Termo de Referência de Endpoint de nova geração (Antivírus Corporativo)

Anexo I

1. **Servidor de Administração e Console Administrativa**

1.1. Compatibilidade:

1.1.1. Microsoft Windows Server 2008 Standard / Enterprise / Foundation / Essentials / Datacenter x64;
1.1.2. Microsoft Storage Server 2008 x64;
1.1.3. Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
1.1.4. Microsoft Storage Server 2012 e 2012 R2 x64;
1.1.5. Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
1.1.6. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
1.1.7. Microsoft Storage Server 2016 x64;
1.1.8. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
1.1.9. Microsoft Storage Server 2019 x64;
1.1.10. Microsoft Windows Server 2022 Standard / Datacenter x64 / Datacenter Azure Edition x64;
1.1.11. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
1.1.12. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
1.1.13. Microsoft Windows 8 Professional / Enterprise x64;
1.1.14. Microsoft Windows 8.1 Professional / Enterprise x32;
1.1.15. Microsoft Windows 8.1 Professional / Enterprise x64;
1.1.16. Windows 10 32-bit/64-bit;
1.1.17. Windows 11

1.2. 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, 2022 x64;
1.2.5. Parallels Desktop 16;
1.2.7. Citrix XenServer 7.1;

1.3. Características:

1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.3.2. A console deve suportar arquitetura on-premise e arquitetura cloud-based;
1.3.3. Console deve ser baseada no modelo cliente/servidor;
1.3.4. A console deve suportar autenticação de dois fatores;

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

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

1.3.7. Deve permitir incluir usuários do AD para fazer login na console de administração

1.3.8. 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;

1.3.9. 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;

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

1.3.11. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.

1.3.12. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

1.3.13. Deve armazenar histórico das alterações feitas em políticas;

1.3.14. 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;

1.3.15. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

1.3.16. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

1.3.17. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

1.3.19. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

1.3.20. 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;

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

1.3.22. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

1.3.23. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
1.3.24. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
1.3.25. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
1.3.26. 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;
1.3.27. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
1.3.28. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
1.3.29. 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.

1.3.30. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
1.3.31. 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;
1.3.32. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
1.3.33. 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;
1.3.34. 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;
1.3.35. 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;

1.3.36. 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;

1.3.37. Deve fornecer as seguintes informações dos computadores:

1.3.37.1. Se o antivírus está instalado;

1.3.37.2. Se o antivírus está iniciado;

1.3.37.3. Se o antivírus está atualizado;

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

1.3.37.5. Minutos/horas desde a última atualização de vacinas;

1.3.37.6. Data e horário da última verificação executada na máquina;

1.3.37.7. Versão do antivírus instalado na máquina;

1.3.37.8. Se é necessário reiniciar o computador para aplicar mudanças;

1.3.37.9. Data e horário de quando a máquina foi ligada;

1.3.37.10. Quantidade de vírus encontrados (contador) na máquina;

1.3.37.11. Nome do computador;

1.3.37.12. Domínio ou grupo de trabalho do computador;

1.3.37.13. Data e horário da última atualização de vacinas;

1.3.37.14. Sistema operacional com Service Pack;

1.3.37.15. Quantidade de processadores;

1.3.37.16. Quantidade de memória RAM;

1.3.37.17. Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);

1.3.37.18. Endereço IP;

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

1.3.37.20. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

1.3.37.21. Vulnerabilidades de aplicativos instalados na máquina;

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

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

1.3.39.1. Alteração de Gateway Padrão;

1.3.39.2. Alteração de subrede;

1.3.39.3. Alteração de domínio;

1.3.39.4. Alteração de servidor DHCP;

1.3.39.5. Alteração de servidor DNS;
1.3.39.6. Alteração de servidor WINS;
1.3.39.7. Alteração de subrede;
1.3.39.8. Resolução de Nome;
1.3.39.9. Disponibilidade de endereço de conexão SSL;

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

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

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

1.3.43. A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;

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

1.3.45. 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;

1.3.46. 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;

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

1.3.48. Capacidade de monitoramento do sistema através de um SNMP client;

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

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

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

1.3.52. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

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

1.3.54. 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;

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

1.3.56. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;

1.3.57. 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);

1.3.59. 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;

1.3.60. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.3.61. 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.

1.3.62. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

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

1.3.64. Deve criar um backup de todos arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

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

1.3.66. Capacidade de realizar resumo de hardware de cada máquina cliente;

1.3.67. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows 7 Professional/Enterprise/Home SP1 x86 / x64;

2.1.2. Microsoft Windows 8 Professional/Enterprise x86 / x64;

2.1.3. Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
2.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;
2.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education x86 / x64;
2.1.6. Microsoft Windows Server 2022 Essentials / Standard / Datacenter;
2.1.7. Microsoft Windows Server 2019 Essentials / Standard / Datacenter;
2.1.8. Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
2.1.9. Microsoft Windows Server 2012 / 2012 R2 Foundation / Essentials / Standard / Datacenter;
2.1.10. Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;
2.1.11. Microsoft Windows Small Business Server 2011 Standard / Standard x64;
2.1.12. Microsoft Windows MultiPoint Server 2011 x64;

2.2. Características:

2.2.1. Deve prover as seguintes proteções:
2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
2.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
2.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
2.2.1.5. Firewall com IDS;
2.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
2.2.1.7. Controle de dispositivos externos;
2.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
2.2.1.9. Controle de acesso a sites por horário;
2.2.1.10. Controle de acesso a sites por usuários;
2.2.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
2.2.1.12. Controle de execução de aplicativos;
2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
2.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
2.2.3. 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);

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

2.2.5. 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;

2.2.6. 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;

2.2.7. Deverá possuir módulo dedicado para proteção contra port scanning;

2.2.8. Deverá possuir módulo dedicado para proteção contra network flooding;

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

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

2.2.11. 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;

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

2.2.13. Ao detectar uma ameaça, a solução deve exibir informações:

2.2.13.1. Do objeto SHA256;

2.2.13.2. Do objeto MD5.

2.2.14. Capacidade de verificar somente arquivos novos e alterados;

2.2.15. Capacidade de verificar objetos usando heurística;

2.2.16. Capacidade de agendar uma pausa na verificação;

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

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

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

2.2.19.1. Perguntar o que fazer, ou;

2.2.19.2. Bloquear acesso ao objeto;

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

2.2.19.2.2. Caso positivo de desinfecção:

2.2.19.2.2.1. Restaurar o objeto para uso;

2.2.19.2.3. Caso negativo de desinfecção:

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

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

2.2.21. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

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

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

2.2.24. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

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

2.2.25.1. Perguntar o que fazer, ou;

2.2.25.2. Bloquear o e-mail;

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

2.2.25.2.2. Caso positivo de desinfecção:

2.2.25.2.2.1. Restaurar o e-mail para o usuário;

2.2.25.2.3. Caso negativo de desinfecção:

2.2.25.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.27. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

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

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

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

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

2.2.31.1. Perguntar o que fazer, ou;

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

2.2.31.3. Permitir acesso ao objeto;

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

2.2.32.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.2.32.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;

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

2.2.34. 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;

2.2.37. 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;

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

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

2.2.40. 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;

2.2.41. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

2.2.42. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

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

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

2.2.43.2. 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.

2.2.44. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.2.44.1. Discos de armazenamento locais;

2.2.44.2. Armazenamento removível;

2.2.44.3. Impressoras;

2.2.44.4. CD/DVD;

2.2.44.5. Drives de disquete;

2.2.44.6. Modems;

2.2.44.7. Dispositivos de fita;

2.2.44.8. Dispositivos multifuncionais;

2.2.44.9. Leitores de smart card;

2.2.44.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
2.2.44.11. Wi-Fi;
2.2.44.12. Adaptadores de rede externos;
2.2.44.13. Dispositivos MP3 ou smartphones;
2.2.44.14. Dispositivos Bluetooth;
2.2.44.15. Câmeras e Scanners.

2.2.45. 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;

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

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

2.2.48. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.

2.2.49. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.

2.2.50. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

2.2.51. 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);

2.2.52. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
2.2.52.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
2.2.52.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.53. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.2.54. 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;

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

2.2.56. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
2.2.57. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
2.2.58. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
2.2.59. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
2.2.60. Capacidade de integração com o Windows Defender Security Center.
2.2.61. Capacidade de integração com a Antimalware Scan Interface (AMSI).
2.2.63. Deve permitir sincronização com soluções de terceiros por meio de API.
2.2.64. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

3. Estações Mac OS X

3.1. Compatibilidade:

3.1.1. macOS Catalina 10.15
3.1.2. macOS Mojave 10.14
3.1.3. masOS High Sierra 10.13
3.1.4. macOS Sierra 10.12
3.1.5. macOS 11.0 Big Sur
3.1.6. macOS 12.5 Monterey

3.2. Características:

3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, 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. 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);

3.2.9. Capacidade de voltar para a base de dados de vacina anterior;

3.2.10. 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;

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

3.2.12. 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;

3.2.13. Capacidade de verificar somente arquivos novos e alterados;

3.2.14. Capacidade de verificar objetos usando heurística;

3.2.15. Capacidade de agendar uma pausa na verificação;

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

3.2.16.1. Perguntar o que fazer, ou;

3.2.16.2. Bloquear acesso ao objeto;

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

3.2.16.2.2. Caso positivo de desinfecção:

3.2.16.2.2.1. Restaurar o objeto para uso;

3.2.16.2.3. Caso negativo de desinfecção:

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

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

3.2.18. Capacidade de verificar arquivos de formato de e-mail;

3.2.19. 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;

3.2.20. Capacidade de, através da mesma console central de gerenciamento:

3.2.20.1. Ser instalado;

3.2.20.2. Ser removido;

3.2.20.3. Ser gerenciado;

4. Estações de trabalho Linux

4.1. Compatibilidade:

4.1.1. Plataforma 32-bits:

4.1.1.1. Ubuntu 16.04 LTS;
4.1.1.2. Red Hat® Enterprise Linux® 6.7 Server;
4.1.1.3. CentOS 6.7;
4.1.1.4. Debian GNU / Linux 9.4 ;
4.1.1.5. Debian GNU / Linux 10;
4.1.1.6. Linux Mint 18.2;
4.1.1.7. Linux Mint 19;
4.1.1.8. GosLinux 6.6;
4.1.1.9. Mageia 4;
4.1.1.10. 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. OracleLinux 7.3;
4.1.2.12. OracleLinux 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. GosLinux 6.6
4.1.2.19. GosLinux 7.2
4.1.2.20. Oracle Linux 6.7;
4.1.2.21. SUSE Linux Enterprise Server 12 SP3;
4.1.2.22. Pardus OS 19.1;
4.1.2.23. RED OS 7.2;

4.2. Características:

4.2.1. Deve prover as seguintes proteções:

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

4.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

4.2.3.1. Via linha de comando;

4.2.3.2. Via console administrativa;

4.2.3.3. Via GUI;

4.2.3.4. Via web (remotamente);

4.2.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:

4.2.4.1. CDs;

4.2.4.2. DVDs;

4.2.4.3. Discos blu-ray;

4.2.4.4. Flash drives (pen drives);

4.2.4.5. HDs externos;

4.2.4.6. Disquetes;

4.2.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

4.2.5.1. Por tipo de dispositivo;

4.2.5.2. Por barramento de conexão.

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

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

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

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

4.2.10. 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;

4.2.11. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

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

4.2.12.1. Alta;

4.2.12.2. Média;

4.2.12.3. Baixa;

4.2.12.4. Recomendado;

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

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

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

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

4.2.18. Capacidade de verificar objetos usando heurística;

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

4.2.20. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.

4.2.21. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

4.2.21.1. Detecção de phishing e sites maliciosos;

4.2.21.2. Bloqueio de download de arquivos maliciosos;

4.2.21.3. Bloqueio de adware;

4.2.22. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

4.2.23. Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

4.2.24. Deve possuir módulo de proteção contra criptografia maliciosa.

5. Servidores Windows

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 / DataCenter SP1 ou posterior;

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

5.1.2.5. Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise / DataCenter SP1 ou posterior;

5.1.2.6. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter 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 MultiPoint Server 2012 Standard / Premium;

5.1.2.12. Microsoft Windows MultiPoint Server 2016

5.1.2.13. Windows 10 Enterprise multi-session;

5.1.2.14. Windows 11 Enterprise multi-session;

5.1.2.15. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

5.1.2.16. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

5.1.2.17. Microsoft Windows Server 2012 Core Standard / Datacenter;

5.1.2.18. Microsoft Windows Server 2012 R2 Core Standard / Datacenter;

5.1.2.19. Microsoft Windows Storage Server 2012;

5.1.2.20. Microsoft Windows Storage Server 2012 R2;

5.1.2.21. Microsoft Windows Hyper-V Server 2012;

5.1.2.22. Microsoft Windows Hyper-V Server 2012 R2;

5.1.2.23. Windows Server 2016 Essentials /Standard / Datacenter;

5.1.2.24. Windows Server 2016 Core Standard / Datacenter;

5.1.2.25. Windows Storage Server 2016;

5.1.2.26. Windows Storage Server 2019;

5.1.2.27. Windows Hyper-V Server 2016;

5.1.2.28. Windows Hyper-V Server 2019;

5.1.2.29. Windows Server 2019 Essentials / Standard / Datacenter / Core / Terminal;

5.1.2.30. Windows Server 2022 Essentials / Standard / Datacenter / Core / Terminal;

5.2. Características:

5.2.1. Deve prover as seguintes proteções:

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

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

5.2.1.3. Firewall com IDS;

5.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

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

5.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

5.2.3.1. Via console administrativa;

5.2.3.2. Via web (remotamente);

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

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

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

5.2.5.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

5.2.5.3. Leitura de configurações;

5.2.5.4. Modificação de configurações;

5.2.5.5. Gerenciamento de Backup e Quarentena;

5.2.5.6. Visualização de logs;
5.2.5.7. Gerenciamento de logs;
5.2.5.8. Gerenciamento de ativação da aplicação;
5.2.5.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
5.2.5.10. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

5.2.6. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.2.6.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.2.6.2. 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.

5.2.7. 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;

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

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

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

5.2.11. Deve possuir funcionalidade de análise personalizada de logs do Windows.

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

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

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

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

5.2.16. 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;

5.2.17. 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;

5.2.18. Capacidade de verificar somente arquivos novos e alterados;

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

5.2.20. Capacidade de verificar objetos usando heurística;

5.2.21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

5.2.22. Capacidade de agendar uma pausa na verificação;

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

5.2.23.1. Perguntar o que fazer, ou;

5.2.23.2. Bloquear acesso ao objeto;

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

5.2.23.2.2. Caso positivo de desinfecção:

5.2.23.2.2.1. Restaurar o objeto para uso;

5.2.23.2.3. Caso negativo de desinfecção:

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

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

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

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

5.2.27. Em caso de detecção de sinais de de uma infecção ativa, deve possuir capacidade de, automaticamente:

5.2.27.1. Executar os procedimentos pré-configurados pelo administrador;

5.2.27.2. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

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

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

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

5.2.31. 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.

5.2.32. Deve possuir controle de dispositivos externos.

6. Servidores Linux

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. GosLinux 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. OracleLinux 7.3;

6.1.2.12. OracleLinux 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. GosLinux 6.6
6.1.2.19. GosLinux 7.2

6.2. Características:

6.2.1. Deve prover as seguintes proteções:
6.2.2. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
6.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
6.2.3.1. Via linha de comando;
6.2.3.2. Via console administrativa;
6.2.3.3. Via GUI;
6.2.3.4. Via web;
6.2.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:
6.2.4.1. CDs;
6.2.4.2. DVDs;
6.2.4.3. Discos Blu-ray;
6.2.4.4. Flash drives;
6.2.4.5. HDs externos;
6.2.4.6. Disquetes;
6.2.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:
6.2.5.1. Por tipo de dispositivo;
6.2.5.2. Por barramento de conexão.
6.2.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.2.7. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.2.8. 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;
6.2.9. Gerenciamento de Quarentena: Deve bloquear objetos suspeitos;
6.2.10. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);
6.2.11. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
6.2.12. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.2.13. Capacidade de verificar objetos usando heurística;

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

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

6.2.15.1. Alta;

6.2.15.2. Média;

6.2.15.3. Baixa;

6.2.15.4. Recomendado;

6.2.16. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.

6.2.17. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

6.2.17.1. Detecção de phishing e sites maliciosos;

6.2.17.2. Bloqueio de download de arquivos maliciosos;

6.2.17.3. Bloqueio de adware;

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

6.2.19. Deve possuir módulo de proteção contra criptografia maliciosa.

7. Smartphones e tablets

7.1. Compatibilidade:

7.1.1. Dispositivos com os sistemas operacionais:

7.1.1.1. Android 5.0 – 5.1.1

7.1.1.2. Android 6.0 – 6.0.1

7.1.1.3. Android 7.0 – 7.12

7.1.1.4. Android 8.0 – 8.1

7.1.1.5. Android 9.0

7.1.1.6. Android 10.0

7.1.1.7. Android 11.0

7.1.1.8. Android 12.0

7.2. Características:

7.2.1. Deve prover as seguintes proteções:

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

7.2.1.2. Proteção contra adware e autodialers;

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

7.2.1.4. Arquivos abertos no smartphone;

7.2.1.5. Programas instalados usando a interface do smartphone

7.2.1.6. 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. Capacidade de desativar por política:

7.4.2.1. Wi-fi;

7.4.2.2. Câmera;

7.4.2.3. Bluetooth.

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

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

7.2.7. Deverá ter firewall pessoal (Android);

7.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente;

7.2.9. Capacidade de enviar comandos remotamente de:

7.2.9.1. Localizar;

7.2.9.2. Bloquear.

7.2.10. Capacidade de detectar Root em dispositivos Android;

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

7.2.12. Capacidade de bloquear o acesso a sites phishing ou maliciosos;

7.2.13. Capacidade de configurar White e blacklist de aplicativos;

7.2.14. Capacidade de localizar o dispositivo quando necessário;

7.2.15. Permitir atualização das definições quando estiver em "roaming";

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

7.2.17. Capacidade de agendar uma verificação (Android);

7.2.18. Capacidade de enviar URL de instalação por e-mail;

7.2.19. Capacidade de fazer a instalação através de um link QRCode;

7.2.20. Capacidade de executar as seguintes ações caso a desinfecção falhe (Android):

- Deletar;
- Ignorar;
- Quarentenar;
- Perguntar ao usuário.

8. Gerenciamento de dispositivos móveis (MDM) - Android

8.1. Compatibilidade:

8.1.1. Dispositivos com os sistemas operacionais:

8.1.1.1. Android 5.0 – 5.1.1
8.1.1.2. Android 6.0 – 6.0.1
8.1.1.3. Android 7.0 – 7.12
8.1.1.4. Android 8.0 – 8.1
8.1.1.5. Android 9.0
8.1.1.6. Android 10.0
8.1.1.7. Android 11.0
8.1.1.8. Android 12.0

8.1.2. Softwares de gerência de dispositivos:

8.1.2.1. VMWare AirWatch 9.3;
8.1.2.2. MobileIron 10.0;
8.1.2.3. IBM Maas360 10.68;
8.1.2.4. Microsoft Intune 1908;
8.1.2.5. 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:
8.2.2.1. Sincronização de e-mail;
8.2.2.2. Uso de aplicativos;
8.2.2.3. Senha do usuário;
8.2.2.4. Criptografia de dados;
8.2.2.5. Conexão de mídia removível.
8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
8.2.4. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
8.2.5. Capacidade de desinstalar remotamente o antivírus do dispositivo;
8.2.6. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
8.2.7. Capacidade de sincronizar com Samsung Knox;

9. Gerenciamento de dispositivos móveis (MDM) – iOS

9.1. Compatibilidade:

9.1.1. Dispositivos com os sistemas operacionais:

9.1.1.1. iOS 10.0 – 10.3.3

9.1.1.2. iOS 11.0 – 11.3

9.1.1.3. iOS 12.0

9.1.1.4. iOS 13.0

9.1.1.5. iOS 14.0

9.1.1.6. iOS 15.0

9.2. Características:

9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

9.2.2. Capacidade de ajustar as configurações de:

9.2.2.1. Sincronização de e-mail;

9.2.2.2. Senha do usuário;

9.2.2.3. Criptografia de dados;

9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

9.2.4. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:

9.2.4.1. Link por e-mail;

9.2.4.2. Link por mensagem de texto;

9.2.4.3. QR Code

9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;

10. Criptografia

10.1. Compatibilidade

10.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

10.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

10.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;

10.1.4. Microsoft Windows 8 Enterprise x86/x64;

10.1.5. Microsoft Windows 8 Pro x86/x64;

10.1.6. Microsoft Windows 8.1 Pro x86/x64;

10.1.7. Microsoft Windows 8.1 Enterprise x86/x64;

10.1.8. Microsoft Windows 10 Enterprise x86/x64;
10.1.9. Microsoft Windows 10 Pro x86/x64;
10.1.10. Microsoft Windows 11 Enterprise x86/x64;
10.1.11. Microsoft Windows 11 Pro x86/x64;

10.2. Características

10.2.1. 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;
10.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
10.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
10.2.4. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;
10.2.5. Permitir criar vários usuários de autenticação pré-boot;
10.2.6. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;
10.2.7. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
10.2.8. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
10.2.8.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
10.2.8.2. Criptografar todos os arquivos individualmente;
10.2.8.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
10.2.8.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
10.2.9. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente.
10.2.10. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
10.2.11. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
10.2.12. Verifica compatibilidade de hardware antes de aplicar a criptografia;
10.2.13. Possibilita estabelecer parâmetros para a senha de criptografia;
10.2.14. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

10.2.15. Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo
10.2.16. Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook";
10.2.17. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
10.2.18. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
10.2.19. Permite criar um grupo de extensões de arquivos a serem criptografados;
10.2.20. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
10.2.21. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
10.2.22. Capacidade de deletar arquivos de forma segura após a criptografia;
10.2.23. Capacidade de criptografar somente o espaço em disco utilizado;
10.2.24. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
10.2.25. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
10.2.26. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
10.2.27. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
10.2.28. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
10.2.29. Capacidade de fazer "Hardware encryption";

11. Gerenciamento de Sistemas

11.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;
11.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
11.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
11.4. 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;
11.5. Capacidade de gerenciar licenças de softwares de terceiros;

11.6. Capacidade de atualizar informações sobre hardware presente nos relatórios após mudanças de hardware nas máquinas gerenciadas;
11.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc);
11.8. Possibilita fazer distribuição de software de forma manual e agendada;
11.9. Suporta modo de instalação silenciosa;
11.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
11.11. Possibilita fazer a distribuição através de agentes de atualização;
11.12. Utiliza tecnologia multicast para evitar tráfego na rede;
11.13. Possibilita criar um inventário centralizado de imagens;
11.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
11.15. Suporte a WakeOnLan para deploy de imagens;
11.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
11.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
11.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
11.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
11.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
11.21. Permite baixar atualizações para o computador sem efetuar a instalação
11.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
11.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
11.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
11.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
11.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
11.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
11.28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
11.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

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

12. Detecção e Resposta

12.1. Compatibilidade

12.1.1. Windows 7 SP1 Home / Professional / Enterprise 32-bit / 64-bit
12.1.2. Windows 8.1.1 Professional / Enterprise 32-bit / 64-bit
12.1.3. Windows 10 RS3 (version 1703) Home / Professional / Education / Enterprise 32-bit / 64-bit
12.1.4. Windows 10 RS4 (version 1803) Home / Professional / Education / Enterprise 32-bit / 64-bit
12.1.5. Windows 10 RS5 (version 1809) Home / Professional / Education / Enterprise 32-bit / 64-bit
12.1.6. Windows 10 RS6 (version 1903) Home / Professional / Education / Enterprise 32-bit / 64-bit
12.1.7. Windows 10 19H2 (version 1909) Home / Professional / Education / Enterprise 32-bit / 64-bit
12.1.8. Windows 10 20H1 (version 2004) Home / Professional / Education / Enterprise 32-bit / 64-bit
12.1.9. Windows 11 Home / Professional / Education / Enterprise 32-bit / 64-bit
12.1.10. Windows Server 2008 R2 Foundation / Standard / Enterprise 64-bit
12.1.11. Windows Server 2012 Foundation / Standard / Enterprise 64-bit
12.1.12. Windows Server 2012 R2 Foundation / Standard / Enterprise 64-bit
12.1.13. Windows Server 2016 Essentials / Standard / Datacenter 64-bit
12.1.14. Windows Server 2019 Essentials / Standard / Datacenter 64-bit

12.2. Características

12.2.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;
12.2.2. A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:
12.2.3. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;
12.2.4. Deve fornecer graficamente a visualização da cadeia do ataque;

12.2.5. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

12.2.5.1. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

- Isolar o host;
- Iniciar uma varredura nas áreas críticas;
- Quarentenar o objeto;

12.2.6. Capacidade de integração com a solução de sandbox;

12.2.7. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

12.2.8. Detecções provenientes da solução de endpoint;

12.2.9. Detecções provenientes da solução de sandbox;

12.2.10. Processos;

12.2.11. Alterações de registro;

12.2.12. DLL's

12.2.13. Conexões remotas;

12.2.14. Criação de arquivos;

12.2.15. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

12.2.16. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

12.2.17. A solução deve oferecer no mínimo as seguintes opções de resposta:

- Prevenir a execução de um arquivo;
- Quarentenar um arquivo;
- Iniciar uma varredura por IoC;
- Parar um processo;
- Executar um processo;

12.2.18. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

12.2.19. A opção de isolamento deve estar disponível junto a visualização do incidente;

12.2.20. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

12.2.21. A visualização da cadeia de ataque deve conter informações setorizadas por módulos do incidente.

12.2.22. Deve possuir as seguintes opções de gerenciamento:

12.2.22.1. Via console administrativa;

12.2.22.2. Via interface web;

12.2.22.3. Gerenciamento baseado em nuvem;

12.2.22.4. Gerenciamento via linha de comando.

12.2.23. Deve fornecer a opção de proteger a aplicação por senha.

12.2.24. A opção de proteção por senha deve permitir especificar uma força mínima para a senha da aplicação.

13. Suporte Técnico

13.1. Suporte Técnico do fabricante:

13.1.1. Deverá oferecer serviço relacionado as operações do produto e suas funcionalidades, tão como orientação no caso de infecção.

13.1.2. Deve possibilitar a abertura de chamados de suporte, para no mínimo, os seguintes métodos: via telefone, e-mail e/ou "website";

13.1.3. Deverá disponibilizar portal da web do suporte técnico do fabricante com aceitação de solicitações 24 horas por dia, 365 dias por ano;

13.1.4. Deverá disponibilizar suporte técnico por telefone em horario comercial e em português;

13.1.5. Deverá disponibilizar suporte técnico por telefone 24x7, podendo este ser em inglês fora do horário comercial (9h as 18h);

13.1.6. Deverá ser permitido autorizar até 4 pessoas a abrir chamados diretamente nas centrais de suporte técnico do fabricante;

13.1.7. O tratamento de incidentes, deve ser realizado por um time dedicado de engenheiros sênior, que atuarão como ponto principal de contato, para fornecer assistencia avançada em horario comercial.

13.1.8. O tratamento de incidentes, deve ser realizado por um time dedicado de engenheiros sênior, que atuarão como ponto principal de contato, para fornecer assistencia avançada 24x7 para casos de severidade **nível 1**.

13.1.9. O atendimento do incidente deve incluir acesso remoto a infraestrutura da contratada, caso necessário.

13.1.10. O suporte deverá ter a mesma validade do licenciamento.

13.2. Do SLA de atendimento:

13.2.1. O tempo máximo para início do atendimento a chamados de **nivel 1** é de **2 horas** contados do recebimento da notificação.

13.2.2. O tempo máximo para início do atendimento a chamados de **nivel 2** é de **6 horas**, contados do recebimento da notificação.

13.2.3. O tempo máximo para início do atendimento a chamados de **nivel 3** é de **8 horas**, contados do recebimento da notificação.

13.2.4. O tempo máximo para início do atendimento a chamados de **nivel 4** é de **10 horas**, contados do recebimento da notificação.

13.3. Níveis de severidade do incidente:

13.3.1. **"Nível de Severidade 1"** (crítico) deve significar um problema crítico do Produto, que afeta a continuidade dos negócios do Cliente por interrupções no funcionamento normal do Produto e que faz com que o (s) Produto (s) ou Sistema Operacional falhe, ou que causa perda de dados, alteração das configurações padrão para valores inseguros ou problemas de segurança, desde que não haja solução alternativa disponível.

A lista de incidentes relacionados ao produto, que se referem ao nível de gravidade 1, inclui, mas não está limitada a:

- ✓ toda a rede local (ou sua parte crítica) está inoperante, o que dificulta ou suspende os principais processos de negócios.

13.3.2. **"Nível de Severidade 2"** (alto) significa um problema moderado que afeta a funcionalidade do produto, mas não causacorrupção / perda de dados ou falha de software. O nível de gravidade 1 é reclassificado para o nível de gravidade 2 quando uma solução alternativa é acessível.

A lista de incidentes relacionados ao produto, que se referem ao nível de gravidade 2, inclui, mas não está limitada a:

- ✓ o produto apresenta mau funcionamento ou não funciona, mas a continuidade dos principais processos de negócios não é interrompida.

13.3.3. **"Nível de Severidade 3"** (médio) significa um problema não crítico ou solicitação de serviço, que não afeta a funcionalidade do produto.

A lista de incidentes, que se refere ao nível de gravidade 3, inclui, mas não se limita aos seguintes problemas:

- ✓ o produto está parcialmente fora de serviço (mau funcionamento), mas outros aplicativos utilizados pelo Cliente não estão envolvidos.

13.3.4. **"Nível de Severidade 4"** (baixo) significa outros problemas não críticos ou solicitações de serviço. Todos os incidentes que não satisfazem qualquer um

dos critérios listados acima, referem-se a este nível de gravidade.

14. Implementação

14.1. Implementação assistida:

14.1.1. O fornecedor/fabricante deverá implementar o módulo de controle e administração em no máximo 8 horas com criação de política de implemtação dos clientes de forma agendada para não haver impacto na rede corporativa.

15. Treinamento

15.1. Treinamento com certificação:

15.1.1. O fornecedor/fabricante deverá treinar 4 membros da equipe de TI do SESC-ES com Certificação Oficial.

16. Licenciamento

16.1. Validade:

16.1.1. A validade do Licenciamento deverá ser de 36 meses.