Operacionais Servidores: Windows Server 2019 , Windows Server 2012R2, Windows Server 2012, Linux Red Hat Enterprise, CentOS 5.6 ou superior, Ubuntu 16.04 LTS ou

Rua Siqueira Campos, S-64 – Centro – CEP 17280-000 – Pederneiras/SP
Tel.: (14) 3283 9570 – Fax: (14) 3284 1764 – www.pederneiras.sp.gov.br

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. Deverá fazer scan em tempo real automático;
14.2. Deverá ser 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. Deverá escanear em tempo real qualquer informação localizadas em mídias de armazenamento como: CD/DVD, Discos Externos, Pen-Drivers, Deverá permitir a escolha e configuração de pastas a serem escaneada;
14.5. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada em Heurística, Baseada em monitoramento contínuo de processos;
14.6. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;
14.7. O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor na Estações de trabalho;
14.8. Deverá possuir 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 deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;
14.10. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;
14.11. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
14.12. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
14.13. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
14.14. Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;

15. Controle de Usuário

15.1. Deverá ter 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. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
16.2. Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CDROM/DVDROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;
16.3. Deverá permitir regras de definição de bloqueio/desbloqueio;
16.4. Deverá permitir regras de exclusão;

17. Atualização

17.1. Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;
17.2. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
17.3. Permitir atualizações de assinatura de hora em hora;

Rua Siqueira Campos, S-64 – Centro – CEP 17280-000 – Pederneiras/SP
Tel.: (14) 3283 9570 – Fax: (14) 3284 1764 – www.pederneiras.sp.gov.br

17.4. Permitir 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. Fornecer proteção para ambiente Exchange
18.2. Oferecer tecnologia para proteção contra spam;
18.3. Oferecer análise comportamental e proteção para zero-day;
18.4. Oferecer 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.
19.2. Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);
19.3. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
19.4. Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra

Rua Siqueira Campos, S-64 – Centro – CEP 17280-000 – Pederneiras/SP
Tel.: (14) 3283 9570 – Fax: (14) 3284 1764 – www.pederneiras.sp.gov.br