VTECH SEGURANÇA DE INFORMAÇÃO

PROPOSTA DE PREÇOS

PREGÃO ELETRÔNICO 004/2021 - SRP

02/09/2021

Cliente:	**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAZONAS**	
Pregão Eletrônico:	Pregão Eletrônico 004/2021 Processo Administrativo n.°23443.001488/2021-11	
Endereçado à:	Comissão de Licitação	
Referência do objeto:	Proposta de serviços de tecnologia da informação e comunicação Fornecimento/Renovação de Licença de Antivírus Kaspersky Endpoint Security for Business Advanced, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.	

QUEM É A VTECH?

A VTECH é uma empresa focada em Segurança da Informação e Comunicação, que fornece soluções inovadoras em TI visando atender aos nossos clientes com celeridade, flexibilidade e inovação, sempre prezando pela qualidade de seus serviços.

Atuando em todo o território nacional, oferecemos soluções para proteção de seus negócios com tecnologia de ponta com o propósito de garantir segurança e privacidade total no mundo digital.

OBJETO

A proposta tem por finalidade o fornecimento /Renovação de Licença de Antivírus do Kaspersky Endpoint Security for Business Advanced para 5.230 licenças pelo período de 36 (trinta e seis) meses, com suporte e atualização, conforme especificações básicas no edital, termo de referência e seus anexos.

Requisitos de Garantia e Manutenção

A VTECH oferecerá garantia de atualização do software, durante todo o período de vigência da Licença, repassando toda e qualquer atualização e/ou correção de software, inclusive atualização de versão, sem qualquer ônus adicional para o IFAM.

A VTECH disponibilizará suporte técnico presencial ou remoto no regime 5x8 (cinco dias por semana, oito horas por dia) por 36 meses.

O suporte poderá ser executado por serviço telefônico ou Internet, em caso de resolução tempestiva de falhas.

O suporte técnico será prestado de forma a assegurar a disponibilidade e manter o software em perfeitas condições de uso.

O suporte técnico também irá auxiliar na resolução de problemas de atualização de novas versões, salvamento e restauração por um período de 36 meses.

Deveres e responsabilidades da VTECH

Indicará formalmente e por escrito, no prazo máximo de 5 (cinco) dias úteis após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;

Atenderá prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

Reparará quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

Propiciará todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

Manterá, durante toda a execução do contrato, as mesmas condições da habilitação;

Manterá, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

Manterá a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

Cederá os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração;

Executará o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

Não irá veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante;

Não irá fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;

Não será admitida a subcontratação do objeto licitatório;

DO FABRICANTE

Fundada em 1997, a Kaspersky Lab é fornecedor internacional de software de segurança de informações. A empresa está sediada em Moscou, na Rússia, com escritórios regionais no Reino Unido, na França, Alemanha, Holanda, Polônia, Japão, China e nos Estados Unidos. Uma grande rede de parceiros que compreende mais de 500 empresas em todo o mundo amplia essa área de abrangência.

Nossos produtos são certificados pela West Coast Labs e costumam receber prêmios regularmente dos principais laboratórios de testes e publicações da área de TI. Em 2003, recebemos o status de Microsoft Gold Certified Partner para Soluções de Segurança. A Kaspersky Lab também tem orgulho de sua parceria com a SUSE e a Red Hat. Nossos especialistas participam ativamente de associações do setor, como a CARO (Computer Antivirus Research Organization) e a ICSA (International Computer Security Association).

Os analistas do Laboratório de Vírus chefiado por Eugene Kaspersky, Costin Raiu e Marc Blanchard possuem mais de uma década de experiência no setor de antivírus, o que lhes permite prever as tendências em segurança de dados. Por exemplo, nós fomos os primeiros a desenvolver e implementar inovações como a análise heurística de vírus e a análise linguística de texto. Essas inovações mantêm o portfólio de produtos da empresa na vanguarda do mercado.

Os anos de desenvolvimento direcionado tornaram a Kaspersky Lab um líder em tecnologia de proteção antivírus. Nosso portfólio de produtos contém soluções que protegem estações de trabalho, servidores de arquivos, gateways de email, firewalls e dispositivos portáteis das ameaças às informações.

Atualmente, a maioria dos malwares é multifuncional e profundamente integrada com os recursos da Internet. As soluções antivírus tradicionais não são mais suficientes para proteger os usuários de todas as ameaças externas. A Kaspersky Lab atua de forma proativa em relação às dinâmicas necessidades do usuário.

Fatos Diretos sobre a Kaspersky

- A maior empresa privada de antimalware do mundo
- Crescimento sem precedentes, oito vezes maior que a média do setor
- Mais de 300 milhões de usuários em todo o mundo
- 50.000 novos sistemas adicionados por semana

Por que a Kaspersky?

A Kaspersky Lab fornece a proteção mais imediata contra ameaças à segurança da TI, que incluem vírus, spyware, crimeware, hackers, phishing e spam. Os nossos produtos fornecem taxas de detecção superiores e o

menor tempo de resposta a surtos do setor para usuários domésticos, pequenas e médias empresas, grandes corporações e o ambiente de computação móvel. A tecnologia da Kaspersky® também é usada em todo o mundo em produtos e serviços dos líderes do setor no fornecimento de soluções de segurança de TI.

Nós investimos todos os nossos recursos e conhecimento para impedir a disseminação dessas ameaças. Nós ajudamos a informar a comunidade envolvida sobre as práticas recomendáveis a fim de assegurar a melhor segurança online possível.

O sucesso de nossa missão resultou no destaque da Kaspersky Lab como a maior empresa privada de antimalware do mundo. Fundada em 1997, a empresa fornece seus produtos e tecnologias para o setor e os consumidores em praticamente todos os países do mundo. Atualmente, mais de 300 milhões de usuários em todo o mundo estão protegidos por nossas tecnologias. E, todas as semanas, adicionamos mais de 50.000 novos sistemas.

Como resultado do suporte às necessidades de nossos clientes, a Kaspersky Lab chegou a mais de 1.800 funcionários, com mais da metade de nós trabalhando em pesquisa e desenvolvimento e no suporte ao cliente. Nossos produtos são continuamente reconhecidos por sua qualidade. Durante a última década e meia, a Kaspersky Lab liderou o setor de antivírus em termos de inovação, tendo iniciado a primeira utilização de assinaturas de bancos de dados externos em 1992, além de ter sido a primeira a desenvolver e implementar a análise heurística de vírus e a análise linguística de texto. Nossa equipe internacional de especialistas analisa continuamente as últimas tendências de segurança, no esquema 24x7x365, permitindo assim o mais rápido tempo de resposta do setor às ameaças da Internet e possibilitando o desenvolvimento de novas tecnologias inovadoras (várias das quais são bastante usadas no momento em produtos de segurança em todo o mundo) à frente da concorrência. A missão da empresa é sempre estar um passo à frente da concorrência ao fornecer excelência: a melhor proteção possível e garantir que o portfólio de produtos da empresa permaneça na vanguarda do mercado.

DOS PREÇOS

Id	Descrição	Quant	Unidade De Medida	Valor Unitário (R$	Valor Total (R$)
01	Fornecimento de software de antivírus Kaspersky Endpoint Security for Business **ADVANCED**, para 5.230 licenças pelo período de 36 (trinta e seis) meses, com suporte e atualização. Modelo: Kaspersky Endpoint Security for Business **ADVANCED** Fabricante: Kaspersky	**5.230**	**UN**	**R$ 106,00**	**R$ 554.380,00**
	Valor total		R$ 554.380,00		

Valor total da proposta R$ 554.380,00 (Quinhentos e cinquenta e quatro mil trezentos e oitenta reais)

As 5.230 licenças devem ser disponibilizadas à medida que os Campi fizeram a contratação

A validade desta proposta é de 60 (Sessenta dias).

O prazo de entrega dos Bens é de 10 (dez) dias, contados a partir do recebimento da nota de Empenho

Os itens serão entregues via download, devendo o link e demais instruções serem enviados para os e-mails informados no edital;

Implantação: A instalação do software será realizada no Datacenter do IFAM e nos Campi que aderirem à solução.

A VTECH informará o canal oficial para suporte.

Prazo de Garantia, licenciamento: de 36 (trinta e seis) meses, com suporte técnico e atualização.

Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo do Edital.

Lauro de Freitas, Bahia 02 de setembro de 2021

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520
Assinado de forma digital por NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520
Dados: 2021.09.02 11:20:06 -03'00'

Natasha de Matos Oliveira Araújo
CPF: 628.604.105-20
RG: 04.705.945-19
Endereço Postal: Avenida Santos Dumont, 4487, Km 3,5, Loja 157, Shopping Passeio Norte, Estrada do Coco, Lauro de Freitas, Bahia, CEP 42.702-400.
Endereço Eletrônico: Comercial@vtechti.com.br / Natasha@vtechti.com.br
Razão social: VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA EIRELI
CNPJ: 22.122.370/0001-34
Cargo: Diretora Geral
Tel: (71)3289-0643 | 71 9625-5980
Insc. Municipal: 001.001.7482 | Insc. Estadual: 123.555.216 ME
Banco do Bradesco Agência 0592-4, Conta Corrente: 11.304-2

ESPECIFICAÇÕES TÉCNICAS

Compatibilidade

1.1.1 Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
1.1.2 Microsoft Storage Server 2012 e 2012 R2 x64;
1.1.3 Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
1.1.4 Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
1.1.5 Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
1.1.6 Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
1.1.7 Microsoft Windows 8 Professional / Enterprise x64;
1.1.8 Microsoft Windows 8.1 Professional / Enterprise x32;
1.1.9 Microsoft Windows 8.1 Professional / Enterprise x64;
1.1.10 Microsoft Windows 10 x32;
1.1.11 Microsoft Windows 10 x64;

Suporta as seguintes plataformas virtuais:

1.2.1 Vmware: Workstation 15.x Pro, vSphere 6.5, vSphere 6.7;
1.2.2 Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64;
1.2.3 Parallels Desktop 14;
1.2.4 Citrix XenServer 7.1;

Características:

1.3.1 A console deve ser acessada via WEB (HTTPS) ou MMC;
1.3.2 A Console deve ser baseada no modelo cliente/servidor;

1.3.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

1.3.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

1.3.5 Deve permitir incluir usuários do AD para logarem na console de administração;

1.3.6 Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

1.3.7 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

1.3.8 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

1.3.9 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

1.3.10 Deve registrar em arquivo de log todas as atividades efetuadas

pelos administradores, permitindo execução de análises em nível

de auditoria;

1.3.11 Deve armazenar histórico das alterações feitas em políticas;

1.3.12 Deve permitir voltar para uma configuração antiga da política de

acordo com o histórico de alterações efetuadas pelo

administrador apenas selecionando a data em que a política foi

alterada;

1.3.13 Deve ter a capacidade de comparar a política atual com a anterior,

informando quais configurações foram alteradas;

1.3.14 A solução de gerência deve permitir, através da console de

gerenciamento, visualizar o número total de licenças gerenciadas;

1.3.15 Através da solução de gerência, deve ser possível verificar qual

licença está aplicada para determinado computador;

1.3.16 Capacidade de instalar remotamente a solução de segurança em

smartphones e tablets de sistema iOS, Android e Windows;

1.3.17 Capacidade de instalar remotamente qualquer “app” em

smartphones e tablets de sistema iOS;

1.3.18 A solução de gerência centralizada deve permitir gerar relatórios,

visualizar eventos, gerenciar políticas e criar painéis de controle;

1.3.19 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

1.3.20 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

1.3.21 Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;

1.3.22 Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

1.3.23 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

1.3.24 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

1.3.25 Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

1.3.26 A comunicação entre cliente e servidor de administração deve ser criptografada;

1.3.27 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

1.3.28 Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

1.3.29 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

1.3.30 Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

1.3.31 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

1.3.32 Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

1.3.33 Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente

importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

1.3.34 Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc.;

1.3.35 Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.3.36 Deve fornecer as seguintes informações dos computadores:

1.3.36.1 Se o antivírus está instalado;

1.3.36.2 Se o antivírus está iniciado;

1.3.36.3 Se o antivírus está atualizado;

1.3.36.4 Minutos/horas desde a última conexão da máquina com o servidor administrativo;

1.3.36.5 Minutos/horas desde a última atualização de vacinas;

1.3.36.6 Data e horário da última verificação executada na máquina;

1.3.36.7 Versão do antivírus instalado na máquina;

1.3.36.8 Se é necessário reiniciar o computador para aplicar mudanças;

1.3.36.9 Data e horário de quando a máquina foi ligada;

1.3.36.10 Quantidade de vírus encontrados (contador) na máquina;

1.3.36.11 Nome do computador;

1.3.36.12 Domínio ou grupo de trabalho do computador;

1.3.36.13 Data e horário da última atualização de vacinas;

1.3.36.14 Sistema operacional com Service Pack;

1.3.36.15 Quantidade de processadores;

1.3.36.16 Quantidade de memória RAM;

1.3.36.17 Usuário (s) logado (s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

1.3.36.18 Endereço IP;

1.3.36.19 Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

1.3.36.20 Atualizações do Windows Update instaladas;

1.3.36.21 Informação completa de hardware contendo:

processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

1.3.36.22 Vulnerabilidades de aplicativos instalados na máquina;

1.3.36.23 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

1.3.36.24 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

1.3.36.25 Alteração de Gateway Padrão;

1.3.36.26 Alteração de subrede;

1.3.36.27 Alteração de domínio;

1.3.36.28 Alteração de servidor DHCP;

1.3.36.29 Alteração de servidor DNS;

1.3.36.30 Alteração de servidor WINS;

1.3.36.31 Alteração de subrede;

1.3.36.32 Resolução de Nome;

1.3.36.33 Disponibilidade de endereço de conexão SSL

1.3.37 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

1.3.38 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.3.39 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.3.40 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

1.3.41 Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.3.42 Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

1.3.43 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

1.3.44 Capacidade de gerar traps SNMP para monitoramento de eventos;

1.3.45 Capacidade de enviar e-mails para contas específicas em caso de algum evento;

1.3.46 Listar em um único local, todos os computadores não gerenciados na rede;

1.3.47 Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

1.3.48 Deve possuir compatibilidade com Microsoft NAP, quandoinstalado em um Windows 2008 Server;

1.3.37 Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

1.3.38 Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

1.3.39 Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

1.3.40 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

1.3.41 Deve por meio de opções de otimização fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;

1.3.42 Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

1.3.43 Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;

1.3.44 Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

1.3.45 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.3.46 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

1.3.47 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

1.3.48 Capacidade de listar updates nas máquinas com o respectivo link para download

1.3.49 Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

1.3.50 Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

1.3.51 Capacidade de realizar inventário de hardware de todas as máquinas clientes;

1.3.52 Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

1.3.53 Capacidade de diferenciar máquinas virtuais de máquinas físicas

2.1.1 Microsoft Windows 8 Professional/Enterprise x86 / x64;

2.1.2 Microsoft Windows 8.1 Professional / Enterprise x86 / x64;

2.1.3 Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;

2.1.4 Microsoft Windows Server 2019 Essentials / Standard / Datacenter;

2.1.5 Microsoft Windows Server 2016 Essentials / Standard / Datacenter;

2.1.6 Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;

2.1.7 Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;

2.1.8 Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;

2.1.9 Microsoft Windows Small Business Server 2011 Standard / Standard x64;

2.1.10 Microsoft Windows MultiPoint Server 2011 x64;

2.2.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc.) que verifique qualquer arquivo criado, acessado ou

modificado;

2.2.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

2.2.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

2.2.4 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de

limpeza;

2.2.5 Firewall com IDS;

2.2.6 Autoproteção (contra-ataques aos serviços/processos do antivírus);

2.2.7 Controle de dispositivos externos;

2.2.8 Controle de acesso a sites por categoria, Ex: Bloquear conteúdo adulto, sites de jogos, etc.;

2.2.9 Controle de acesso a sites por horário;

2.2.10 Controle de acesso a sites por usuários;

2.2.11 Controle de acesso a websites por dados, ex: Bloquear websites com conteúdo de vídeo e áudio;

2.2.12 Controle de execução de aplicativos;

2.2.13 Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2.2.14 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.2.15 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora

independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

2.2.16 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.2.17 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.2.18 Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

2.2.19 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.2.20 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.2.21 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.2.22 Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

2.2.23 Capacidade de verificar somente arquivos novos e alterados;

2.2.24 Capacidade de verificar objetos usando heurística;

2.2.25 Capacidade de agendar uma pausa na verificação;

2.2.26 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

2.2.27 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

2.2.28 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.2.28.1 Perguntar o que fazer, ou;

2.2.28.2 Bloquear acesso ao objeto;

2.2.28.3 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.29 Caso positivo de desinfecção:

2.2.29.1 Restaurar o objeto para uso;

2.2.30 Caso negativo de desinfecção:

2.2.30.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.31 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.2.32 Capacidade de verificar e-mails recebidos e enviados nos

protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

2.2.33 Capacidade de verificar links inseridos em e-mails contra phishings;

2.2.34 Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;

2.2.35 Capacidade de verificação de corpo e anexos de e-mails usando heurística;

2.2.36 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.2.36.1 Perguntar o que fazer, ou;

2.2.36.2 Bloquear o e-mail;

2.2.36.3 Apagar o objeto ou tentar desinfectá-lo (de

acordo com a configuração pré-estabelecida pelo

administrador);

2.2.37 Caso positivo de desinfecção:

2.2.37.1 Restaurar o e-mail para o usuário;

2.2.38 Caso negativo de desinfecção:

2.2.38.1 Mover para quarentena ou apagar o objeto (de

acordo com a configuração pré-estabelecida pelo administrador);

2.2.39 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

2.2.40 Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

2.2.41 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

2.2.42 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;

2.2.43 Deve ter suporte total ao protocolo Ipv6;

2.2.44 Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

2.2.45 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.2.45.1Perguntar o que fazer, ou;

2.2.45.2 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.2.45.3Permitir acesso ao objeto;

2.2.46 O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.2.46.1Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo

real, ou; 2.2.46.2Verificação de buffer, onde os dados são recebidos e armazenados para posterior

verificação;

2.2.47 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

2.2.48 Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

2.2.49 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

2.2.50 Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

2.2.51Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);

2.2.52 Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.2.53 Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada

juntamente com as vacinas;

2.2.54 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.2.55 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.2.56 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.2.57 Deve possuir módulo que habilite ou não o funcionamento dos

seguintes dispositivos externos, no mínimo:

2.2.57.1 Discos de armazenamento locais;

2.2.57.2 Armazenamento removível;

2.2.57.3 Impressoras;

2.2.57.4 CD/DVD;

2.2.57.5 Drives de disquete;

2.2.57.6 Modems;

2.2.57.7 Dispositivos de fita;

2.2.57.8 Dispositivos multifuncionais;

2.2.57.9 Leitores de smart card;

2.2.57.10 Dispositivos de sincronização via ActiveSync

(Windows CE, Windows Mobile, etc)

2.2.57.11 Wi-Fi;

2.2.57.12 Adaptadores de rede externos;

2.2.57.13 Dispositivos MP3 ou smartphones;

2.2.57.14 Dispositivos Bluetooth;

2.2.57.15 Câmeras e Scanners.

2.2.58 Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

2.2.59 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

2.2.60 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

2.2.61 Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

2.2.62 Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

2.2.63 Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

2.2.64 O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.2.65 Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.66 White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.67 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.2.68 Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

2.2.69 Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até o controle de aplicativos, dispositivos e acesso à web;

2.2.70 Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até o controle de aplicativos,

dispositivos e acesso à web.

2.2.71 Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.2.72 Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.2.73 Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.2.74 Capacidade de integração com o Windows Defender Security Center.

2.2.75 Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.2.76 Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

3.1.1 MacOS Catalina 10.15

3.1.2 MacOS Mojave 10.14

3.1.3 MacOS High Sierra 10.13

3.1.4 MacOS Sierra 10.12

3.2.1 Deve prover proteção residente para arquivos (anti-spyware, antitrojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.2.2 Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar

endereços https;

3.2.3 Possuir módulo de bloqueio á ataques na rede;

3.2.4 Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

3.2.5 Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

3.2.6 Possibilidade de importar uma chave no pacote de instalação;

3.2.7 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.2.8 A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;

3.2.9 Deve possuir suportes a notificações utilizando o Growl;

3.2.10 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

3.2.11 Capacidade de voltar para a base de dados de vacina anterior;

3.2.12 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

3.2.13 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto

do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado; 3.2.14 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

3.2.15 3.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

3.2.16 Capacidade de verificar somente arquivos novos e alterados;

3.2.17 Capacidade de verificar objetos usando heurística;

3.2.18 Capacidade de agendar uma pausa na verificação;3.2.19 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.2.19.1 Perguntar o que fazer, ou;

3.2.19.2 Bloquear acesso ao objeto;

3.2.19.3 Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

3.2.20 Caso positivo de desinfecção:

3.2.20.1 Restaurar o objeto para uso;

3.2.21 Caso negativo de desinfecção:

3.2.21.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

3.2.22 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

3.2.23 Capacidade de verificar arquivos de formato de e-mail;

3.2.24 Possibilidade de trabalhar com o produto pela linha de comando,com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

3.2.25 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

EstaçõesdeTrabalhoLinux

4.1 Compatibilidade

4.1.1 Plataforma 32-bits:

4.1.1.1 Ubuntu 16.04 LTS

4.1.1.2 Ubuntu 16.04 LTS;

4.1.1.3 Red Hat® Enterprise Linux® 6.7 Server;

4.1.1.4 CentOS 6.7;

4.1.1.5 Debian GNU / Linux 9.4 ;

4.1.1.6 Debian GNU / Linux 10;

4.1.1.7 Linux Mint 18.2;

4.1.1.8 Linux Mint 19;

4.1.1.9 Gos Linux 6.6;

4.1.1.10 Mageia 4;

4.1.1.11 OS Lotos ;

4.1.2 Plataforma 64-bits:

4.1.2.1 Ubuntu 16.04 LTS;

4.1.2.2 Ubuntu 18.04 LTS;

4.1.2.3 Red Hat Enterprise Linux 6.7;

4.1.2.4 Red Hat Enterprise Linux 7.2;

4.1.2.5 Red Hat Enterprise Linux 8.0;

4.1.2.6 CentOS 6.7;

4.1.2.7 CentOS 7.2;

4.1.2.8 CentOS 8.0;

4.1.2.9 Debian GNU / Linux 9.4

4.1.2.10 Debian GNU / Linux 10.1;

4.1.2.11 Oracle Linux 7.3;

4.1.2.12 Oracle Linux 8;

4.1.2.13 SUSE® Linux Enterprise Server 15;

4.1.2.14 OpenSUSE® Leap 15;

4.1.2.15 Amazon Linux AMI

4.1.2.16 Linux Mint 18.2;

4.1.2.17 Linux Mint 19;

4.1.2.18 Gos Linux 6.6

4.1.2.19 Gos Linux 7.24.2 Características

4.2.1 Antivírus de arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

4.2.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

4.2.3 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

4.2.4 Capacidade de criar exclusões por local, máscara e nome da ameaça;

4.2.5 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.2.6 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

4.2.7 Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

4.2.8 Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

4.2.8.1 Alta;

4.2.8.2 Média;

4.2.8.3 Baixa;

4.2.8.4 Recomendado;

4.2.9 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

4.2.10 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

4.2.11 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

4.2.12 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

4.2.13 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

4.2.14 Capacidade de verificar objetos usando heurística;

4.2.15 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

5. ServidoresWindo

5.1 Compatibilidade

5.1.1 Plataforma 32-bits:

5.1.1.1 Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;

5.1.1.2 Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

5.1.1.3 Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;

5.1.1.4 Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior;

5.1.2 Plataforma 64-bits

5.1.2.1 Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;

5.1.2.2 Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

5.1.2.3 Microsoft Windows Server 2008 Standard / Enterprise / Data Center SP1 ou posterior;ws

5.1.2.4 Microsoft Windows Server 2008 Core Standard / Enterprise / Data Center SP1 ou posterior.

5.1.2.5 Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise / Data Center SP1 ou posterior;

5.1.2.6 Microsoft Windows Server 2008 R2 Core Standard /Enterprise / Data Center SP1 ou posterior;

5.1.2.7 Microsoft Small Business Server 2008 Standard / Premium

5.1.2.8 Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;

5.1.2.9 Microsoft Microsoft Small Business Server 2011 Essentials / Standard

5.1.2.10 Microsoft Windows MultiPoint Server 2011

5.1.2.11 Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter / MultiPoint;

5.1.2.12 Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

5.1.2.13 Microsoft Windows Server 2012 Core Standard / Datacenter;

5.1.2.14 Microsoft Windows Server 2012 R2 Core Standard / Datacenter;

5.1.2.15 Microsoft Windows Storage Server 2012;

5.1.2.16 Microsoft Windows Storage Server 2012 R2;

5.1.2.17 Microsoft Windows Hyper-V Server 2012;

5.1.2.18 Microsoft Windows Hyper-V Server 2012 R2;

5.1.2.19 Windows Server 2016 Essentials /Standard / Datacenter/ MultiPoint Premium Server;

5.1.2.20 Windows Server 2016 Core Standard / Datacenter;

5.1.2.21 Windows Storage Server 2016;

5.1.2.22 Windows Hyper-V Server 2016;

5.1.2.23 Microsoft Windows Server 2019 Core / Terminal / HyperV

5.1.2.24 Windows Server IoT 2019 for Storage

5.2 Características

5.2.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

5.2.2 Auto-proteção contra-ataques aos serviços/processos do antivírus;

5.2.3 Firewall com IDS;

5.2.4 Controle de vulnerabilidades do Windows e dos aplicativos instalados;

5.2.5 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

5.2.6 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

5.2.7 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

5.2.7.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

5.2.7.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

5.2.7.3 Leitura de configurações;

5.2.7.4 Modificação de configurações;

5.2.7.5 Gerenciamento de Backup e Quarentena;

5.2.7.6 Visualização de relatórios;

5.2.7.7 Gerenciamento de relatórios;

5.2.7.8 Gerenciamento de chaves de licença;

5.2.7.9 Gerenciamento de permissões (adicionar/excluir permissões acima);

5.2.8 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:5.2.8.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

5.2.8.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

5.8.9 Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

5.8.10 Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;

5.8.11 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia,erros, etc);

5.8.12 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

5.8.13 Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

5.8.14 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

5.8.15 Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

5.8.16 Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

5.8.17 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

5.8.18 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também,de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

5.8.19 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

5.8.20 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

5.8.21 Capacidade de verificar somente arquivos novos e alterados;

5.8.22 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

5.8.23 Capacidade de verificar objetos usando heurística;

5.8.24 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

5.8.25 Capacidade de agendar uma pausa na verificação;

5.8.26 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

5.8.27 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

5.8.27.1 Perguntar o que fazer, ou;

5.8.27.2 Bloquear acesso ao objeto;5.8.27.3 Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

5.8.28 Caso positivo de desinfecção:

5.8.28.1 Restaurar o objeto para uso;

5.8.29 Caso negativo de desinfecção:

5.8.29.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

5.8.30 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

5.8.31 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

5.8.32 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

5.8.33 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

5.8.34 Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

5.8.35 Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

5.8.36 Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

6. ServidoresLinux

6.1 Compatibilidade

6.1.1 Plataforma 32-bits:

6.1.1.1 Ubuntu 16.04 LTS;

6.1.1.2 Red Hat® Enterprise Linux® 6.7 Server;

6.1.1.3 CentOS 6.7;

6.1.1.4 Debian GNU / Linux 9.4;

6.1.1.5 Debian GNU / Linux 10;

6.1.1.6 Linux Mint 18.2;

6.1.1.7 Linux Mint 19;

6.1.1.8 Gos Linux 6.6;

6.1.1.9 Mageia 4;

6.1.1.10 OS Lotos;

6.1.2 Plataforma 64-bits:

6.1.2.1 Ubuntu 16.04 LTS;

6.1.2.2 Ubuntu 18.04 LTS;

6.1.2.3 Red Hat Enterprise Linux 6.7;

6.1.2.4 Red Hat Enterprise Linux 7.2;

6.1.2.5 Red Hat Enterprise Linux 8.0;

6.1.2.6 CentOS 6.7;

6.1.2.7 CentOS 7.2;

6.1.2.8 CentOS 8.0;

6.1.2.9 Debian GNU / Linux 9.4

6.1.2.10 Debian GNU / Linux 10.1;

6.1.2.11 Oracle Linux 7.3;

6.1.2.12 Oracle Linux 8;

6.1.2.13 SUSE® Linux Enterprise Server 15;

6.1.2.14 OpenSUSE® Leap 15;

6.1.2.15 Amazon Linux AMI

6.1.2.16 Linux Mint 18.2;

6.1.2.17 Linux Mint 19;

6.1.2.18 Gos Linux 6.6

6.1.2.19 Gos Linux 7.26.2 Características

6.2.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

6.2.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

6.2.3 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

6.2.4 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

6.2.5 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

6.2.6 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

6.2.7 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

6.2.8 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

6.2.9 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

6.2.10 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

6.2.11 Capacidade de verificar objetos usando heurística;

6.2.12 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

6.2.13 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

6.2.14 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

7. Smartphoneset

7.1 Compatibilidade:

Dispositivos com os sistemas operacionais:

7.1.1 Android 5.0 – 5.1.1

7.1.2 Android 6.0 – 6.0.1

7.1.3 Android 7.0 – 7.12

7.1.4 Android 8.0 – 8.1

7.1.5 Android 9.0

7.1.6 Android 10.0

7.1.7 Android 11.0

7.1.8 iOS 10.0 – 10.3.3

7.1.9 iOS 11.0 – 11.3

7.1.10 iOS 12.0

7.1.11 iOS 13.0

7.1.12 iOS 14.0ablets

7.2 Características

7.2.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

7.2.1.1 Proteção contra adware e autodialers;

7.2.1.2 Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar downmodalidaded usando o browser;

7.2.1.3 Arquivos abertos no smartphone;

7.2.1.4 Programas instalados usando a interface do smartphone

7.2.1.5 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

7.2.2 Deverá isolar em área de quarentena os arquivos infectados;

7.2.3 Deverá atualizar as bases de vacinas de modo agendado;

7.2.4 Deverá bloquear spams de SMS por meio de Black lists;

7.2.5 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;

7.2.6 Capacidade de desativar por política: Wi-fi; Câmera; Bluetooth.

7.2.7 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

7.2.8 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

7.2.9 Deverá ter firewall pessoal (Android);

7.2.10 Capacidade de tirar fotos quando a senha for inserida incorretamente;

7.2.11 Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

7.2.12 Capacidade de enviar comandos remotamente de:

· Localizar;

· Bloquear.

7.2.13 Capacidade de detectar Jailbreak em dispositivos iOS;

7.2.14 Capacidade de bloquear o acesso a site por categoria em dispositivos;

7.2.15 Capacidade de bloquear o acesso a sites phishing ou malicioso;

7.2.16 Capacidade de criar containers de aplicativos, separando dados

corporativos de dados pessoais;

7.2.17 Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;

7.2.18 Capacidade de configurar White e blacklist de aplicativos;

7.2.19 Capacidade de localizar o dispositivo quando necessário;

7.2.20 Permitir atualização das definições quando estiver em “roaming”;

7.2.21 Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

7.2.22 Deve permitir verificar somente arquivos executáveis;

7.2.23 Deve ter a capacidade de desinfetar o arquivo se possível;

7.2.24 Capacidade de agendar uma verificação;

7.2.25 Capacidade de enviar URL de instalação por e-mail;

7.2.26 Capacidade de fazer a instalação através de um link QRCode;

7.2.27 Capacidade de executar as seguintes ações caso a desinfecção

falhar:

· Deletar;

· Ignorar;

· Quarentenar;

· Perguntar ao usuário

8. Gerenciamentodedispositivosmóveis(MDM)

8.1 Compatibilidade:

8.1.1 Android 5.0 – 5.1.1

8.1.2 Android 6.0 – 6.0.1

8.1.3 Android 7.0 – 7.12

8.1.4 Android 8.0 – 8.1

8.1.5 Android 9.0

8.1.6 Android 10.0

8.1.7 Android 11.0

8.1.8 iOS 10.0 – 10.3.3

8.1.9 iOS 11.0 – 11.3

8.1.10 iOS 12.0

8.1.11 iOS 13.0

Softwares de gerência de dispositivos:

8.1.12 VMWare AirWatch 9.3;

8.1.13 MobileIron 10.0;

8.1.14 IBM Maas360 10.68;

8.1.15 Microsoft Intune 1908;

8.1.16 SOTI MobiControl 14.1.4 (1693);

8.2 Características

8.2.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

8.2.2 Capacidade de ajustar as configurações de:

8.2.3 Sincronização de e-mail;

8.2.4 Uso de aplicativos;

8.2.5 Senha do usuário;

8.2.6 Criptografia de dados;

8.2.7 Conexão de mídia removível.

8.2.8 Capacidade de instalar certificados digitais em dispositivos móveis;

8.2.9 Capacidade de, remotamente, resetar a senha de dispositivos iOS;

8.2.10 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

8.2.11 Capacidade de, remotamente, bloquear um dispositivo iOS;

8.2.12 Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

8.2.13 Possibilidade de exigir senha para abrir aplicações instaladas em container;

8.2.14 Deve permitir que o usuário utilize autenticação do Active Directory para abrir aplicações em container;

8.2.15 Deve permitir que uma senha seja digitada a cada x(minutos) para continuar utilizando uma aplicação em container;

8.2.16 Deve permitir a criptografia de dados salvos pelas aplicações em container;

8.2.17 Permitir sincronização com perfil do “Touch Down”;

8.2.18 Capacidade de desinstalar remotamente o antivírus do dispositivo;

8.2.19 Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

8.2.20 Capacidade de sincronizar com Samsung Knox;

9. Criptofia

9.1 Compatibilidade

9.1.1 Microsoft Windows 7 Professional SP1 ou superior x86/x64;

9.1.2 Microsoft Windows 8 Enterprise x86/x64;

9.1.3 Microsoft Windows 8 Pro x86/x64;

9.1.4 Microsoft Windows 8.1 Pro x86/x64;

9.1.5 Microsoft Windows 8.1 Enterprise x86/x64;

9.1.6 Microsoft Windows 10 Pro / Enterprise / Home / Education x86 /

x64;rafia

9.2 Características

9.2.1 O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

9.2.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

9.2.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

9.2.4 Capacidade de utilizar Single Sign On para a autenticação de pré-boot;

9.2.5 Permitir criar vários usuários de autenticação pré-boot;

9.2.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

9.2.7 Capacidade de criptografar drives removíveis de acordo com

regra criada pelo administrador, com as opções:

9.2.8 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

9.2.9 Criptografar todos os arquivos individualmente;

9.2.10 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

9.2.11 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

9.2.12 Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

9.2.13 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

9.2.14 Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

9.2.15 Verificar compatibilidade de hardware antes de aplicar a criptografia;

9.2.16 Possibilita estabelecer parâmetros para a senha de criptografia;

9.2.17 Bloqueia o reuso de senhas;

9.2.18 Bloqueia a senha após um número de tentativas pré- estabelecidas;

9.2.19 Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

9.2.20 Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;

9.2.21 Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do Outlook”;

9.2.22 Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

9.2.23 Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc.;

9.2.24 Permite criar um grupo de extensões de arquivos a serem criptografados;

9.2.25 Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

9.2.26 Permite criptografia de dispositivos móveis mesmo quando o Endpoint não possuir comunicação com a console de gerenciamento.

9.2.27 Capacidade de deletar arquivos de forma segura após a criptografia;

9.2.28 Capacidade de criptografar somente o espaço em disco utilizado;

9.2.29 Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;9.2.30 Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

9.2.31 Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc.;

9.2.32 Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

9.2.33 Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

9.2.34 Capacidade de fazer “Hardware encryption”;

10. GerenciamentodeSistemas

10.1 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

10.2 Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

10.3 Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

10.4 Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

10.5 Capacidade de gerenciar licenças de softwares de terceiros;

10.6 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

10.7 Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;

10.8 Possibilita fazer distribuição de software de forma manual e agendada;

10.9 Suporta modo de instalação silenciosa;

10.10 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

10.11 Possibilita fazer a distribuição através de agentes de atualização;

10.12 Utiliza tecnologia multicast para evitar tráfego na rede;

10.13 Possibilita criar um inventário centralizado de imagens;

10.14 Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

10.15 Suporte a WakeOnLan para deploy de imagens;

10.16 Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

10.17 Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

10.18 Capacidade de gerar relatórios de vulnerabilidades e patches;

10.19 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

10.20 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

10.21 Permite baixar atualizações para o computador sem efetuar a instalação

10.22 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

10.23 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

10.24 Permite selecionar produtos a serem atualizados pela console de gerenciamento;

10.25 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

10.26 Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

10.27 Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

10.28 Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;

10.29 Deve permitir selecionar o idioma das aplicações que serão atualizadas;

10.30 Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520

Assinado de forma digital por NATASHA DE MATOS OLIVEIRA ARAUJO:62860410520
Dados: 2021.09.02 11:21:12 -03'00'