COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

CETESB

DIVISÃO DE SUPRIMENTOS
SETOR DE GESTÃO DE CONTRATOS E CADASTRO DE FORNECEDORES

COTAÇÃO DE PREÇOS Nº 33/2020/326

OBJETO: Cotação de preços para renovação da solução para proteção de estações de trabalho e servidores (EndPoint) – McAfee CTP compreendendo: manutenção, apoio à operação e assistência técnica do tipo preventiva, preditiva e corretiva, compreendendo procedimentos destinados a recolocar e/ou manter em perfeito estado de operação os serviços da plataforma de EndPoint e servidores. 2.250 (duas mil duzentos e cinquenta) licenças de antivírus para desktops-usuários, conforme Planilha de Quantidades e Preços – Anexo "1" e Termo de Referência – Anexo "2".

ENCERRAMENTO: 04/12/2020 às 17:00 hs

CONDIÇÕES GERAIS:

1 - PROPOSTA: Apresentar a proposta de preço de acordo com o disposto nesta Cotação e seus anexos, redigida em português, salvo quanto às expressões técnicas de uso corrente. Devendo estar considerado, além do lucro, todos os custos diretos e indiretos, bem como os encargos, benefícios e despesas indiretas (BDI) e demais despesas de qualquer natureza, relacionadas com a prestação dos serviços.

a) Condição de Pagamento – **30 DDL**

b) **VALIDADE DA PROPOSTA**: A validade da proposta não deverá ser inferior a **60 dias.**

c) **PRAZO**: Prazo de Execução: **12 (doze) meses.**

d) A proposta deverá ter o nome do responsável por sua formulação, bem como os dados cadastrais da empresa, **CNPJ, Razão Social, Endereço, Inscrições Estadual e Municipal e Telefone** para contato.

e) A proposta deverá ser encaminhada em formato.**pdf**, Word.**doc**. ou .Excel **.xls**, por e-mail para: proposta_cetesb@sp.gov.br ou fax: 11 - 3133-3244, até a data e horário de **ENCERRAMENTO**.

CRITÉRIO DE AVALIAÇÃO: A avaliação será feita por **VALOR GLOBAL**

São Paulo, 10 de novembro de 2020.

Eduardo Rodrigues
Fone: 011 - 3133.4185
eduardorodrigues@sp.gov.br

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

CETESB

DIVISÃO DE SUPRIMENTOS
SETOR DE GESTÃO DE CONTRATOS E CADASTRO DE FORNECEDORES

COTAÇÃO DE PREÇOS Nº 33/2020/326

ANEXO "1"
PLANILHA DE QUANTIDADES E PREÇOS

ITEM	COMPOSIÇÃO DO ITEM	QTDE	PREÇO UNITÁRIO	TOTAL
1	LICENÇAS DE ANTIVIRUS – DESKTOPS - USUÁRIOS, COM ATUALIZAÇÃO DE VERSÃO E BASE DE DADOS POR 12 MESES.	**2.250**		
1.2	LICENÇAS DE ANTIVIRUS – SERVIDORES, COM ATUALIZAÇÃO DE VERSÃO E BASE DE DADOS POR 12 MESES	**2.250**		
SUB-TOTAL				
2	SUPORTE TÉCNICO, MANUTENÇÃO DA SOLUÇÃO OFERTADA - PERÍODO DE 12 MESES)	**12**		
VALOR TOTAL				

IMPORTANTE: DEVERÃO CONSTAR NA PLANILHA DE PROPOSTA OS VALORES UNITÁRIOS E TOTAIS.

Data _____/_____/_____

_____

Assinatura com carimbo da empresa

ANEXO "2"

TERMO DE REFERÊNCIA

ESPECIFICAÇÃO TÉCNICA DETALHADA DA SOLUÇÃO

ITEM	DESCRIÇÃO
1	Solução para Proteção de Estações de Trabalho e Servidores – McAfee CTP com gerenciamento remoto
2	Solução para resposta à incidentes – EDR
3	SOC 24x7 – Gerenciamento de solução de Endpoint com ação proativa, preditiva e reativa

ITEM DESCRIÇÃO
1 Solução para Proteção de Estações de Trabalho e Servidores – McAfee CTP com gerenciamento remoto
2 Solução para resposta à incidentes – EDR
3 SOC 24x7 – Gerenciamento de solução de Endpoint com ação proativa, preditiva e reativa

DETALHAMENTO TÉCNICO DOS PRODUTOS:

1. Renovação da Solução para Proteção de Estações de Trabalho e Servidores (EndPoint) - McAfee CTP

1.1. Manutenção, apoio à operação e assistência técnica do tipo preventiva, preditiva e corretiva, compreendendo procedimentos destinados a recolocar e/ou manter em perfeito estado de operação os serviços da plataforma de endpoint e servidores tais como:

1.1.1. Do software destinado ao gerenciamento e repositórios relacionados à plataforma do EndPoint (aplicativos e sistema operacional): desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados. Quanto às atualizações pertinentes aos softwares, entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, "patches", "fixes", "updates", "service-packs", novas "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado.

1.1.2. Durante todo o contrato a Licitante vencedora será responsável por manter a

plataforma de segurança atualizado, bem como monitorar se as definições / políticas estão atualizados e sendo aplicados em conformidade. Esse monitoramento deverá ser 24 x 7.

1.1.3. Procedimentos destinados a prevenir a ocorrência de erros e problemas dos sistemas, de forma proativa, sempre que necessário ou requisitado pela CETESB, a fim de realizar avaliações no parque de endpoints instalados e nos softwares de configuração que gerenciam a solução em uso da CETESB.

1.1.4. As inspeções rotineiras a ser realizadas semanalmente, de forma remota ou presencial (quando necessário) de 2 (duas) horas, por técnico qualificado e certificado pelo fabricante da solução em uso na CETESB, para verificação de eventos de erro, coleta e avaliação de logs, verificação e inspeção visual das condições de funcionamento da solução e limpeza dos equipamentos. Caso haja necessidade de atualização de versão, correção do sistema e melhoria nas configurações baseado em melhores práticas da ferramenta, a CETESB agendará uma data para realização da atividade, sem comprometer as horas das visitas semanais.

1.1.5. A agenda das inspeções técnicas deverá ser controlada por meio de cronograma, com datas e horários a serem previamente definidos pela Licitante Vencedora em conjunto com a equipe técnica da CETESB. Caberá à CETESB aprovar a planilha e controlar o cumprimento da agenda aprovada.

1.1.6. Inclui atendimento remoto e on-site. O atendimento on-site deve ser realizado pela CONTRATADA, caso haja necessidade de intervenção do fabricante, esta deverá ser realizada em conjunto com a Contratada.

1.1.7. Reuniões gerenciais, mensais, para avaliação e acompanhamento dos serviços de manutenção e assistência técnica, em que deverá estar presente o Gestor Técnico responsável pelo contrato.

1.1.8. Após a execução dos procedimentos manutenção e assistência técnica preventiva, a empresa Licitante Vencedora deverá fornecer à CETESB um Relatório de Atividade descrevendo todos os procedimentos efetuados, com base nas especificações e melhores práticas recomendadas pelo fabricante.

1.1.9. A execução dos serviços contratados será realizada de forma indireta por meio de Ordem de Serviço.

1.1.10. A Licitante Vencedora elaborará relatórios, quando solicitado pelo CONTRATANTE dos serviços executados, classificados em “Operação e manutenção preventiva”, “Manutenção corretiva” e “Programação/Configuração”. Além destes itens, a CETESB poderá, mediante informação prévia à contratada, atualizar os itens necessários para a Ordem de Serviço e suas classificações em razão de redefinição ou implantação de novos processos.

1.1.11. As Ordens de Serviços conterão os PRODUTOS e SERVIÇOS a serem entregues, com critérios claros para a sua homologação e aceite;

1.1.12. As definições detalhadas dos serviços, que abrangem procedimentos e metodologias a serem empregadas, de níveis de serviço e descrição de cada um dos serviços constantes do objeto da contratação estão elencados de forma objetiva no

item tabelas de severidade e solução de chamado e nos demais procedimentos descritos neste edital.

1.2. Os serviços de manutenção e assistência técnica / suporte técnico deverão ser prestados 24 (vinte e quatro) horas x 7 (sete) dias por semana e deverá ser realizado em 3 (três) níveis descritos a seguir. A classificação de uma solicitação a um incidente deverá estar de acordo com o estabelecido na tabela abaixo:

TABELA DE SEVERIDADE DE CHAMADO PARA TODOS OS HARDWARES E SOFTWARES		
Severidade	**Descrição**	**Tempo de Início de Atendimento**
Alta	Serviço parado no ambiente de produção.	Em até 2 (duas) horas.
Média	Erros ou problemas reincidentes que impactam o ambiente de produção.	Em até 2 (duas) horas.
Baixa	Problemas confortáveis que não afetem a integridade e funcionalidade do sistema.	Em até 8 (oito) horas.

1.3. Em caso de necessidade e em qualquer classificação de severidade, a critério da Cetesb, deverá ser prestado atendimento “On-Site”. Os serviços “On-Site” deverão iniciar-se em no máximo 02 (duas) horas após confirmação da CETESB ou conforme agendamento a critério da CETESB.

1.4. Após o início do atendimento, o tempo de solução do problema deverá ser de acordo com a Tabela de Solução do Chamado (conforme tabela a seguir), não devendo ultrapassar os prazos estabelecidos para as respectivas severidades, contados a partir da abertura do chamado técnico. Esta tabela identifica o tempo em que o problema deverá ser solucionado, tanto para os hardwares como para os softwares

TABELA DE SOLUÇÃO DO CHAMADO PARA TODOS OS HARDWARES E SOFTWARES		
Severidade	**Descrição**	**Tempo de Solução**
Alta	Serviço parado no ambiente de produção, incluindo reposição de peça defeituosa ou substituição temporária do equipamento.	Em até 4 (quatro) horas da abertura do chamado.
Média	Erros ou problemas reincidentes que impactam o ambiente de produção.	Em até 5 (cinco) horas da abertura do chamado.
Baixa	Problemas confortáveis que não afetem a integridade e funcionalidade do sistema.	Em até 10 (dez) horas da abertura do chamado.

1.5. Características Gerais da Solução
1.5.1. Deve possuir suporte a arquiteturas 32-bits e 64-bits;
1.5.2. Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 3Gb de memória RAM;
1.5.3. Deve suportar as seguintes plataformas clientes:
1.5.3.1. Windows 10;
1.5.3.2. Windows 8.1
1.5.3.3. Windows 8;
1.5.3.4. Windows 7;
1.5.3.5. Sierra 10.12.x
1.5.3.6. El Captain 10.11.x
1.5.4. Deve suportar as seguintes plataformas servidores:
1.5.4.1. Windows Server 2016;
1.5.4.2. Windows Server 2012 R2;
1.5.4.3. Windows Server 2012;
1.5.4.4. Windows Storage Server 2012;
1.5.4.5. Windows 2008 R2 (Standard/Datacenter/Enterprise/Web)
1.5.4.5.1. Deve inclusive suportar o modo Server Core;
1.5.5. Deve suportar, pelo menos a função de antivírus, as seguintes distribuições de Linux:
1.5.5.1. Red Hat Enterprise 5.x e 6.x, 32 e/ou 64bits;
1.5.5.2. SUSE Linux Enterprise Server/Desktop 10.x e 11.x, 32 e/ou 64bits;
1.5.5.3. Ubuntu 10.04, 11.04, 11.10, 12.04, 12.10, 13.04 e 13.10, 32 e/ou 64bits;
1.5.5.4. CentOS 5.x e 6.x, 32 e/ou 64bits;
1.5.5.5. Oracle Linux 5 e 6, 32 e/ou 64bits;
1.5.5.6. Amazon Linux 32 e/ou 64bits;
1.5.6. Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:
1.5.6.1. AWS;
1.5.6.2. Azure;
1.5.6.3. Citrix XenApp;
1.5.6.4. Citrix XenDesktop;
1.5.6.5. Citrix XenServer;
1.5.6.6. Microsoft Hyper-V 2012 R2;
1.5.6.7. Vmware ESXi;
1.5.6.8. Vmware Player;
1.5.6.9. Vmware vShpere;
1.5.6.10. Vmware Workstation;
1.5.7. Deve possuir proteção, pelo menos da funcionalidade de

antivírus, para ambientes de Storage, incluindo:
1.5.7.1. NetApp;
1.5.7.2. EMC;
1.5.7.3. IBM;
1.5.7.4. HP;
1.5.7.5. DELL;
1.5.7.6. Hitachi.
1.5.8. Toda a proteção deverá ser realizada através de um único agente de proteção com as funcionalidades descritas neste termo, não sendo aceitos plugins ou softwares adicionais para a composição do pacote;
1.5.9. O agente único deve compreender as seguintes funcionalidades:
1.5.9.1. Prevenção de Ameaças
1.5.9.2. Firewall
1.5.9.3. Controle Web
1.5.9.4. Inteligência contra Ameaças
1.5.10. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:
1.5.10.1. Relatórios;
1.5.10.2. Dashboards;
1.5.10.3. Políticas;
1.5.10.4. Configuração;
1.5.10.5. Instalação/Desinstalação;
1.5.11. O cliente deve ser capaz de operar em modo autônomo (selfmanaged) e permitir que as configurações sejam aplicadas diretamente no cliente.
1.5.12. O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfix'es a partir de um servidor definido pelo administrador ou diretamente nos servidores da McAfee.
1.5.13. A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente;
1.5.14. A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;
1.5.15. A solução deve conter módulo capaz de proteger contra botnets, negação de serviço, executáveis não confiáveis e conexões web maliciosas;
1.5.16. A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)
1.5.17. A solução deve conter módulo capaz de garantir integração entre as soluções do fabricante proposto e entre fabricantes

terceiros, compartilhando as informações do paciente dia zero para melhor mitigar novas ameaças.
1.5.17.1. Este módulo deve estar público para o desenvolvimento da comunidade via Github;

1.6. Proteção Clientes Windows

1.6.1. O módulo de proteção contra ameaças deve incluir, no mínimo, os seguintes componentes:
1.6.1.1. **Prevenção de exploração:**
1.6.1.1.1. Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).
1.6.1.1.2. Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.
1.6.1.1.3. Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.
1.6.1.1.4. Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;
1.6.1.1.5. Deve ser possível bloquear contra falsificação de IP (IP Spoofing)
1.6.1.1.6. Deve ser possível incluir exclusões por:
1.6.1.1.6.1. Processo
1.6.1.1.6.1.1. Nome;
1.6.1.1.6.1.2. Caminho do Arquivo;
1.6.1.1.6.1.3. Hash MD5
1.6.1.1.6.2. Módulo chamador:
1.6.1.1.6.2.1. Nome
1.6.1.1.6.2.2. Caminho
1.6.1.1.6.2.3. Hash MD5
1.6.1.1.6.2.4. Signatário Digital
1.6.1.2. **Proteção de acesso**
1.6.1.2.1. Deve fornecer regras de proteção nativamente, ou seja definida pelo fabricante da solução, no mínimo, para:
1.6.1.2.1.1. Acesso remoto a pastas locais;
1.6.1.2.1.2. Alteração políticas de direitos dos usuários;
1.6.1.2.1.3. Alterar os registros de extensão dos arquivos;
1.6.1.2.1.4. Criação de novos arquivos na pasta Arquivo de Programas;
1.6.1.2.1.5. Criação de novos executáveis na pasta Windows;
1.6.1.2.1.6. Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema;
1.6.1.2.1.7. Criar ou Modificar remotamente arquivos ou pastas;
1.6.1.2.1.8. Desativar o editor de registro e o gerenciador de tarefas;

1.6.1.2.1.9. Executar arquivos das pastas do usuário;
1.6.1.2.1.10. Execução de scripts pelo host de script do Windows;
1.6.1.2.1.11. Instalar objetos de ajuda a navegação ou extensões de shell;
1.6.1.2.1.12. Instalar novos CLSIDs, APPIDs e TYPELIBs;
1.6.1.2.1.13. Modificar configurações de rede;
1.6.1.2.1.14. Modificar configurações do Internet Explorer;
1.6.1.2.1.15. Modificar processos principais do Windows;
1.6.1.2.1.16. Navegadores iniciando programas da pasta de downloads;
1.6.1.2.1.17. Registrar programas para execução automática;
1.6.1.2.2. As regras especificadas devem permitir o seu:
1.6.1.2.2.1. Bloqueio, ou
1.6.1.2.2.2. Informação, ou
1.6.1.2.2.3. Bloqueio e Informação;
1.6.1.2.3. Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parametros:
1.6.1.2.3.1. Processos;
1.6.1.2.3.1.1. Nome do processo;
1.6.1.2.3.1.2. Hash MD5;
1.6.1.2.3.1.3. Assinatura Digital;
1.6.1.2.3.2. Usuário
1.6.1.2.3.3. Arquivos;
1.6.1.2.3.3.1. Criação;
1.6.1.2.3.3.2. Deletar;
1.6.1.2.3.3.3. Executar;
1.6.1.2.3.3.4. Alteração de permissão;
1.6.1.2.3.3.5. Leitura;
1.6.1.2.3.3.6. Renomear;
1.6.1.2.3.3.7. Escrever;
1.6.1.2.3.4. Chave de Registro
1.6.1.2.3.4.1. Escrever;
1.6.1.2.3.4.2. Criar;
1.6.1.2.3.4.3. Deletar;
1.6.1.2.3.4.4. Ler;
1.6.1.2.3.4.5. Enumerar;
1.6.1.2.3.4.6. Carregar;
1.6.1.2.3.4.7. Substituir;
1.6.1.2.3.4.8. Restaurar;
1.6.1.2.3.4.9. Alterar permissão;
1.6.1.2.3.5. Valor de Registro
1.6.1.2.3.5.1. Ler;

1.6.1.2.3.5.2. Criar;
1.6.1.2.3.5.3. Deletar;
1.6.1.2.3.6. Processo
1.6.1.2.3.6.1. Qualquer acesso;
1.6.1.2.3.6.2. Criar thread;
1.6.1.2.3.6.3. Modificar;
1.6.1.2.3.6.4. Terminar;
1.6.1.2.3.6.5. Executar;
1.6.1.2.4. Deve permitir a criação de exclusões;
1.6.1.3. **Varredura ao acessar;**
1.6.1.3.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;
1.6.1.3.2. Deve iniciar a proteção durante a inicialização do sistema operacional;
1.6.1.3.3. Deve ser capaz de realizar análise no setor de boot;
1.6.1.3.4. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;
1.6.1.3.5. Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo;
1.6.1.3.6. Deve possibilitar ao administrador a análise de instaladores confiáveis;
1.6.1.3.7. Deve realizar análise durante cópia entre pastas locais;
1.6.1.3.8. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;
1.6.1.3.8.1. Deve permitir a configuração do nível de agressividade da análise entre:
1.6.1.3.8.1.1. Muito Baixo
1.6.1.3.8.1.2. Baixo
1.6.1.3.8.1.3. Médio
1.6.1.3.8.1.4. Alto
1.6.1.3.8.1.5. Muito Alto
1.6.1.3.9. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;
1.6.1.3.10. Deve realizar varredura quando o processo:
1.6.1.3.10.1. Ler o disco;
1.6.1.3.10.2. Gravar no disco;
1.6.1.3.10.3. Deixar a solução de proteção decidir;
1.6.1.3.11. Deve possibilitar análise em
1.6.1.3.11.1. Unidades de Rede;

1.6.1.3.11.2. Arquivos abertos para backup;
1.6.1.3.11.3. Arquivos compactados, por exemplo .jar;
1.6.1.3.11.4. Arquivos codificados (MIME)
1.6.1.3.12. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;
1.6.1.3.13. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
1.6.1.3.13.1. Limpar o arquivo;
1.6.1.3.13.2. Excluir o arquivo;
1.6.1.3.13.3. Negar acesso ao arquivo;
1.6.1.3.14. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
1.6.1.3.14.1. Limpar o arquivo;
1.6.1.3.14.2. Excluir o arquivo;
1.6.1.3.14.3. Permitir acesso ao arquivo;
1.6.1.3.14.4. Negar acesso ao arquivo;
1.6.1.3.15. Deve possibilitar ao administrador a gestão de uma lista de exclusões;
1.6.1.3.16. Deve possuir módulo capaz de interceptar scripts (Javascript e VBScript) destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;
1.6.1.3.16.1. Deve permitir a criação de listas de exclusão de URL's que não sofrerão interceptação e análise de scripts;
1.6.1.3.17. Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.
1.6.1.4. **Varredura sob demanda;**
1.6.1.4.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.
1.6.1.4.1.1. Deve permitir a criação de repetição da tarefa.
1.6.1.4.1.2. Deve permitir definir a hora da execução da tarefa de análise;
1.6.1.4.1.3. Deve permitir a criação da tarefa de varredura de maneira aleatória;
1.6.1.4.2. Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.
1.6.1.4.3. Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:
1.6.1.4.3.1. Os locais da varredura, dentre eles:
1.6.1.4.3.1.1. Memória para rootkits;

1.6.1.4.3.1.2. Processos em execução;
1.6.1.4.3.1.3. Arquivos registrados;
1.6.1.4.3.1.4. Meu computador;
1.6.1.4.3.1.5. Todas as unidades locais;
1.6.1.4.3.1.6. Todas as unidades fixas;
1.6.1.4.3.1.7. Todas as unidades removíveis;
1.6.1.4.3.1.8. Todas as unidades mapeadas;
1.6.1.4.3.1.9. Pasta inicial;
1.6.1.4.3.1.10. Pasta de perfil do usuário;
1.6.1.4.3.1.11. Pasta Windows;
1.6.1.4.3.1.12. Pasta de arquivos de programas;
1.6.1.4.3.1.13. Pasta temporária;
1.6.1.4.3.1.14. Lixeira;
1.6.1.4.3.1.15. Arquivo ou pasta especificada pelo administrador;
1.6.1.4.3.1.16. Setor de inicialização (boot);
1.6.1.4.3.1.17. Arquivos compactados;
1.6.1.4.3.1.18. Arquivos MIME;
1.6.1.4.3.2. Os tipos de arquivos que serão analisados;
1.6.1.4.3.3. Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.
1.6.1.4.3.4. Áreas de exclusão que não deverão ser varridas;
1.6.1.4.4. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada.
1.6.1.4.5. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
1.6.1.4.5.1. Limpar o arquivo;
1.6.1.4.5.2. Excluir o arquivo;
1.6.1.4.5.3. Negar acesso ao arquivo;
1.6.1.4.6. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
1.6.1.4.6.1. Limpar o arquivo;
1.6.1.4.6.2. Excluir o arquivo;
1.6.1.4.6.3. Permitir acesso ao arquivo;
1.6.1.4.6.4. Negar acesso ao arquivo;
1.6.1.4.7. Para minimizar o impacto ao usuário, a solução deve permitir:
1.6.1.4.7.1. Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;
1.6.1.4.7.2. Iniciar a varredura apenas quando o sistema estiver ocioso;

1.6.1.4.7.3. Permitir ao usuário retomar varreduras pausadas;
1.6.1.4.8. Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;
1.7. O módulo de Firewall deve incluir as seguintes capacidades:
1.7.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;
1.7.2. Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura contra ataques dia zero;
1.7.3. Deve possuir um firewall de estação statefull bloqueando tráfego de entrada e controlando o tráfego de saída;
1.7.4. Deve possuir assinaturas de proteção para:
1.7.4.1. Arquivos
1.7.4.2. Chave de Registro
1.7.4.3. Processos
1.7.4.4. Serviços;
1.7.5. Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;
1.7.6. Deve ser possível bloquear trafego bridge;
1.7.7. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;
1.7.8. Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;
1.7.9. Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações:
1.7.9.1. Nome
1.7.9.2. Nome do arquivo ou Caminho;
1.7.9.3. Hash MD5
1.7.9.4. Assinador Digital
1.7.10. Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;
1.7.10.1. As conexões identificadas pelo Centro de Inteligência podem ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.
1.7.11. Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;
1.7.12. Deve permitir inspeção do protocolo FTP;
1.7.13. Deve ser possível bloquear trafego de protocolos não suportados;
1.7.14. O módulo de Firewall deve vir com regras pré-indicadas pelo

próprio fabricante.
1.7.15. O módulo de firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:
1.7.15.1. Ação
1.7.15.1.1. Bloquear
1.7.15.1.2. Permitir
1.7.15.2. Direção
1.7.15.2.1. Ambas
1.7.15.2.2. Entrada
1.7.15.2.3. Saída
1.7.15.3. Protocolo
1.7.15.3.1. Qualquer protocolo
1.7.15.3.2. Protocolo IP
1.7.15.3.2.1. Ipv4
1.7.15.3.2.2. Ipv6
1.7.15.3.2.3. Protocolo Não-IP
1.7.15.3.3. Tipo de Conexão
1.7.15.3.3.1. Rede Sem Fio
1.7.15.3.3.2. Rede Cabeada
1.7.15.3.3.3. Rede Virtual
1.7.15.3.4. Especificação da Rede
1.7.15.3.4.1. Endereço IP
1.7.15.3.4.2. Subnet
1.7.15.3.4.3. Range
1.7.15.3.4.4. FQDN
1.7.15.3.5. Protocolo de Transporte
1.7.15.3.5.1. Todos
1.7.15.3.5.2. ICMP
1.7.15.3.5.3. ICMPv6
1.7.15.3.5.4. TCP
1.7.15.3.5.5. UDP
1.7.15.3.5.6. STP
1.7.15.3.5.7. GRE
1.7.15.3.5.8. IGMP
1.7.15.3.5.9. IPSEC AH
1.7.15.3.5.10. IPSEC ESP
1.7.15.3.5.11. Ipv6 in Ipv4
1.7.15.3.5.12. ISIS over Ipv4
1.7.15.3.5.13. L2TP
1.7.15.3.6. Agendamento
1.7.15.3.6.1. Dias da Semana
1.7.15.3.6.2. Hora Inicio

1.7.15.3.6.3. Hora Fim
1.7.15.3.7. Aplicações
1.8. O modulo de Controle Web deve possuir as seguintes funcionalidades:
1.8.1. Deve permitir o bloqueio de browsers não suportados, dentre eles:
1.8.1.1. Opera
1.8.1.2. Safari for Windows;
1.8.1.3. Netscape
1.8.1.4. Maxthon
1.8.1.5. Flock;
1.8.1.6. Avant Browser;
1.8.1.7. Deepnet Explorer
1.8.1.8. PhaseOut
1.8.2. Deve permitir o controle de browsers suportados, dentre eles:
1.8.2.1. Chrome
1.8.2.2. Firefox
1.8.2.3. Internet Explorer
1.8.3. Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado.
1.8.4. Deve possuir, no mínimo, as seguintes categorias:
1.8.4.1. Browser Exploits;
1.8.4.2. Download Maliciosos;
1.8.4.3. Sites Maliciosos;
1.8.4.4. Phishing;
1.8.4.5. Pornografia;
1.8.4.6. Hacking/Computer Crime;
1.8.4.7. Spyware/Adware/Keyloggers;
1.8.4.8. Anonymizer;
1.8.4.9. Anonymizer Utilities;
1.8.4.10. Alcohol;
1.8.4.11. Blogs/Wiki;
1.8.4.12. Business;
1.8.4.13. Chat;
1.8.4.14. Content Server;
1.8.4.15. Dating
1.8.4.16. Dating/Social Networking
1.8.4.17. Digital Postcards
1.8.4.18. Discrimination;
1.8.4.19. Drugs;
1.8.4.20. Education;
1.8.4.21. Entertainment;

1.8.4.22. Extreme
1.8.4.23. Fashion
1.8.4.24. Finance
1.8.4.25. For Kids
1.8.4.26. Forum
1.8.4.27. Gambling
1.8.4.28. Game/Cartoon Violence
1.8.4.29. Games
1.8.4.30. General News
1.8.4.31. Government/Military
1.8.4.32. Gruesome Content
1.8.4.33. Health
1.8.4.34. Historical Revisionism
1.8.4.35. History
1.8.4.36. Humor/Comics
1.8.4.37. Illegal UK
1.8.4.38. Incidental Nudity
1.8.4.39. Information Security
1.8.4.40. Instant Messaging
1.8.4.41. Interactive Web Applications
1.8.4.42. Internet Radio/TV
1.8.4.43. Internet Services
1.8.4.44. Job Search
1.8.4.45. Major Global Religions
1.8.4.46. Marketing/Merchandising
1.8.4.47. Media Downloads
1.8.4.48. Media Sharing
1.8.4.49. Messaging
1.8.4.50. Mobile Phone
1.8.4.51. Moderated
1.8.4.52. Motor Vehicles
1.8.4.53. Non-Profit/Advocacy/NGO
1.8.4.54. Nudity
1.8.4.55. Online Shopping
1.8.4.56. P2P/File Sharing
1.8.4.57. Parked Domain
1.8.4.58. Personal Network Storage
1.8.4.59. Personal Pages
1.8.4.60. Pharmacy
1.8.4.61. Politics/Opinion
1.8.4.62. Portal Sites
1.8.4.63. Potential Criminal Activities

1.8.4.64. Potential Illegal Software
1.8.4.65. Potentially Unwanted Programs
1.8.4.66. Profanity
1.8.4.67. Professional Networking
1.8.4.68. Provocative Attire
1.8.4.69. Public Information
1.8.4.70. Real Estate
1.8.4.71. Recreation/Hobbies
1.8.4.72. Religion/Ideology
1.8.4.73. Remote Access
1.8.4.74. Residential IP Addresses
1.8.4.75. Resource Sharing
1.8.4.76. Restaurants
1.8.4.77. School Cheating Information
1.8.4.78. Search Engines
1.8.4.79. Sexual Materials
1.8.4.80. Shareware/Freeware
1.8.4.81. Social Networking
1.8.4.82. Software/Hardware
1.8.4.83. Spam URLs
1.8.4.84. Sports
1.8.4.85. Stock Trading
1.8.4.86. Streaming Media
1.8.4.87. Technical Information
1.8.4.88. Technical/Business Forums
1.8.4.89. Text Translators
1.8.4.90. Text/Spoken Only
1.8.4.91. Tobacco
1.8.4.92. Travel
1.8.4.93. Uncategorized
1.8.4.94. Usenet News
1.8.4.95. Violence
1.8.4.96. Visual Search Engine
1.8.4.97. Weapons
1.8.4.98. Web Ads
1.8.4.99. Web Mail
1.8.4.100. Web Meetings
1.8.4.101. Web Phone

1.8.5. Deve ser possível bloquear um site conforme a sua classificação:
1.8.5.1. Vermelho: Alto Risco
1.8.5.2. Amarelo: Médio Risco

1.8.5.3. Cinza: Não categorizado
1.8.6. Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;
1.8.7. Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;
1.8.8. Deve permitir a varredura de arquivos baixados da internet;
1.8.9. Deve ser possível excluir endereços IP da análise;
1.8.10. Deve permitir a busca segura para buscadores, dentre eles:
1.8.10.1. Google;
1.8.10.2. Yahoo
1.8.10.3. Bing;
1.8.10.4. Ask;
1.8.11. Deve bloquear links que direcionem para sites com alto risco.
1.8.12. Deve permitir a customização das mensagens apresentadas para o usuário;
1.8.13. Caso o módulo detecte que exista um McAfee Web Gateway na rede, deverá deixar a análise a cargo deste último.
1.9. O módulo de proteção contra ameaças avançadas deve conter os seguintes mecanismos:
1.9.1. Confinamento dinâmico de aplicações:
1.9.1.1. A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware)
1.9.1.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;
1.9.1.3. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico
1.9.1.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada
1.9.1.5. Solução deve manter um cache de reputação local com informações de aplicações – conhecidas, desconhecidas e maliciosas.
1.9.1.6. Dentre os comportamentos maliciosos, deve ser capaz de:
1.9.1.6.1. Bloquear acesso local a partir de cookies;
1.9.1.6.2. Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs
1.9.1.6.3. Criação de arquivos em qualquer local de rede
1.9.1.6.4. Criação de novos CLSIDs, APPIDs e TYPELIBs
1.9.1.6.5. Criação de threads em outro processo
1.9.1.6.6. Bloquear a desativação de executáveis críticos do sistema operacional

1.9.1.6.7. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares
1.9.1.6.8. Gravação e Leitura na memória de outro processo
1.9.1.6.9. Bloqueio de Modificação da política de firewall do windows
1.9.1.6.10. Bloqueio de Modificação da pasta de tarefas do Windows
1.9.1.6.11. Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro
1.9.1.6.12. Bloqueio de Modíficação de arquivos executáveis portáteis;
1.9.1.6.13. Bloqueio de Modificação de bit de atributo oculto
1.9.1.6.14. Bloqueio de Modificação de bit de atributo somente leitura
1.9.1.6.15. Bloqueio de Modificação de entradas de registro de DLL AppInit;
1.9.1.6.16. Bloqueio de Modificação de locais do registro de inicialização
1.9.1.6.17. Bloqueio de Modificação de pastas de dados de usuários;
1.9.1.6.18. Bloqueio de Modificação do local do Registro de Serviços
1.9.1.6.19. Bloqueio de Suspensão de um processo
1.9.1.6.20. Bloqueio de Término de outro processo
1.9.1.7. Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.
1.9.1.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada.
1.9.1.9. O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;
1.9.1.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário
1.9.2. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção
1.9.3. Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de "machine-learning";
1.10. O módulo de inteligência contra ameaças deve conter os seguintes mecanismos:
Solução de Base de Dados Local de Ameaças
1.10.1. Da Arquitetura

1.10.1.1. A solução deve ser compreendida nos seguintes módulos:
1.10.1.1.1. Servidor de Orquestração e Base de Dados
1.10.1.1.2. Agentes
1.10.1.2. O servidor de orquestração deverá habilitar a troca de informação de ameaças entre os itens propostos neste edital, compreendendo:
1.10.1.2.1. Solução de Proteção de Endpoints
1.10.1.2.2. Solução para análise de malwares dia zero
1.10.1.3. A instalação do componente central deverá habilitar um protocolo de troca de informações de ameaças que permita o intercambio de informações entre soluções do mesmo fabricante e de fabricantes terceiros;
1.10.1.4. A troca de informação de ameaças deve ser dar por meio de protocolo performático;
1.10.1.5. O servidor de orquestração deve permitir a instalação em modo centralizado ou em modo descentralizado, permitindo que localidades remotas possuam um servidor local;
1.10.1.6. De forma a permitir menor impacto na rede, para tal o método de consulta dos clientes a base de dados poderá ser síncrona ou assíncrona;

1.10.2. Da Solução

1.10.2.1. A solução deve possuir capacidade de criar uma reputação local através da catalogação de todos os executáveis existentes no ambiente;
1.10.2.2. A solução deverá apresentar a reputação definida para cada um dos ativos conectados, dentre eles:
1.10.2.2.1. Reputaçao Local
1.10.2.2.2. Reputação do Analisador de Malware dia Zero
1.10.2.2.3. Reputação do Filtro de Conteúdo Web
1.10.2.2.4. Reputação do Centro de Inteligência
1.10.2.3. A solução deve possuir capacidade de criar uma reputação local através da catalogação de todos os executáveis existentes no ambiente;
1.10.2.4. Ao catalogar um arquivo, a solução deve apresentar, no mínimo, as seguintes informações sobre o mesmo:
1.10.2.4.1. Nome do arquivo
1.10.2.4.2. Caminho do arquivo
1.10.2.4.3. Hash SHA-1
1.10.2.4.4. Hash MD5
1.10.2.4.5. Hash 256
1.10.2.4.6. Primeira visualização do arquivo na rede
1.10.2.4.7. Última visualização do arquivo na rede

1.10.2.4.8. Tamanho do arquivo
1.10.2.4.9. Data de compilação
1.10.2.4.10. Se o mesmo consta no Adicionar/Remover Programas
1.10.2.4.11. Se está registrado como serviço
1.10.2.4.12. Se está registrado para ser executado automaticamente
1.10.2.4.13. Tipo de compactador
1.10.2.4.14. Se é arquivo do sistema
1.10.2.4.15. Se foi executado a partir do cmd.exe
1.10.2.4.16. Se tem entrada no menu iniciar
1.10.2.4.17. Se foi executado a partir de uma mídia removível
1.10.2.4.18. Se foi executado a partir da raiz da unidade do sistema
1.10.2.4.19. Caso o arquivo tenha como origem a Internet, a solução deverá ser capaz de informar a partir de qual URL o arquivo foi obtido e a reputação desta última;
1.10.2.5. Deve ser possível realizar uma pesquisa do arquivo em base de conhecimento de terceiros (Exemplo: VirusTotal);
1.10.2.6. Após análise o administrador deve ter a possibilidade de:
1.10.2.6.1. Rastrear em quais estações o arquivo foi executado;
1.10.2.6.2. Identificar o país de origem do arquivo;
1.10.2.6.3. Identificar o arquivo como confiável;
1.10.2.6.4. Identificar o arquivo como desconhecido;
1.10.2.6.5. Identificar o arquivo como malicioso
1.10.2.7. Deve ser capaz de analisar o certificado associado ao arquivo;
1.10.2.8. Deve ser capaz de identificar o certificado associado como confiável ou malicioso;
1.10.2.9. Para minimizar o impacto a solução deve ter a capacidade de ser ativada no modo de observação;
1.10.2.10. Deve ser possível configurar o limiar mínimo para bloqueio de arquivos, variando entre:
1.10.2.10.1. Malicioso
1.10.2.10.2. Provavelmente malicioso;
1.10.2.10.3. Desconhecido
1.10.2.11. Deve ser possível bloquear a execução de arquivos nunca antes visto no ambiente e informar o usuário por meio de mensagem customizada em Português.
1.10.2.12. Caso a solução detecte arquivos não verificados pela solução de análise de dia zero, esta deverá ser capaz de enviar os arquivos de maneira automática para análise.

1.10.2.13. Deve ser capaz de identificar manualmente um arquivo como malicioso impedindo sua execução no ambiente;
1.10.2.14. Deve ser gerenciado pela mesma console proposta na Solução de Proteção de Endpoints.
1.11. Módulo de Proteção de Email
1.11.1. Servidores Microsoft Exchange Server
1.11.2. Compatíveis com as plataformas Windows 2008 e Windows 2012
1.11.3. Suporte a exchange 2007 SP2 ou superior, Exchange 2010 SP2 ou superior e Exchange 2013
1.11.4. Rastreamento em tempo real, para arquivos anexados a mensagens do Exchange, antes de entregar a mensagem na caixa postal do(s) destinatário(s), com as seguintes opções:
1.11.4.1. Limpar o arquivo infectado e entregá-lo limpo para o(s) destinatário(s);
1.11.4.2. Gravar o arquivo infectado na área de segurança (quarentena) e não entregá-lo para o(s) destinatário(s);
1.11.4.3. Gerar notificações e alertas e entregar o arquivo para o(s) destinatário(s)
1.11.5. Rastreamento manual às pastas do Exchange, com opção de limpeza.
1.11.6. Programação de rastreamentos automáticos do Exchange com as seguintes opções:
1.11.6.1. Escopo: Todas as pastas locais, ou pastas específicas
1.11.6.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena)
1.11.6.3. Frequência: Horária, diária, semanal, mensal
1.11.7. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional
1.11.8. Gerar notificações de eventos de vírus através de mensagens do Exchange para quem enviou e quem recebeu a mensagem, e para um Administrador (usuário opcional)
1.11.9. Identificação de remetente e destinatário das mensagens
1.11.10. Permitir bloqueios baseados nos seguintes critérios:
1.11.10.1. Tipo de arquivo;
1.11.10.2. Nome do arquivo;
1.11.10.3. Tamanho do arquivo;
1.11.11. Permitir a instalação em ambientes em Cluster Microsoft
1.11.12. Capacidade de filtragem de conteúdo por categorias como: Sexo, Drogas, entre outros;
Módulo de Controle de Dispositivos

1.11.13. Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, Ipods, Dispositivos Bluetooth, DVDs, e CDS regraváveis;
1.11.14. Deve permitir a configuração dos dispositivos nos modos:
1.11.14.1. Bloqueio, ou;
1.11.14.2. Somente Leitura;
1.11.15. Deve classificar os dispositivos removíveis em 3 categorias:
1.11.15.1. Gerenciado;
1.11.15.2. Ingerenciável (Exemplo: Bateria de Notebooks);
1.11.15.3. Não Gerenciado;
1.11.16. Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:
1.11.16.1. Tipo de BUS;
1.11.16.2. Classe do Dispotivo (Device Class)
1.11.16.3. ID do fabricante (Vendor ID)
1.11.16.4. ID do produto (Product ID)
1.11.17. Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:
1.11.17.1. Tipo de BUS
1.11.17.2. Se o sistema de arquivo é passível de escrita;
1.11.17.3. Se o sitema de arquivo é somente leitura;
1.11.17.4. Tipo de Sistema de Arquivo
1.11.17.5. Nome do Sistema de Arquivo;
1.11.17.6. Número de Série do Sistema de Arquivo;
1.11.18. Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado a rede do órgão libera o uso de pen-drive);
1.12. Módulo de Controle de Aplicações
1.12.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas, aplicar o controle de execução imposto pela política e realizar controle e auditoria sobre as alterações realizadas pelos usuários;
1.12.2. Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes.
1.12.3. Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão;
1.12.4. Ao detectar um executável, a solução deverá consultar o Centro de Inteligência do fabricante e esta deverá informar um nível de confidência (Bom, Mau ou Não Classificado);
1.12.5. Deve ser possível criar uma imagem base para a criação de uma

política geral;
1.12.6. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;
1.12.7. A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos;
1.12.8. Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:
1.12.8.1. Desabilitado: proteção desativada
1.12.8.2. Monitoramento: Monitora toda a atividade da Estação de Trabalho;
1.12.8.3. Atualização: a cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido;
1.12.9. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA-1).
1.12.10. A solução deve suportar as seguintes modalidades de proteção:
1.12.10.1. **Application Whitelisting:** criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impadidas de serem executadas.
1.12.10.2. **Application Blocking / Blacklisting:** criação de uma lista de aplicações não autorizadas que não podem ser executadas.
1.12.10.3. **Memory Protection:** monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.
1.12.11. Solução suporta criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.
1.12.12. Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação do aplicativo ou arquivo.
1.12.13. Suporta os mecanismos:
1.12.13.1. Application Code Protection: permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, etc) possam ser executados. Além disso, permite proteção contra adulterações de programas em Whitelist (ex.: arquivos do programa) e, opcionalmente, chaves de registros contra modificações em disco.
1.12.13.2. Memory Protection: permite proteção contra ataques e exploração de vulnerabilidades para os programas em

Whitelist.
1.12.14. Suporta criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de Whitelist, através de:
1.12.14.1. **Binário:** binário específico identificado através de seu nome ou de algorítmo de verificação SHA-1.
1.12.14.2. **Trusted Publisher:** fornecedor específico, assinado digitalmente por um certificado de segurança emitido, para este fornecedor, por uma Autoridade Certificadora (CA – Certificate Authority).
1.12.14.3. **Trusted Installer:** software instalado por um programa instalador específico, identificações por seu algorítmo de verificação, independentemente de sua origem.
1.12.14.4. **Trusted Directories:** pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.
1.12.14.5. **Trusted Program / Authorized Updater:** programas identificados pelo nome, para adicionar e/ou atualizar aplicações.
1.12.14.6. **Trusted Users / Authorized Users:** somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.
1.12.14.7. **Trusted Time Window / Update Mode:** janela de tempo para manutenção de aplicações.
1.12.15. Deve ser capaz de proteger em modo standalone – online ou offline;
1.12.16. Deve ser capaz de prevenir a criação de novos arquivos (incluindo diretórios e chaves de registro);
1.12.17. Deve ser capaz de monitorar a modificação de arquivos existentes, diretórios e chaves de registro;
1.12.18. Caso o arquivo seja sensível ou crítico, o administrador pode optar por receber um e-mail detalhando cada alteração realizada;
1.12.19. Deve ser capaz de limitar não apenas a escrita em chaves de registro, mas também a leitura;
1.12.20. A solução deve prover um conjunto de regras que limitam as ações nas chaves de registro;
1.12.21. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do órgão;
1.12.22. Deve prevenir as seguintes ações:
1.12.22.1. Deletar
1.12.22.2. Renomear

1.12.22.3. Criar links
1.12.22.4. Modificar Conteúdo
1.12.23. Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento (Exemplo: %HOMEPATH%, %HOMEDRIVE%, %USERPROFILE%, %APPDATA%)
1.12.24. Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo: %PROGRAMFILES (x86)%
1.12.25. Deve ser possível comparar dois arquivos ou duas versões de um arquivo da mesma estação de trabalho ou de estações diferentes, como forma de mitigar possíveis ameaças persistentes;
1.12.26. Deve ser possível autorizar usuários específicos que terão privilégios de alteração nos arquivos e chaves de registro protegidos na estação de trabalho;
1.12.26.1. Essa autorização deve utilizar o Active Directory para importar os usuários autorizados;
1.12.27. Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:
1.12.27.1. Critical Address Space Protection;
1.12.27.2. NX – No eXecute (mp-nx)
1.12.27.3. Virtual Address Space Randomization
1.12.27.3.1. Mp-vasr-randomization
1.12.27.3.2. Mp-vasr-relocation
1.12.27.3.3. Mp-vasr-reloc
1.12.27.4. Forced DLL Relocation
1.12.28. Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho.
1.12.29. Permitir o bloqueio de aplicações e os processos que a aplicação interage
1.12.30. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não.
1.12.31. Permitir monitoração de Hooking de aplicações onde se podem determinar quais processos pode ser executado ou não.
1.13. Módulo de Gerência
1.13.1. A gerência deve ser centralizada e suportar a gestão de todos os módulos listados neste Termo de Referência;
1.13.2. Não serão aceitas soluções que possuam mais de uma console de gestão;
1.13.3. Deve suportar a instalação nos seguintes sistemas operacionais:
1.13.3.1. Windows Server 2012 Release 2;
1.13.3.2. Windows Server 2012
1.13.3.3. Windows Server 2008 Service Pack 2 (SP2) Standard,

Enterprise ou Datacenter;
1.13.3.4. Windows Server 2008 R2 Standard, Enterprise ou Datacenter;
1.13.3.5. A arquitetura dos Sistemas Operacionais deve ser 64-bits;
1.13.4. Deve suportar a instalação em Cluster Microsoft;
1.13.5. Deve suportar Ipv4 e Ipv6;
1.13.6. Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:
1.13.6.1. Vmware ESX
1.13.6.2. Citrix Xen Server
1.13.6.3. Microsoft Hyper-V
1.13.7. Deve possuir suporte a base de dados:
1.13.7.1. SQL Server 2012 ou superior
1.13.8. Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;
1.13.9. A console de gerência deve ser acessada via WEB;
1.13.10. Deve possuir compatibilidade com os seguintes browsers:
1.13.10.1. Google Chrome;
1.13.10.2. Firefox;
1.13.10.3. Internet Explorer 7 ou superior;
1.13.10.4. Safari 6.0 ou superior;
1.13.11. Deve ser possível segregar a instalação da solução em:
1.13.11.1. Servidor Console Central
1.13.11.2. Servidor Base de Dados
1.13.11.3. Servidor de Interação com os Agentes
1.13.11.4. Agentes Distribuidores de Vacina
1.13.12. Deve suportar o uso do SQL Server em ambientes SAN;
1.13.13. Permitir a instalação dos Módulos da Solução a partir de um único servidor
1.13.14. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota
1.13.15. Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE nesta contratação presente ou futura.
1.13.16. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.
1.13.17. Visualização das características básicas de hardware das máquinas
1.13.18. Integração e Importação automática da estrutura de domínios do

Active Directory já existentes na rede local
1.13.19. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede.
1.13.20. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado
1.13.21. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.
1.13.22. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados.
1.13.23. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente
1.13.24. Permitir a criação de grupos virtuais através de “TAGs”
1.13.25. Permitir aplicar as “TAGs” nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;
1.13.26. Forçar a configuração determinada no servidor para os clientes;
1.13.27. Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente.
1.13.28. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS
1.13.29. Forçar a instalação dos Módulos da Solução nos clientes;
1.13.30. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido.
1.13.31. Customização dos relatórios gráficos gerados;
1.13.32. Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML
1.13.33. Geração de relatórios que contenham as seguintes informações:
1.13.34. Máquinas com a lista de definições de vírus desatualizada;
1.13.35. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;
1.13.36. Os vírus que mais foram detectados;
1.13.37. As máquinas que mais sofreram infecções em um determinado período de tempo
1.13.38. Os usuários que mais sofreram infecções em um determinado período de tempo
1.13.39. Gerenciamento de todos os módulos da suíte;
1.13.40. Possuir dashboards no gerenciamento da solução;
1.13.41. Ao identificar um novo arquivo sendo executado, este deve ser

submetido ou comparado a base do Virustotal;
1.13.42. Deve ser capaz de identificar e apresentar uma visibilidade sobre quais estações executaram um determinado arquivo (executável);
1.13.43. Deve ser capaz de identificar o arquivo e bloqueá-lo baseado na reputação e em critério de risco;
1.13.44. Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:
1.13.45. Relatório dos últimos 30 dias da detecção de códigos maliciosos;
1.13.46. Top 10 Computadores com Infecções;
1.13.47. Top 10 Computadores com Sites bloqueados pela politica;
1.13.48. Resumo das ações tomadas nos últimos 30 dias no que se refere a Filtro de Navegação na web;
1.13.49. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota
1.13.50. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva
1.13.51. Ter a capacidade de gerar registros/logs para auditoria
1.13.52. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.
1.13.53. A solução de gerenciamento deve permitir acesso a sua console via web.

2. Solução para resposta à incidentes - EDR

2.1. Características Gerais da Solução

2.1.1. A solução deve contemplar as seguintes funcionalidades básicas, descritas a seguir:
2.1.1.1. Deve possuir suporte a arquiteturas 32-bits e 64-bits.
2.1.1.2. Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho
2.1.1.3. Deve suportar as seguintes plataformas clientes:
2.1.1.3.1. Windows 10;
2.1.1.3.2. Windows 8.1;
2.1.1.3.3. Windows 8;
2.1.1.3.4. Windows 7;
2.1.1.3.5. Sierra 10.12.x
2.1.1.3.6. El Captain 10.11.x
2.1.1.4. Deve suportar as seguintes plataformas servidores:

2.1.1.4.1. Windows Server 2016;
2.1.1.4.2. Windows Server 2012 R2;
2.1.1.4.3. Windows Server 2012;
2.1.1.4.4. Windows 2008 R2 (Standard/Enterprise);
2.1.1.5. Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:
2.1.1.5.1. AWS;
2.1.1.5.2. Azure;
2.1.1.5.3. Citrix XenApp;
2.1.1.5.4. Citrix XenDesktop;
2.1.1.5.5. Citrix XenServer;
2.1.1.5.6. Microsoft Hyper-V 2012 R2;
2.1.1.5.7. Vmware ESXi;
2.1.1.5.8. Vmware Player;
2.1.1.5.9. Vmware vShpere;
2.1.1.5.10. Vmware Workstation;
2.1.1.6. Toda a proteção deverá ser realizada através de um único agente de proteção com as funcionalidades descritas neste termo, não sendo aceitos plugins ou softwares adicionais para a composição do pacote.
2.1.1.7. O agente único deve compreender as seguintes funcionalidades:
2.1.1.7.1. Prevenção de Ameaças;
2.1.1.7.2. Firewall;
2.1.1.7.3. Controle Web;
2.1.1.7.4. Inteligência contra Ameaças;
2.1.1.8. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:
2.1.1.8.1. Relatórios;
2.1.1.8.2. Dashboards;
2.1.1.8.3. Políticas;
2.1.1.8.4. Configuração;
2.1.1.8.5. Instalação/Desinstalação;
2.1.1.9. O cliente deve ser capaz de operar em modo autonomo (selfmanaged) e permitir que as configurações sejam aplicadas diretamente no cliente.
2.1.1.10. O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfix'es a partir de um servidor definido pelo administrador ou diretamente nos servidores da McAfee.
2.1.1.11. A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem

informações para uma análise mais inteligente;
2.1.1.12. A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;
2.1.1.13. A solução deve conter módulo capaz de proteger contra botnets, negação de serviço, executáveis não confiáveis e conexões web maliciosas;
2.1.1.14. A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)
2.1.1.15. A solução deve conter módulo capaz de garantir integração entre as soluções do fabricante proposto e entre fabricantes terceiros, compartilhando as informações do paciente dia zero para melhor mitigar novas ameaças.
2.1.1.15.1. Este módulo deve estar público para o desenvolvimento da comunidade via Github;

2.2. Proteção Clientes Windows

Proteção de Ameaças

2.2.1. Prevenção de exploração:

2.2.1.1. Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).
2.2.1.2. Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.
2.2.1.3. Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.
2.2.1.4. Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;
2.2.1.5. Deve ser possível incluir exclusões por:
2.2.1.5.1. Processo
2.2.1.5.1.1. Nome;
2.2.1.5.1.2. Caminho do Arquivo;
2.2.1.5.1.3. Hash MD5
2.2.1.5.2. Módulo chamador:
2.2.1.5.2.1. Nome
2.2.1.5.2.2. Caminho
2.2.1.5.2.3. Hash MD5
2.2.1.5.2.4. Signatário Digital

2.2.2. Proteção de acesso

2.2.2.1. Deve fornecer regras de proteção nativamente, ou seja definida pelo fabricante da solução, no mínimo, para:
2.2.2.1.1. Acesso remoto a pastas locais;
2.2.2.1.2. Alteração políticas de direitos dos usuários;

2.2.2.1.3. Alterar os registros de extensão dos arquivos;
2.2.2.1.4. Criação de novos arquivos na pasta Arquivo de Programas;
2.2.2.1.5. Criação de novos executáveis na pasta Windows;
2.2.2.1.6. Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema;
2.2.2.1.7. Criar ou Modificar remotamente arquivos ou pastas;
2.2.2.1.8. Desativar o editor de registro e o gerenciador de tarefas;
2.2.2.1.9. Executar arquivos das pastas do usuário;
2.2.2.1.10. Execução de scripts pelo host de script do Windows;
2.2.2.1.11. Instalar objetos de ajuda a navegação ou extensões de shell;
2.2.2.1.12. Instalar novos CLSIDs, APPIDs e TYPELIBs;
2.2.2.1.13. Modificar configurações de rede;
2.2.2.1.14. Modificar configurações do Internet Explorer;
2.2.2.1.15. Modificar processos principais do Windows;
2.2.2.1.16. Navegadores iniciando programas da pasta de downloads;
2.2.2.1.17. Registrar programas para execução automática;
2.2.2.2. As regras especificadas devem permitir o seu:
2.2.2.2.1. Bloqueio, ou
2.2.2.2.2. Informação, ou
2.2.2.2.3. Bloqueio e Informação;
2.2.2.3. Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parâmetros:
2.2.2.3.1. Processos;
2.2.2.3.1.1. Nome do processo;
2.2.2.3.1.2. Hash MD5;
2.2.2.3.1.3. Assinatura Digital;
2.2.2.3.2. Usuário
2.2.2.3.3. Arquivos;
2.2.2.3.3.1. Criação;
2.2.2.3.3.2. Deletar;
2.2.2.3.3.3. Executar;
2.2.2.3.3.4. Alteração de permissão;
2.2.2.3.3.5. Leitura;
2.2.2.3.3.6. Renomear;
2.2.2.3.3.7. Escrever;
2.2.2.3.4. Chave de Registro
2.2.2.3.4.1. Escrever;
2.2.2.3.4.2. Criar;
2.2.2.3.4.3. Deletar;
2.2.2.3.4.4. Ler;

2.2.2.3.4.5. Enumerar;
2.2.2.3.4.6. Carregar;
2.2.2.3.4.7. Substituir;
2.2.2.3.4.8. Restaurar;
2.2.2.3.4.9. Alterar permissão;
2.2.2.3.5. Valor de Registro
2.2.2.3.5.1. Ler;
2.2.2.3.5.2. Criar;
2.2.2.3.5.3. Deletar;
2.2.2.3.6. Processo
2.2.2.3.6.1. Qualquer acesso;
2.2.2.3.6.2. Criar thread;
2.2.2.3.6.3. Modificar;
2.2.2.3.6.4. Terminar;
2.2.2.3.6.5. Executar;
2.2.2.3.7. Deve permitir a criação de exclusões;

2.2.3. Varredura ao acessar

2.2.3.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;
2.2.3.2. Deve iniciar a proteção durante a inicialização do sistema operacional;
2.2.3.3. Deve ser capaz de realizar análise no setor de boot;
2.2.3.4. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;
2.2.3.5. Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo;
2.2.3.6. Deve possibilitar ao administrador a análise de instaladores confiáveis;
2.2.3.7. Deve realizar análise durante copia entre pastas locais;
2.2.3.8. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;
2.2.3.9. Deve permitir a configuração do nível de agressividade da análise entre:
2.2.3.9.1. Muito Baixo
2.2.3.9.2. Baixo
2.2.3.9.3. Médio
2.2.3.9.4. Alto
2.2.3.9.5. Muito Alto
2.2.3.10. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;

2.2.3.11. Deve realizar varredura quando o processo:
2.2.3.11.1. Ler o disco;
2.2.3.11.2. Gravar no disco;
2.2.3.11.3. Deixar a solução de proteção decidir;
2.2.3.12. Deve possibilitar análise em
2.2.3.12.1. Unidades de Rede;
2.2.3.12.2. Arquivos abertos para backup;
2.2.3.12.3. Arquivos compactados, por exemplo .jar;
2.2.3.12.4. Arquivos codificados (MIME)
2.2.3.13. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;
2.2.3.14. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
2.2.3.14.1. Limpar o arquivo;
2.2.3.14.2. Excluir o arquivo;
2.2.3.14.3. Negar acesso ao arquivo;
2.2.3.15. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
2.2.3.15.1. Limpar o arquivo;
2.2.3.15.2. Excluir o arquivo;
2.2.3.15.3. Permitir acesso ao arquivo;
2.2.3.15.4. Negar acesso ao arquivo;
2.2.3.16. Deve possibilitar ao administrador a gestão de uma lista de exclusões;
2.2.3.17. Deve possuir módulo capaz de interceptar scripts destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;
2.2.3.18. Deve permitir a criação de listas de exclusão de URL's que não sofrerão interceptação e análise de scripts;
2.2.3.19. Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

2.2.4. Varredura sob demanda

2.2.4.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.
2.2.4.1.1. Deve permitir a criação de repetição da tarefa.
2.2.4.1.2. Deve permitir definir a hora da execução da tarefa de análise;
2.2.4.1.3. Deve permitir a criação da tarefa de varredura de maneira aleatória;
2.2.4.2. Deve permitir a realização de varreduras agendadas após

logon do usuário ou durante inicialização do sistema operacional.
2.2.4.3. Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:
2.2.4.3.1. Os locais da varredura, dentre eles:
2.2.4.3.1.1. Memória para rootkits;
2.2.4.3.1.2. Processos em execução;
2.2.4.3.1.3. Arquivos registrados;
2.2.4.3.1.4. Meu computador;
2.2.4.3.1.5. Todas as unidades locais;
2.2.4.3.1.6. Todas as unidades fixas;
2.2.4.3.1.7. Todas as unidades removíveis;
2.2.4.3.1.8. Todas as unidades mapeadas;
2.2.4.3.1.9. Pasta inicial;
2.2.4.3.1.10. Pasta de perfil do usuário;
2.2.4.3.1.11. Pasta Windows;
2.2.4.3.1.12. Pasta de arquivos de programas;
2.2.4.3.1.13. Pasta temporária;
2.2.4.3.1.14. Lixeira;
2.2.4.3.1.15. Arquivo ou pasta especificada pelo administrador;
2.2.4.3.1.16. Setor de inicialização (boot);
2.2.4.3.1.17. Arquivos compactados;
2.2.4.3.1.18. Arquivos MIME;
2.2.4.3.2. Os tipos de arquivos que serão analisados;
2.2.4.3.3. Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.
2.2.4.3.4. Áreas de exclusão que não deverão ser varridas;
2.2.4.4. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada para a detecção de ameaças desconhecidas.
2.2.4.5. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
2.2.4.5.1. Limpar o arquivo;
2.2.4.5.2. Excluir o arquivo;
2.2.4.5.3. Negar acesso ao arquivo;
2.2.4.6. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
2.2.4.6.1. Limpar o arquivo;
2.2.4.6.2. Excluir o arquivo;
2.2.4.6.3. Permitir acesso ao arquivo;
2.2.4.6.4. Negar acesso ao arquivo;

2.2.4.7. Para minimizar o impacto ao usuário, a solução deve permitir:
2.2.4.7.1. Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;
2.2.4.7.2. Iniciar a varredura apenas quando o sistema estiver ocioso;
2.2.4.7.3. Permitir ao usuário retomar varreduras pausadas;
2.2.4.8. Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;

2.3. Proteção de Rede

2.3.1. O módulo de Firewall de Host deve incluir as seguintes capacidades:
2.3.1.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;
2.3.1.2. Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura contra ataques dia zero;
2.3.1.3. Deve possuir um firewall de estação statefull bloqueando tráfego de entrada e controlando o tráfego de saída;
2.3.1.4. Deve possuir assinaturas de proteção para:
2.3.1.4.1. Arquivos
2.3.1.4.2. Chave de Registro
2.3.1.4.3. Processos
2.3.1.4.4. Serviços;
2.3.1.5. Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;
2.3.1.6. Deve ser possível bloquear trafego bridge;
2.3.1.7. Deve ser possível bloquear contra falsificação de IP (IP Spoofing)
2.3.1.8. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;
2.3.1.9. Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;
2.3.1.10. Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações:
2.3.1.10.1. Nome
2.3.1.10.2. Nome do arquivo ou Caminho;
2.3.1.10.3. Hash MD5
2.3.1.10.4. Assinador Digital

2.3.1.11. Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;
2.3.1.11.1. As conexões identificadas pelo Centro de Inteligência podem ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.
2.3.1.12. Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;
2.3.1.13. Deve permitir inspeção do protocolo FTP;
2.3.1.14. Deve ser possível bloquear trafego de protocolos não suportados;
2.3.1.15. O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.
2.3.1.16. O módulo de firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:
2.3.1.16.1. Ação
2.3.1.16.1.1. Bloquear
2.3.1.16.1.2. Permitir
2.3.1.16.2. Direção
2.3.1.16.2.1. Ambas
2.3.1.16.2.2. Entrada
2.3.1.16.2.3. Saída
2.3.1.16.3. Protocolo
2.3.1.16.3.1. Qualquer protocolo
2.3.1.16.3.2. Protocolo IP
2.3.1.16.3.2.1. Ipv4
2.3.1.16.3.2.2. Ipv6
2.3.1.16.3.2.3. Protocolo Não-IP
2.3.1.16.3.3. Tipo de Conexão
2.3.1.16.3.3.1. Rede Sem Fio
2.3.1.16.3.3.2. Rede Cabeada
2.3.1.16.3.3.3. Rede Virtual
2.3.1.16.3.4. Especificação da Rede
2.3.1.16.3.4.1. Endereço IP
2.3.1.16.3.4.2. Subnet
2.3.1.16.3.4.3. Range
2.3.1.16.3.4.4. FQDN
2.3.1.16.3.5. Protocolo de Transporte
2.3.1.16.3.5.1. Todos
2.3.1.16.3.5.2. ICMP
2.3.1.16.3.5.3. ICMPv6
2.3.1.16.3.5.4. TCP

2.3.1.16.3.5.5. UDP
2.3.1.16.3.5.6. STP
2.3.1.16.3.5.7. GRE
2.3.1.16.3.5.8. IGMP
2.3.1.16.3.5.9. IPSEC AH
2.3.1.16.3.5.10. IPSEC ESP
2.3.1.16.3.5.11. Ipv6 in Ipv4
2.3.1.16.3.5.12. ISIS over Ipv4
2.3.1.16.3.5.13. L2TP
2.3.1.16.3.6. Agendamento
2.3.1.16.3.6.1. Dias da Semana
2.3.1.16.3.6.2. Hora Inicio
2.3.1.16.3.6.3. Hora Fim
2.3.1.16.3.7. Aplicações
2.3.1.17. Deve possuir as seguintes proteções:
2.3.1.17.1. Generic Buffer Overflow Protection;
2.3.1.17.2. Suspicious caller and caller validation;
2.3.1.17.3. Exploit Prevention
2.3.1.17.4. Access Protection;
2.3.1.17.5. Data Execution Protection
2.3.1.17.6. Generic Privilege Escalation Protection

2.4. Proteção Web

2.4.1. O modulo de Controle Web deve possuir as seguintes funcionalidades:
2.4.1.1. Deve permitir o bloqueio de browsers não suportados, dentre eles:
2.4.1.1.1. Opera
2.4.1.1.2. Safari for Windows;
2.4.1.1.3. Netscape
2.4.1.1.4. Maxthon
2.4.1.1.5. Flock;
2.4.1.1.6. Avant Browser;
2.4.1.1.7. Deepnet Explorer
2.4.1.1.8. PhaseOut
2.4.1.2. Deve permitir o controle de browsers suportados, dentre eles:
2.4.1.2.1. Chrome
2.4.1.2.2. Firefox
2.4.1.2.3. Internet Explorer
2.4.1.3. Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado.
2.4.1.4. Deve possuir, no mínimo, as seguintes categorias:
2.4.1.4.1. Browser Exploits;

2.4.1.4.2. Download Maliciosos;
2.4.1.4.3. Sites Maliciosos;
2.4.1.4.4. Phishing;
2.4.1.4.5. Pornografia;
2.4.1.4.6. Hacking/Computer Crime;
2.4.1.4.7. Spyware/Adware/Keyloggers;
2.4.1.4.8. Anonymizer;
2.4.1.4.9. Anonymizer Utilities;
2.4.1.4.10. Alcohol;
2.4.1.4.11. Blogs/Wiki;
2.4.1.4.12. Business;
2.4.1.4.13. Chat;
2.4.1.4.14. Content Server;
2.4.1.4.15. Dating
2.4.1.4.16. Dating/Social Networking
2.4.1.4.17. Digital Postcards
2.4.1.4.18. Discrimination;
2.4.1.4.19. Drugs;
2.4.1.4.20. Education;
2.4.1.4.21. Entertainment;
2.4.1.4.22. Extreme
2.4.1.4.23. Fashion
2.4.1.4.24. Finance
2.4.1.4.25. For Kids
2.4.1.4.26. Forum
2.4.1.4.27. Gambling
2.4.1.4.28. Game/Cartoon Violence
2.4.1.4.29. Games
2.4.1.4.30. General News
2.4.1.4.31. Government/Military
2.4.1.4.32. Gruesome Content
2.4.1.4.33. Health
2.4.1.4.34. Historical Revisionism
2.4.1.4.35. History
2.4.1.4.36. Humor/Comics
2.4.1.4.37. Illegal UK
2.4.1.4.38. Incidental Nudity
2.4.1.4.39. Information Security
2.4.1.4.40. Instant Messaging
2.4.1.4.41. Interactive Web Applications
2.4.1.4.42. Internet Radio/TV
2.4.1.4.43. Internet Services

2.4.1.4.44. Job Search
2.4.1.4.45. Major Global Religions
2.4.1.4.46. Marketing/Merchandising
2.4.1.4.47. Media Downloads
2.4.1.4.48. Media Sharing
2.4.1.4.49. Messaging
2.4.1.4.50. Mobile Phone
2.4.1.4.51. Moderated
2.4.1.4.52. Motor Vehicles
2.4.1.4.53. Non-Profit/Advocacy/NGO
2.4.1.4.54. Nudity
2.4.1.4.55. Online Shopping
2.4.1.4.56. P2P/File Sharing
2.4.1.4.57. Parked Domain
2.4.1.4.58. Personal Network Storage
2.4.1.4.59. Personal Pages
2.4.1.4.60. Pharmacy
2.4.1.4.61. Politics/Opinion
2.4.1.4.62. Portal Sites
2.4.1.4.63. Potential Criminal Activities
2.4.1.4.64. Potential Illegal Software
2.4.1.4.65. Potentially Unwanted Programs
2.4.1.4.66. Profanity
2.4.1.4.67. Professional Networking
2.4.1.4.68. Provocative Attire
2.4.1.4.69. Public Information
2.4.1.4.70. Real Estate
2.4.1.4.71. Recreation/Hobbies
2.4.1.4.72. Religion/Ideology
2.4.1.4.73. Remote Access
2.4.1.4.74. Residential IP Addresses
2.4.1.4.75. Resource Sharing
2.4.1.4.76. Restaurants
2.4.1.4.77. School Cheating Information
2.4.1.4.78. Search Engines
2.4.1.4.79. Sexual Materials
2.4.1.4.80. Shareware/Freeware
2.4.1.4.81. Social Networking
2.4.1.4.82. Software/Hardware
2.4.1.4.83. Spam URLs
2.4.1.4.84. Sports
2.4.1.4.85. Stock Trading

2.4.1.4.86. Streaming Media
2.4.1.4.87. Technical Information
2.4.1.4.88. Technical/Business Forums
2.4.1.4.89. Text Translators
2.4.1.4.90. Text/Spoken Only
2.4.1.4.91. Tobacco
2.4.1.4.92. Travel
2.4.1.4.93. Uncategorized
2.4.1.4.94. Usenet News
2.4.1.4.95. Violence
2.4.1.4.96. Visual Search Engine
2.4.1.4.97. Weapons
2.4.1.4.98. Web Ads
2.4.1.4.99. Web Mail
2.4.1.4.100. Web Meetings
2.4.1.4.101. Web Phone
2.4.1.5. Deve ser possível bloquear um site conforme a sua classificação:
2.4.1.5.1. Vermelho: Alto Risco
2.4.1.5.2. Amarelo: Médio Risco
2.4.1.5.3. Cinza: Não categorizado
2.4.1.6. Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;
2.4.1.7. Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;
2.4.1.8. Deve permitir a varredura de arquivos baixados da internet;
2.4.1.9. Deve ser possível excluir endereços IP da análise;
2.4.1.10. Deve permitir a busca segura para buscadores, dentre eles:
2.4.1.10.1. Google;
2.4.1.10.2. Yahoo
2.4.1.10.3. Bing;
2.4.1.10.4. Ask;
2.4.1.11. Deve bloquear links que direcionem para sites com alto risco.
2.4.1.12. Deve permitir a customização das mensagens apresentadas para o usuário;
2.4.1.13. Caso o módulo detecte que exista um McAfee Web Gateway na rede, deverá deixar a análise a cargo deste último.

2.5. Blindagem das estações de trabalho

2.5.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas, aplicar o controle de execução (Blindagem da estação de trabalho) e realizar controle e auditoria sobre as alterações realizadas pelos

usuários;
2.5.1.1. Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes.
2.5.1.1.1. Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão;
2.5.1.2. Ao detectar um executável, a solução deverá consultar o Centro de Inteligência do fabricante e esta deverá informar um nível de confidência (Bom, Mau ou Não Classificado);
2.5.1.3. Para o caso de problema com o envio de informações para o fabricante, este deverá possibilitar executar a tarefa por meio do servidor de reputação local;
2.5.1.4. Deve ser possível criar uma imagem base para a criação de uma política geral;
2.5.1.5. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;
2.5.1.6. A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos;
2.5.1.7. Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:
2.5.1.7.1. **Desabilitado:** proteção desativada
2.5.1.7.2. **Monitoramento:** Monitora toda a atividade da Estação de Trabalho;
2.5.1.7.3. **Atualização:** a cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido;
2.5.1.8. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA-1).
2.5.1.9. A solução deve suportar as seguintes modalidades de proteção:
2.5.1.9.1. **Application Whitelisting:** criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impadidas de serem executadas.
2.5.1.9.2. **Application Blocking / Blacklisting:** criação de uma lista de aplicações não autorizadas que não podem ser executadas.
2.5.1.9.3. **Memory Protection:** monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em

memória.
2.5.1.9.4. **Change Control:** Deve monitorar mudanças de arquivos e chaves de registro em tempo real.
2.5.1.10. Solução suporta criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.
2.5.1.11. Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação do aplicativo ou arquivo.
2.5.1.12. Suporta os mecanismos:
2.5.1.12.1. **Application Code Protection:** permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, etc) possam ser executados. Além disso, permite proteção contra adulterações de programas em Whitelist (ex.: arquivos do programa) e, opcionalmente, chaves de registros contra modificações em disco.
2.5.1.12.2. **Memory Protection:** permite proteção contra ataques e exploração de vulnerabilidades para os programas em Whitelist.
2.5.1.13. Suporta criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de Whitelist, através de:
2.5.1.13.1. **Binário:** binário específico identificado através de seu nome ou de algorítmo de verificação SHA-1.
2.5.1.13.2. **Trusted Publisher:** fornecedor específico, assinado digitalmente por um certificado de segurança emitido, para este fornecedor, por uma Autoridade Certificadora (CA - Certificate Authority).
2.5.1.13.3. **Trusted Installer:** software instalado por um programa instalador específico, identificações por seu algorítmo de verificação, independentemente de sua origem.
2.5.1.13.4. **Trusted Directories:** pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.
2.5.1.13.5. **Trusted Program / Authorized Updater:** programas identificados pelo nome, para adicionar e/ou atualizar aplicações.
2.5.1.13.6. **Trusted Users / Authorized Users:** somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.
2.5.1.13.7. **Trusted Time Window / Update Mode:** janela de tempo para manutenção de aplicações.

2.5.1.14. Deve ser capaz de proteger em modo standalone - online ou offline;
2.5.1.15. Deve ser capaz de prevenir a criação de novos arquivos (incluindo diretórios e chaves de registro);
2.5.1.16. Deve ser capaz de monitorar a modificação de arquivos existentes, diretórios e chaves de registro;
2.5.1.17. Caso o arquivo seja sensível ou crítico, o administrador pode optar por receber um e-mail detalhando cada alteração realizada;
2.5.1.18. Deve ser capaz de limitar não apenas a escrita em chaves de registro, mas também a leitura;
2.5.1.19. A solução deve prover um conjunto de regras que limitam as ações nas chaves de registro;
2.5.1.20. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do orgão;
2.5.1.21. Deve prevenir as seguintes ações:
2.5.1.21.1. Deletar;
2.5.1.21.2. Renomear;
2.5.1.21.3. Criar links;
2.5.1.21.4. Modificar Conteúdo;
2.5.1.21.5. Alterar o dono;
2.5.1.22. Deve ser capaz de monitorar alterações relacionadas as contas de usuários dentro dos seguintes parâmetros:
2.5.1.22.1. Criação de Conta
2.5.1.22.2. Alteração de Conta
2.5.1.22.3. Deleção de Conta
2.5.1.22.4. Log On (Sucesso e Falha)
2.5.1.22.5. Log Off
2.5.1.23. Deve suportar o monitoramento de atributos para os seguintes tipos de arquivo:
2.5.1.23.1. Zip
2.5.1.23.2. Tar
2.5.1.23.3. Dll
2.5.1.23.4. Exe
2.5.1.23.5. Jar
2.5.1.23.6. Sys
2.5.1.23.7. 7z
2.5.1.23.8. Bz2
2.5.1.23.9. Bz
2.5.1.23.10. Tgz
2.5.1.23.11. Gz

2.5.1.23.12. Bmp
2.5.1.23.13. Jpg
2.5.1.23.14. tiff
2.5.1.24. Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento (Exemplo: %HOMEPATH%, %HOMEDRIVE%, %USERPROFILE%, %APPDATA%)
2.5.1.25. Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo: %PROGRAMFILES (x86)%)
2.5.1.26. Deve ser possível comparar dois arquivos ou duas versões de um arquivo da mesma estação de trabalho ou de estações diferentes, como forma de mitigar possíveis ameaças persistentes;
2.5.1.27. Deve ser possível autorizar usuários específicos que terão privilégios de alteração nos arquivos e chaves de registro protegidos na estação de trabalho;
2.5.1.28. Essa autorização deve utilizar o Active Directory para importar os usuários autorizados;
2.5.1.29. Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:
2.5.1.29.1. Critical Address Space Protection;
2.5.1.29.2. NX - No eXecute (mp-nx)
2.5.1.29.3. Virtual Address Space Randomization
2.5.1.29.4. Mp-vasr-rebase
2.5.1.29.5. Mp-vasr-randomization
2.5.1.29.6. Mp-vasr-relocation
2.5.1.29.7. Mp-vasr-reloc
2.5.1.29.8. Forced DLL Relocation
2.5.1.30. Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho.
2.5.1.31. Permitir o bloqueio de aplicações e os processos que a aplicação interage
2.5.1.32. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não.
2.5.1.33. Permitir monitoração de Hooking de aplicações onde se podem determinar quais processos pode ser executado ou não

2.6. Proteção Adaptativa de Ameaças

2.6.1. O módulo de inteligência contra ameaças deve conter os seguintes mecanismos:
2.6.1.1. Confinamento dinâmico de aplicações:
2.6.1.1.1. A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios

maliciosos (Ransomware)
2.6.1.1.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executandoas em ambiente controlado;
2.6.1.1.3. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico
2.6.1.1.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada
2.6.1.1.5. Solução deve manter um cache de reputação local com informações de aplicações – conhecidas, desconhecidas e maliciosas.
2.6.1.1.5.1. Deve ser possível a classificação de cada aplicativo de maneira manual e até mesmo sua reclassificação através da console de administração central.
2.6.1.1.6. Dentre os comportamentos maliciosos, deve ser capaz de:
2.6.1.1.6.1. Bloquear acesso local a partir de cookies;
2.6.1.1.6.2. Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs
2.6.1.1.6.3. Criação de arquivos em qualquer local de rede
2.6.1.1.6.4. Criação de novos CLSIDs, APPIDs e TYPELIBs
2.6.1.1.6.5. Criação de threads em outro processo
2.6.1.1.6.6. Bloquear a desativação de executáveis críticos do sistema operacional
2.6.1.1.6.7. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares
2.6.1.1.6.8. Gravação e Leitura na memória de outro processo
2.6.1.1.6.9. Bloqueio de Modificação da política de firewall do windows
2.6.1.1.6.10. Bloqueio de Modificação da pasta de tarefas do Windows
2.6.1.1.6.11. Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro
2.6.1.1.6.12. Bloqueio de Modificação de arquivos executáveis portáteis;
2.6.1.1.6.13. Bloqueio de Modificação de bit de atributo oculto
2.6.1.1.6.14. Bloqueio de Modificação de bt de atributo somente leitura
2.6.1.1.6.15. Bloqueio de Modificação de entradas de registro de DLL AppInit;
2.6.1.1.6.16. Bloqueio de Modificação de locais do registro de inicialização
2.6.1.1.6.17. Bloqueio de Modificação de pastas de dados de

usuários;
2.6.1.1.6.18. Bloqueio de Modificação do local do Registro de Serviços
2.6.1.1.6.19. Bloqueio de Suspensão de um processo
2.6.1.1.6.20. Bloqueio de Término de outro processo
2.6.1.1.7. Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.
2.6.1.1.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada.
2.6.1.1.9. O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;
2.6.1.1.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário
2.6.1.1.11. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção
2.6.1.2. Reputação local de ameaças
2.6.1.2.1. O módulo de reputação local deve manter uma base de dados com todos os executáveis detectados no ambiente.
2.6.1.2.2. Para cada executável, deverão ser apresentadas as reputações:

2.6.1.2.2.1. Local
2.6.1.2.2.2. Centro de Inteligência do Fabricante
2.6.1.2.2.3. Analisador Dia Zero
2.6.1.2.2.4. Filtro de Conteúdo Web
2.6.1.2.3. Deve permitir uma visualização analítica sobre cada arquivo detectado no ambiente, com no mínimo as seguintes informações:
2.6.1.2.3.1. Data do último acesso;
2.6.1.2.3.2. Tamanho do arquivo;
2.6.1.2.3.3. Se está listado no Adicionar/Remover programas do Windows;
2.6.1.2.3.4. Data de compilação;
2.6.1.2.3.5. Registrado como serviço;
2.6.1.2.3.6. Registrado como autorun;
2.6.1.2.3.7. Mais de 6 meses de idade;
2.6.1.2.3.8. Idade foi falsificada;
2.6.1.2.3.9. Executado a partir do cmd.exe
2.6.1.2.4. Deve ser capaz de informar a URL de origem do arquivo

e sua reputação;
2.6.1.2.5. Deve permitir integração com base global de virus – VirusTotal – para comparação e se o arquivo sob análise já foi detectado por outro fabricante;
2.6.1.2.6. Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de "machine-learning";
2.6.1.2.7. Deve ser capaz de user a técnica de "machine-learning" sem conectividade com a nuvem do fabricante.
2.6.1.2.8. Deve permitir o rastreamento da execução do arquivo malicioso pelo ambiente informando qual foi a sua primeira execução e sua última.
2.6.1.2.8.1. Deve permitir a identificação da estação de trabalho e do usuário associado a mesma;
2.6.1.2.9. O módulo deve permitir automatização de contramedidas a partir de soluções do mesmo fabricante e de fabricantes terceiros;

2.7. Módulo Detecção, Resposta e Adaptação

2.7.1. A solução deve ser capaz de implantar o pilar de Detecção, Resposta e Adaptação.

2.7.2. Módulo de Detecção

2.7.2.1. Deve possuir painel único de visibilidade das ameaças do momento que se inicia, como se moveu pelo ambiente e toda a timeline da ameaça em questão.
2.7.2.2. Deve possuir capacidade automática de priorização de riscos baseado no comportamento da ameaça, permitindo uma investigação mais ágil do que é prioritário
2.7.2.3. Deve ser possível pesquisar informações da ameaça em tempo real e em modo histórico para determinar o escopo completo do ataque.
2.7.2.4. Deve permitir o monitoramento do ambiente através de coletores customizados para buscar por indicadores de ataques que não estão somente em execução, mas também por ameaças em modo dormente e demais que foram deletadas.

2.7.3. Módulo de Resposta

2.7.3.1. Deve ser capaz de utilizar gatilhos e reações para detectar eventos de ameaça e reagir de maneira automática.
2.7.3.2. Deve ser capaz de implementar visibilidade dos dados gerados pelo Endpoint, através dos seguintes coletores:
2.7.3.3. Processos;
2.7.3.4. Flows de Rede;

2.7.3.5. Arquivos;
2.7.3.6. Perfil de Usuários;
2.7.3.7. Registro do Windows;
2.7.3.8. Updates Instalados;
2.7.3.9. Grupos Locais
2.7.3.10. Informação do Host;
2.7.3.11. Deve ser capaz de permitir a criação de coletores customizados para a coleta das informações desejadas;
2.7.3.12. Deve permitir a configuração de gatilhos que resultarão em uma reação ou contramedida frente ao dado coletado;
2.7.3.13. Deve ser capaz de implementar ações nos sistemas classificados como comprometidos;
2.7.3.14. Deve permitir a execução de scripts nas linguagens:
2.7.3.14.1. Comandos do Sistema Operacional;
2.7.3.14.2. PowerShell
2.7.3.14.3. Bash
2.7.3.14.4. Python
2.7.3.14.5. Visual Basic
2.7.3.15. Deve vir com políticas de monitoramento pré-configuradas pelo fabricante da solução;
2.7.3.16. Deve ser capaz de executar busca por padrões nas estações clientes em tempo real;
2.7.3.17. O campo de busca deve ser intuitivo e sugerir campos de informação durante a inserção de informações
(auto completar)
2.7.3.18. Deve ser capaz de salvar buscas realizadas previamente;
2.7.3.19. Deve ser capaz de apresentar, no mínimo, as seguintes informações após a busca:
2.7.3.19.1. Endereço IP Local;
2.7.3.19.2. Hash do processo em execução;
2.7.3.19.3. ID do processo;
2.7.3.19.4. Status da transação TCP;
2.7.3.19.5. Número da porta que originou o pacote de rede;
2.7.3.19.6. Nome do arquivo;
2.7.3.19.7. Última data de gravação do arquivo;
2.7.3.19.8. Data de Criação do arquivo
2.7.3.19.9. Data de deleção do arquivo
2.7.3.19.10. Versão do Sistema Operacional;
2.7.3.19.11. Nome do Grupo de usuários
2.7.3.19.12. Se o grupo é local
2.7.3.19.13. SID do grupo
2.7.3.19.14. MAC de origem

2.7.3.19.15. MAC de destino
2.7.3.19.16. FLAGS TCP (ACK, SYN, RST e FIN)
2.7.3.19.17. Número de transação TCP;
2.7.3.19.18. Kernel Time;
2.7.3.19.19. User Time;
2.7.3.19.20. Comando que iniciou o processo;
2.7.3.19.21. Quantidade de RAM utilizada pelo processo;
2.7.3.19.22. Quantidade de Threads criadas pelo processo;
2.7.3.19.23. MD5 do processo;
2.7.3.19.24. SHA-1 do processo;
2.7.3.19.25. Valor da chave de registro
2.7.3.19.26. Caminho da chave de registro;
2.7.3.20. A resposta a uma determinada condição deverá ser executada como um serviço não interativo;
2.7.3.21. Deve permitir a execução de reação diretamente do painel de visibilidade de ameaças, permitindo por exemplo que se pare um processo malicioso em execução.
2.7.4. Módulo de Adaptação
2.7.4.1. Deve possuir a capacidade de criação de coletores e reações customizadas para melhor adaptar as investigações de ameaças e fluxos de detecção.
2.7.4.2. Deve possuir a capacidade de adaptar as configurações de proteção para bloquear ataques persistentes.
2.7.4.3. Ao registrar um artefato malicioso, esta predisposição (Malicioso ou Não Malicioso) deverá ser informada aos componentes interconectados.
2.8. Módulo de Análise Dia Zero
Caso o endpoint detecte um novo arquivo no ambiente, este deve ser encaminhado ao módulo dia zero para análise
2.8.1. Deve ser capaz de analisar os seguintes tipos de arquivos
2.8.1.1. Arquivos Executáveis (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl)
2.8.1.2. Arquivos Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf)
2.8.1.3. Arquivos Compactados (.zip, .rar)
2.8.1.4. Arquivos de Aplicativos Android (.apk)
2.8.1.5. Arquivos Java (jar)
2.8.2. Dispor de engine de múltiplas fases para verificação de Malwares e códigos maliciosos, dentre elas:
2.8.3. Deve se integrar com o centro de inteligência do fabricante para verificar se o arquivo já foi identificado em outro local do mundo
2.8.4. Deve possuir capacidade de emulação de arquivos

2.8.5. Deve possuir motor de análise contra malwares (antivirus engine)
2.8.6. Deve possuir capacidade de Desempacotar Malwares
2.8.7. Deve possuir capacidade de emulação de código
2.8.8. Deve possuir capacidade de Disassembly do código
2.8.9. Deve ser capaz de realizar Análise Dinâmica através de sandbox (instâncias de máquinas virtuais)
2.8.10. Deve realizar análise heurística (IE-FFx-Acrobat Emulation) baseado em análise estatística comportamental da geometria do arquivo, semântica e comportamento do código.
2.8.11. Deve realizar o Desempacotamento e análise do código latente
2.8.12. Deve realizar a análise estática de código e aplicar a engenharia reversa automatizada e o disassembly da análise de código
2.8.13. Deve permitir a análise de modo interativo durante a execução dinâmica do código
2.8.14. A análise dinâmica deve suportar a execução nos seguintes ambientes:
2.8.14.1. Android
2.8.14.2. Windows XP Service Pack 3
2.8.14.3. Windows 7 - 32 bits
2.8.14.4. Windows 7 - 64 bits
2.8.14.5. Windows Server 2003
2.8.14.6. Windows Server 2008 Service Pack 1
2.8.14.7. Windows Server 2008 R2
2.8.15. Deve suportar a análise de URL's submetidas para a solução
2.8.16. Deve ser capaz de inspecionar arquivos criptografados
2.8.17. Toda a verificação e análise de Malwares e/ou códigos maliciosos devem ocorrer em tempo real, não sendo aceitas verificações em cache engine ou batch mode
2.8.18. Analisar de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador
2.8.19. Deve possuir mecanismo para a identificação de Malwares em anexos de e-mails e URLs
2.8.20. Detectar Malwares que utilizem mecanismo de Exploit em arquivos, como PDF
2.8.21. Toda a verificação e análise de Malwares e/ou códigos maliciosos devem ocorrer em tempo real, não sendo aceitas verificações em cache engine ou batch mode
2.9. Módulo de Gerência
2.9.1. A gerência deve ser centralizada e suportar a gestão de todos os módulos listados neste Termo de Referência;

2.9.2. Não serão aceitas soluções que possuam mais de uma console de gestão;
2.9.3. Deve suportar a instalação nos seguintes sistemas operacionais:
2.9.3.1. Windows Server 2012 Release 2;
2.9.3.2. Windows Server 2012
2.9.3.3. Windows Server 2008 Service Pack 2 (SP2) Standard, Enterprise ou Datacenter;
2.9.3.4. Windows Server 2008 R2 Standard, Enterprise ou Datacenter;
2.9.4. A arquitetura dos Sistemas Operacionais deve ser 64-bits;
2.9.5. Deve suportar a instalação em Cluster Microsoft;
2.9.6. Deve suportar Ipv4 e Ipv6;
2.9.7. Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:
2.9.7.1. Vmware ESX
2.9.7.2. Citrix Xen Server
2.9.7.3. Microsoft Hyper-V
2.9.8. Deve possuir suporte a base de dados:
2.9.8.1. SQL Server 2012 ou superior
2.9.9. Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;
2.9.10. A console de gerência deve ser acessada via WEB;
2.9.11. Deve possuir compatibilidade com os seguintes browsers:
2.9.11.1. Google Chrome;
2.9.11.2. Firefox;
2.9.11.3. Internet Explorer 7 ou superior;
2.9.11.4. Safari 6.0 ou superior;
2.9.12. Deve ser possível segregar a instalação da solução em:
2.9.12.1. Servidor Console Central
2.9.12.2. Servidor Base de Dados
2.9.12.3. Servidor de Interação com os Agentes
2.9.12.4. Agentes Distribuidores de Vacina
2.9.13. Deve suportar o uso do SQL Server em ambientes SAN;
2.9.14. Permitir a instalação dos Módulos da Solução a partir de um único servidor
2.9.15. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota
2.9.16. Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE nesta contratação presente ou futura.

2.9.17. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.
2.9.18. Visualização das características básicas de hardware das máquinas
2.9.19. Integração e Importação automática da estrutura de domínios do Active Directory já existentes na rede local
2.9.20. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede.
2.9.21. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado
2.9.22. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.
2.9.23. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados.
2.9.24. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente
2.9.25. Permitir a criação de grupos virtuais através de “TAGs”
2.9.26. Permitir aplicar as “TAGs” nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;
2.9.27. Forçar a configuração determinada no servidor para os clientes;
2.9.28. Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente.
2.9.29. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS
2.9.30. Forçar a instalação dos Módulos da Solução nos clientes;
2.9.31. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido.
2.9.32. Customização dos relatórios gráficos gerados;
2.9.33. Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML
2.9.34. Geração de relatórios que contenham as seguintes informações:
2.9.35. Máquinas com a lista de definições de vírus desatualizada;
2.9.36. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;
2.9.37. Os vírus que mais foram detectados;
2.9.38. As máquinas que mais sofreram infecções em um determinado período de tempo
2.9.39. Os usuários que mais sofreram infecções em um determinado

período de tempo
2.9.40. Gerenciamento de todos os módulos da suíte;
2.9.41. Possuir dashboards no gerenciamento da solução;
2.9.42. Ao identificar um novo arquivo sendo executado, este deve ser submetido ou comparado a base do Virustotal;
2.9.43. Deve ser capaz de identificar e apresentar uma visibilidade
sobre quais estações executaram um determinado arquivo (executável);
2.9.44. Deve ser capaz de identificar o arquivo e bloqueá-lo baseado na reputação e em critério de risco;
2.9.45. Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:
2.9.46. Cobertura da proteção de Navegação Segura;
2.9.47. Relatório dos últimos 30 dias da detecção de códigos maliciosos;
2.9.48. Top 10 Computadores com Infecções;
2.9.49. Top 10 Computadores com Sites bloqueados pela política;
2.9.50. Resumo das ações tomadas nos últimos 30 dias no que se refere a Filtro de Navegação na web;
2.9.51. Resumo dos tipos de sites acessados nos últimos 30 dias no que se refere a Filtro de Navegação Segura;
2.9.52. Gerenciar a atualização do antivírus em computadores portáteis
(notebooks), automaticamente, mediante conexão em rede local ou remota
2.9.53. Suportar o uso de múltiplos repositórios para atualização de
produtos e arquivo de vacina com replicação seletiva
2.9.54. Ter a capacidade de gerar registros/logs para auditoria
2.9.55. A solução de gerenciamento deve ter a capacidade de atribuir
etiquetas as máquinas, facilitando assim a distribuição
automática dentro dos grupos hierárquicos na estrutura de gerenciamento.
2.9.56. A solução de gerenciamento deve permitir acesso a sua console via web.

OBSERVAÇÕES:

CATÁLOGOS: Os catálogos apresentados junto à proposta deverão expressar fielmente o equipamento oferecido bem como as condições de operação do mesmo.

Em caso de discrepâncias entre as especificações disponíveis publicamente a partir de documentos disponíveis para "download" a partir da página do fabricante, e informações providas pela licitante, prevalecerão como válidas as informações disponíveis nos documentos disponibilizados pelo fabricante.

MANUAL: deverá ser entregue com manual de operação em português do Brasil ou em inglês.

LOCAL DE ENTREGA E INSTALAÇÃO: Av. Prof. Frederico Hermann Jr., 345 – Alto de Pinheiros – São Paulo – SP.