APÊNDICE "A"

REQUISITOS MÍNIMOS DA SOLUÇÃO

1. Especificações Técnicas para Solução.

1.1. Inicialmente, apresenta-se na tabela-A a lista de produtos previstos para Contratação de solução de proteção de perímetro, incluindo fornecimento de licenças de software, suporte técnico especializado, atualizações, garantia do fabricante e serviços correlatos por registro de preço:

GRUPO	ITEM	DESCRIÇÃO	QTD
1	1	Renovação de suporte técnico e garantia das licenças para CheckPoint 9700 SAND BLAST Appliance da ANTT.	2
	2	Renovação de suporte técnico e garantia das licenças para CheckPoint 9300 SAND BLAST Appliance da ANTT.	2
	3	Serviço de renovação de suporte técnico e garan a da licença para Security Management Software da ANTT.	1
	4	Fornecimento de licenças, suporte técnico e garantia, para solução de proteção contra ataques de serviços DDoS.	1
	5	Solução para proteção de ferramentas colaborativas baseadas no Office 365 na nuvem, Harmony email collaboration.	2000
	6	Solução de Acesso Remoto Seguro Harmony Sase Internet Access.	600

Tabela A - Produtos a serem adquiridos

2. Requisitos para a Solução de NGFW - Grupo 1 – Item 1 - Contratação do serviço de suporte e manutenção para solução de NG Firewall.

2.1. Esta seção trata de especificações para os equipamentos que compõem a Solução

de alta disponibilidade de Next Generation Firewall, licenças e periféricos necessários para o seu pleno funcionamento nos ambientes on premises da ANTT.

2.2. Como o Firewall é uma solução que identifica e protege, em tempo real, Redes e dispositivos dos contratantes, que estão submetidos a ataques constantemente renovados, este mecanismo fica comprometido quando desatualizado. Portanto, é imprescindível assegurar que a solução de Firewall esteja sempre em sua versão mais recente.

2.3. O Grupo 1 contempla os itens que compõem a solução de segurança cibernética da ANTT. Integram o grupo os serviços de renovação de garantia, atualização de assinaturas de proteção e suporte técnico dos equipamentos Check Point atualmente em operação na Agência (itens 1 e 2), bem como os serviços de renovação de suporte técnico e garantia da solução de gerenciamento centralizado de segurança (item 3) e da solução de proteção contra ataques distribuídos de negação de serviço - DDoS (item 4).

2.4. O grupo contempla ainda a contratação de solução de proteção de ferramentas colaborativas baseadas no Microsoft 365, por meio da solução Harmony Email & Collaboration (item 5), e de solução de acesso remoto seguro à Internet baseada em arquitetura SASE, por meio da solução Harmony SASE Internet Access (item 6), ampliando as capacidades de proteção da infraestrutura tecnológica da Agência.

2.5. Dessa forma, o Grupo 1 reúne os itens de serviços de continuidade operacional e de ampliação das capacidades de segurança cibernética da ANTT, contemplando a contratação pelo período de 12 (doze) meses.

3. Especificação dos Equipamentos do Grupo 1 - itens 1 e 2 - dos Tipos I, II

3.1. Os equipamentos Tipos I e II são os equipamentos que foram dimensionados pelo fabricante Checkpoint e estão em produção no ambiente da ANTT, sem previsibilidade de “End of Life”.

3.2. O Equipamento Tipo I é o modelo Quantum 9700 Plus do fabricante Checkpoint.

3.3. O Equipamento Tipo II corresponde aos modelos Quantum Force 9300 Plus do fabricante Checkpoint.

3.4. No caso de troca de equipamentos, os novos equipamentos devem ter capacidade idêntica ou superior ao antigo e possibilitar o uso de todas as funcionalidades do equipamento

anterior, bem como as especificações do item 1.4 deste Anexo.

4. Grupo 1 - Item 1 do Edital - Renovação de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 12 meses.

4.1. Cada equipamento que compõe o cluster da solução Next Generation Firewall do Tipo I deverá atender às seguintes especificações.

4.2. Throughput de NGFW mínimo esperado de, no mínimo, 57 Gbps (cinquenta e sete Gigabits por segundo) e com, pelo menos, as funcionalidades de Firewall, IPS, Application Control e logs habilitadas;

4.3. Throughput de Threat Prevention de, no mínimo, 20 Gbps (vinte Gigabits por segundo) incluindo, pelo menos, as funcionalidades de Firewall, IPS, Application Control, filtro de URLs, proteção Anti-Malware e logs habilitados;

4.4. Número de conexões simultâneas de, no mínimo, 15.000.000 (quinze milhões);

4.5. Número de novas conexões por segundo de, no mínimo, 530.000 (quinhentos e trinta mil);

4.6. Deve suportar VPN IPSec client-to-site para no mínimo 6.000 usuários simultâneos;

4.7. Mínimo de 2 (dois) Discos Rígidos com capacidade, mínima, por disco de 960 GB (Gigabytes), tipo CFAST/SSD/M.2, operando em redundância, por appliance;

4.8. Mínimo de 4 (quatro) Interfaces 100/1000 GbE (UTP) por appliance;

4.9. Mínimo de 12 (doze) Interfaces SFP+(10Gb)/SFP(1Gb) por appliance.

Observação: As taxas de transferência (throughput) e quantidades de conexões devem ser comprovadas por meio de documentação técnica oficial do fabricante da solução.

5. Grupo 1 - Item 2 do Edital – Renovação de solução de alta disponibilidade para roteamento e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 12 meses.

5.1. Cada equipamento que compõe o cluster da solução Next Generation Firewall do

Tipo II deverá atender às seguintes especificações.

5.2. Throughput de NGFW mínimo esperado de, no mínimo, 28 Gbps (vinte e oito Gigabits por segundo) e com, pelo menos, as funcionalidades de Firewall, IPS, Application Control e logs habilitadas.

5.3. Throughput de Threat Prevention de, no mínimo, 10 Gbps (Dez Gigabits por segundo) incluindo, pelo menos, as funcionalidades de Firewall, IPS, Application Control, filtro de URLs, proteção Anti-Malware e logs habilitados.

5.4. Número de conexões simultâneas de, no mínimo, 7.000.000 (sete milhões).

5.5. Número de novas conexões por segundo de, no mínimo, 300.000 (trezentos mil).

5.6. Mínimo de 1 (um) Disco Rígido com capacidade mínima, por disco, de 480 GB (Gigabytes), tipo SSD, por appliance.

5.7. Mínimo de 8 (oito) Interfaces SFP+(10Gb)/SFP(1Gb) por appliance.

5.8. Mínimo de 8 (oito) Interfaces UTP 1Gb (Gigabit), tipo RJ-45 por appliance.

Observação: As taxas de transferência (throughput) e quantidades de conexões devem ser comprovadas por meio de documentação técnica oficial do fabricante da solução.

6. Características comuns para os equipamentos do Grupo 1 - Itens 1, 2 e 4 do Edital, Tipos I e II.

6.1. A seguir serão especificadas as características comuns para os equipamentos referentes ao Grupo 1, itens 1 e 2 do Edital e Termo de Referência da presente contratação.

6.2. O hardware para cada equipamento appliance que compõem o cluster deve constar as seguintes características:

a) Deve ser apropriado para o uso em ambiente tropical, com umidade relativa entre 10 e 85% (sem condensação) e temperatura ambiente na faixa de 0°C a 40°C;
b) O fluxo do ar refrigerado deve ser recebido pela parte dianteira e dispensado na parte traseira do equipamento;
c) Possuir 2 (duas) fontes de alimentação independentes, redundantes e com capacidade de substituição sem desligar o equipamento (*hot-swappable*), com alimentação nominal de 100~120VAC e 210~230VAC, frequência de funcionamento de 50 ou 60Hz,

ou ainda com ajuste automático de tensão e frequência (*auto-ranging*), por appliance;

d) Deverá vir acompanhado de cabos de alimentação para todas as fontes, com, no mínimo, 1,80m, com plugue tripolar 2P+T no padrão ABNT NBR 14136;

e) Deverá vir acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos, etc.) para fixação em bastidor (rack) padrão EIA-310 com largura de 19" (dezenove polegadas);

f) Possuir no mínimo 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI);

g) Possuir, no mínimo, 1 (uma) interface *out-of-band* dedicada para gerenciamento com capacidade compatível com o tipo do equipamento, I, II e III;

h) Possuir, no mínimo, 1 (uma) interface para o sincronismo de estados da solução de alta disponibilidade;

i) A interface de sincronismo não precisa, necessariamente, estar rotulada para a finalidade de sincronismo do recurso de alta disponibilidade, sendo aceitável qualquer interface do equipamento;

j) Possuir, no máximo, 4Us de altura;

k) Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, sem custos adicionais;

l) Possuir certificação de conformidade sustentável de acordo com os padrões EPA (Enviromental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Hazardous Substances), WEEE (Waste Electrical and Electronic Equipment) ou EMI Certifications FCC part 15, CE, EN55022, EN55024;

m) Possuir certificação de conformidade da ANATEL ou serem fabricados no Brasil;

n) Deve informar, no painel de gerência do equipamento, a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede, podendo ser mostrado também no sistema de gerência centralizado, e;

o) Deve informar, no painel de gerência do equipamento, o número de conexões simultâneas e de novas conexões por segundo do equipamento, podendo ser mostrado também no sistema de gerência centralizado.

6.3. Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale.

6.4. Cada equipamento (appliance) deve oferecer, no mínimo, as seguintes funcionalidades:

a) Suportar os protocolos IPv4 e IPv6;
b) Suportar, no mínimo, 1.024 VLANs no padrão IEEE802.1q;
c) Suportar agregação de links no padrão IEEE802.3ad;
d) Suportar o protocolo DHCP;
e) Suportar o protocolo NTP;
f) Suportar as funcionalidades de roteamento estático e dinâmico, em IPv4 e IPv6;
g) Suportar os protocolos RIP, OSPF v2, OSPF v3, BGP v4 (RFC 4271) e BGP v6;
h) Suportar os protocolos IGMP v2, IGMP v3 e PIM-SM;
i) Suportar os protocolos SNMP v2c e SNMP v3;
j) Possuir Management Information Base (MIB) própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;
k) Suportar Policy Based Routing (PBR), ou Policy Based Forwarding (PBF), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;
l) Suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), camada 2 de rede (*layer*-2), camada 3 de rede (*layer*-3), e suas combinações;
m) Permitir o acesso ao equipamento via CLI (console), SSH e interface web HTTPS;
n) Possuir funcionalidades de Backup/Restore de sua configuração e políticas de segurança;
o) Permitir o agendamento automático dos Backups, podendo ser realizado pela solução de gerenciamento;
p) Armazenar os Backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP e SCP, e;
q) Criptografar e autenticar a comunicação com a solução de gerenciamento centralizado.

6.5. Funcionalidades de identificação de usuários da solução (appliance):

a) Promover a integração com serviços de diretório LDAP, via serviço de diretórios OpenLDAP e Active Directory, baseados em caracteres da língua portuguesa, para a

identificação, autenticação, autorização e registro de eventos de acessos e ameaças;

b) Deve identificar de forma transparente os usuários autenticados por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory e servidores RADIUS, e ainda, para LDAP será admissível o uso de agentes nas estações de trabalho e servidores;

c) Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory, RADIUS e proxies internos;

d) Será permitido que a solução de gerenciamento centralizado possua um "appliance virtual" específico para atendimento às necessidades de identificação e autenticação de usuários;

e) Possuir portal de autenticação (*Captive Portal*) para a identificação e autenticação de usuários não registrados ou não reconhecidos por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory, servidores RADIUS;

f) O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP via serviço de diretórios OpenLDAP e Active Directory;

g) Permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP via serviço de diretórios OpenLDAP e Active Directory;

h) Registrar a identificação do usuário em todos os logs de eventos de acesso e de ameaças gerados pelo equipamento;

i) Registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (*batches*) ou processos de correlação após a ocorrência do evento em questão, e;

j) Deve estar licenciado e permitir a identificação e autenticação de pelo menos 10.000 (dez mil) usuários simultâneos.

6.6. Funcionalidades de Firewall por equipamento (appliance)

a) Não deve possuir restrições ao número de máquinas ou usuários protegidos;

b) Suportar a implementação tanto em modo transparente (*layer*-2) quanto em modo gateway (*layer*-3);

c) Suportar inspeção Stateful de tráfegos IPv4 e IPv6;

d) Suportar controle de acesso para pelo menos 90 serviços e protocolos pré-definidos;

e) Suportar os protocolos para transmissão de áudio e vídeo H.323, SIP e MGCP;

f) Suportar os protocolos de Streaming com compressão RTCP, RTMP, RTSP e RTP;

g) Implementar mecanismo de conversão de endereços NAT (*Network Address Translation*), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT, dependendo da origem, destino ou porta);

h) Permitir transição entre endereços de redes IPv4 e IPv6, permitindo a comunicação entre dispositivos que usam esses protocolos diferentes, por meio de NAT N46 (que permite IPv4 acessar IPv6) e NAT64 (que permite IPv6 acessar IPv4).

i) Permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;

j) Implementar mecanismo de proteção contra ataques de falsificação de endereços IP (*anti-spoofing*), tanto para IPv4 quanto para IPv6;

k) Implementar mecanismo de captura de pacotes;

l) Identificar os usuários para qualquer protocolo ou aplicação baseada em TCP/UDP, na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);

m) Suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6;

n) Suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período, e suas combinações;

o) Deve ser possível a aplicação de novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas, salvo as conexões atingidas pelas regras alteradas, e;

p) Possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: Endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, status dos flags “ACK”, “SYN” e “FIN” ou sinalizar nos logs que o *Three-way-handshake* não foi concluído com sucesso, ação sobre o pacote (permitido ou negado).

q) A solução deve ser capaz de exportar dados de fluxo de tráfego (flows) para ferramentas externas de monitoramento e análise, usando protocolos tais como IPFIX (IP *Flow Information Export*) ou sFlow ou Netflow;

6.7. Funcionalidades de geolocalização por equipamento (appliance):

a) Identificar os países de origem e destino de todas as conexões estabelecidas com a Internet através do equipamento;
b) Suportar a atualização automática das listas de geolocalização;
c) Aplicar as atualizações sem perda das conexões ativas;
d) Armazenar as listas de geolocalização no próprio equipamento;
e) Permitir a criação de políticas de segurança baseadas em geolocalização, permitindo também o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países;
f) Possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças;

6.8. Funcionalidades de controle de acesso à Internet por equipamento (appliance)

a) Prover o controle e a proteção de acesso à Internet por meio do reconhecimento das aplicações, independente de porta e protocolo, e da classificação de URLs;
b) Identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas;
c) Identificar se as aplicações estão utilizando sua porta default;
d) Identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS;
e) Identificar aplicações criptografadas usando SSL/TLS;
f) Identificar um mínimo de 5.000 (cinco mil) aplicações, incluindo, mas não se limitando a: *peer-to-peer*, *streaming* de áudio e vídeo, *update* de *software*, instant messaging, redes sociais, *proxies*, *anonymizers*, acesso e controle remoto, VoIP e e-mail;
g) Deve ser capaz de identificar, pelo menos, as seguintes aplicações: Torrent, TOR, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook,

   Facebook Messenger ou Facebook Chat, Google+, Google Chat, Tinder, Instagram, Twitter (X), Linkedin, Dropbox, Google Drive, One Drive, Logmein, TeamViewer, MSRDP, VNC, Ultrasurf, Webex, Zoom;
h) Permitir a criação de assinaturas para identificação de aplicações proprietárias do órgão, sem a necessidade de ação ou intervenção do fabricante;
i) Suportar a atualização automática da base de assinaturas utilizada na identificação das aplicações;
j) Permitir aplicar as atualizações sem perda das conexões ativas e das assinaturas

customizadas;

k) Armazenar preferencialmente a base de assinaturas no próprio equipamento, aceitando-se também na solução de gerenciamento centralizado;

l) Classificar as aplicações em categorias, tecnologia e fator de risco;

m) Identificar os usuários que estão utilizando as aplicações, na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);

n) Permitir o bloqueio de aplicações que não estejam utilizando suas portas default;

o) Suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. As políticas descritas poderão ser aplicadas individualmente ou combinadas, conforme a necessidade da contratante;

p) Permitir a utilização ou bloqueio individualizado das aplicações, para determinados usuários ou grupo de usuários;

q) Permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado;

r) Permitir o controle de uso de banda de *download* ou *upload* utilizada pelas aplicações (*traffic shaping*) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. Os controles descritos poderão ser aplicados individualmente ou combinados, conforme a necessidade da contratante;

s) Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categorias;

t) Possuir, no mínimo, 60 categorias de URLs, incluindo, mas não se limitando, às seguintes categorias ou suas semelhantes[2]: *adult, chat, drugs, gambling, games, hacking, hate speech, remote proxies, social networks, streaming média, violence, weapons*;

u) Permitir sobrescrever as categorias de uma URL que se considere indevidamente classificada;

v) Permitir a criação de categorias/listas customizadas;

w) Permitir a inclusão de URLs customizadas nas categorias já existentes ou previamente customizadas;

x) Suportar a atualização automática das listas de categorias, e aplicação das atualizações

sem perda das conexões ativas e das URLs customizadas;

y) Armazenar as listas de categorias no próprio equipamento ou na solução de gerenciamento centralizado;

z) Deve identificar os usuários que estão acessando as páginas web na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);

aa) Suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. As políticas descritas poderão ser implementadas individualmente ou combinados, conforme a necessidade da contratante;

bb) Alertar o usuário quando uma URL for bloqueada por meio da página de bloqueio que possa ser customizada no próprio equipamento, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada;

cc) Permitir o bloqueio e continuação da navegação web (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" ou a inclusão de usuário e senha, para possibilitar o usuário continuar acessando o site), e;

dd) Registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado;

6.9. Funcionalidades de prevenção de ameaças por equipamento (appliance):

a) Possuir, no mínimo, funcionalidades de IPS, Antivírus, Anti-Bot, Anti-Malware e Anti-Spyware;

b) Possuir, no mínimo, os seguintes mecanismos de detecção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, detecção baseada em comportamento, nível de severidade do ataque e nível de confiança de detecção do ataque;

c) Possuir proteção contra ataques de negação de serviço DoS e DDoS;

d) Possuir assinaturas para bloqueio de ataques "buffer overflow";

e) Possuir mecanismo automático de captura de pacotes de eventos de IPS, para fins de "troubleshooting" e análise forense;

f) Deve ser capaz de inspecionar tráfego criptografado usando protocolo SSL/TLS;
g) Deve ser capaz de inspecionar integralmente todos os pacotes de dados, sem prejuízo na performance do equipamento, até os limites indicados nas seções 1.1., 1.2 e 1.3;
h) Possuir referência cruzada da base de assinaturas de detecção com os identificadores CVE (*Common Vulnerabilities and Exposures*);
i) Possibilitar a criação de assinaturas customizadas;
j) Identificar os usuários relacionados aos eventos de IPS na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);
k) Possibilitar a criação de políticas de segurança que emitam alertas, sem realizar bloqueios, ao detectar a ocorrência de um ataque específico, identificando sua origem ou destino com base em um endereço IP ou rede CIDR específicos;
l) Permitir a criação de políticas de segurança capazes de bloquear ataques específicos por meio de ações como DROP (descarte) e/ou RESET (reinicialização da conexão), com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;
m) Permitir a criação de exceções ou exclusões para a inspeção de uma determinada assinatura ou grupo de assinaturas, com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;
n) Registrar todos os eventos de IPS, incluindo o usuário identificado;
o) Identificar e bloquear a comunicação com botnets;
p) Bloquear *malwares* e *spywares*;
q) Inspecionar e bloquear vírus, ao menos, nos seguintes tipos de tráfego: FTP, HTTP, HTTPS e SMTP;
r) Suportar proteção contra vírus em conteúdo HTML e javascript, *software* espião (*spyware*) e *worms*;
s) Suportar a inspeção de vírus em arquivos comprimidos utilizando algoritmo deflate, como o padrão zip, gzip, entre outros;
t) Suportar bloqueio de *download* de pelo menos 50 tipos de arquivos como, arquivos tipo Executáveis, PDF, DLLs, Arquivos de Código, MSI, doc, xls, ppt, entre outros;
u) Suportar a atualização automática das bases de assinaturas para prevenção de ameaças;
v) Suportar aplicação das atualizações de prevenção de ameaças sem reinicialização do equipamento e nem perda das conexões ativas que não sejam afetadas pelas

atualizações;

w) Armazenar as bases de assinaturas de prevenção de ameaças no próprio equipamento ou na solução de gerenciamento centralizado;

x) Identificar os usuários relacionados aos eventos de bloqueio relacionados a prevenção de ameaças na forma da seção 1.4.4 - Funcionalidades de identificação de usuários da solução (appliance);

y) Permitir a criação de políticas de segurança que gerem alertas, sem realizar bloqueios, ao detectar a ocorrência de uma ameaça específica, com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;

z) Permitir a criação de políticas de segurança que bloqueiem a ocorrência de ameaças específicas com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos, e;

aa) Suportar notificações e alertas sobre ameaças via e-mail, SNMP traps e log de pacotes;

6.10. Características de QoS por equipamento (appliance):

a) Permitir o controle de tráfego com base nas aplicações com, no mínimo as ações: permitir, negar, agendar o uso, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou cada usuário;

b) Suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp);

c) Suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP e RTP;

d) Suportar a marcação de pacotes DiffServ;

e) Permitir o monitoramento do uso da priorização de tráfego que as aplicações fazem por bytes, sessões e por usuário.

6.11. Características de inspeção SSL/TLS por equipamento (appliance):

a) Identificar, descriptografar e analisar o tráfego SSL e TLS 1.2/1.3 tanto em conexões de entrada (*Inbound*) quanto de saída (*Outbound*);

b) Deve permitir a descriptografia da área útil do pacote de dados (*payload*) para fins de controle de acesso à Internet e proteção contra ameaças, e;

c) Permitir a diferenciação de conexões pessoais (Bancos, *Shopping*, etc.) e conexões

não pessoais por meio de classificação automática.

6.12. Características de VPN por equipamento (appliance):

a) Deve disponibilizar licenciamento para VPN *site-to-site*, sem limite do número de usuários simultâneos e sem limite do uso de túneis;
b) Suportar VPN *site-to-site* em topologias *Full Meshed* (todos os *gateways* possuem links específicos para todos os demais *gateways*) e também Estrela (*gateways* satélites se comunicam somente com um único *gateway* central);
c) Suportar, pelo menos, criptografias AES-128, AES-256;
d) Suportar integridade de dados com SHA-1 e SHA-256;
e) Suportar o protocolo IKE, fases I e II;
f) Suportar os algoritmos RSA e pelo menos 4 dos grupos Diffie-Hellman groups 1, 2, 5, 14, 15, 16, 17, 18;
g) Suportar NAT-T (NAT Transversal);
h) Deve possuir cliente próprio para instalação nos dispositivos fixos e móveis dos usuários, sem custo adicional e sem limite do número de usuários, e;
i) O cliente de VPN *client-to-site* deve ser compatível, ou suportar, o cliente nativo de pelo menos os seguintes Sistemas Operacionais: Windows 10 e Windows 11, Apple IOS versão 15 ou superior, Android versão 14 ou superior, Mac OS e Linux.
j) Deve permitir conexão VPN *client-to-site* de forma *Clientless*, com autenticação via *browser*, para fechar a VPN através de um portal TLS;
k) Deve suportar atribuição de endereço IP e de DNS nos clientes remotos de VPN;
l) Suportar Autenticação em Dois Fatores (2FA) para VPN, para os 6.000 usuários previstos, sendo uma autenticação via usuário e senha, validados por bases LDAP com uso de serviço de diretórios OpenLdap, Active Directory, e base de usuários interna do appliance. Já o segundo fator pode ser Token gerado por e-mail (obrigatoriamente) e também protocolo TOTP e Certificado digital, admite-se ainda que o segundo fator seja implementado com ferramenta de terceiros;
m) Em relação ao certificado digital do item anterior, deverá ser compatível com: certificado emitido por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, CA externa de terceiros, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, e

certificados emitidos por autoridade certificadora no padrão ICP-Brasil;

n) O túnel VPN do cliente ao *gateway* (*client-to-site*) deve fornecer uma solução de autenticação única (*single-sign-on*) aos usuários, integrando-se, no mínimo, com as ferramentas de Windows *login* da empresa Microsoft;

o) Permitir criação de políticas para usuários e grupos para tráfego de VPN *client-to-site*;

p) Integrar com serviços diretórios LDAP, via OpenLDAP e Active Directory, para a autenticação de usuários de VPN e também definição de regras de acesso;

q) Permitir a definição de condições específicas para autorizar o acesso remoto às redes internas via VPN *client-to-site*, garantindo maior segurança e controle. Entre essas condições, é necessário, no mínimo, suportar a verificação das versões dos Sistemas Operacionais dos dispositivos dos usuários, a exigência de um software antivírus instalado, ativo e com as definições atualizadas, e a validação das últimas atualizações "KBs" da Microsoft para ambientes Windows. Além disso, o sistema deve permitir a criação de uma lista de equipamentos autorizados, utilizando filtros como MAC-Address ou Hostname, e incluir restrições adicionais baseadas em registros do sistema (*registry*) do Windows. As condições descritas poderão ser aplicadas individualmente ou combinadas, conforme a necessidade da contratante;

r) Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12;

s) Suportar a leitura e verificação de CRLs (*certification revogation* lists), e;

t) Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL/TLS.

6.13. Funcionalidades de Prevenção de Perda de Dados (Data Loss Prevention)

a) Evitar vazamento de informações em meio digital (Data Loss Prevention- DLP), atuando de maneira preventiva por meio do monitoramento de mensagens e arquivos transitados, e;

b) Caso seja identificado algum conteúdo que não deve ser transitado, a solução deve alertar o usuário que este conteúdo é sensível, ou mesmo bloquear o tráfego associado, baseado em filtros de conteúdo definidos pelo contratante.

6.14. Características da alta disponibilidade:

a) Deve operar em alta disponibilidade (HA) nativamente no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo, com sincronismo de estados integrado;
b) Suportar o balanceamento de carga interno na arquitetura ativo/ativo, disponibilizando a capacidade agregada dos dois equipamentos no cluster;
c) Suportar, no mínimo, 2 equipamentos por cluster. No caso de uso de três equipamentos será permitido que um permaneça em *stand by*;
d) Deve sincronizar entre os nós do Cluster todas as configurações recursos necessários para que a solução mantenha o funcionamento pleno em caso de falha de um dos equipamentos, como conexões e sessões TCP/IP, tabelas NAT, listas e assinaturas utilizadas para controle de acesso à Internet e proteção contra ameaças, tabelas FIB, associações de segurança das VPNs, entre outros.
e) Monitorar a falha dos links de comunicação e entre os nós do cluster;
f) Identificar e transferir automaticamente a operação do sistema (procedimento de *failover*) sempre que ocorrer: Falha de um cluster (quando existirem mais de um cluster instalado no contratante), transferindo a carga para o outro em data center distinto. Falha de um dos membros do cluster. Falha de qualquer componente ou processo crítico de um dos membros do cluster. Falha de um dos links de comunicação monitorados, e;
g) Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e interrupções no tráfego.

6.15. Funcionalidades para tratamento de ameaças desconhecidas (Zero-Day)

a) Deve contemplar ferramenta compatível com conceito de Sandboxing para prevenção de ataques *zero-day*;
b) Prevenção de ataques por meio do bloqueio efetivo de *malwares* desconhecidos (Dia Zero), oriundos da comunicação Web (HTTP e HTTPS), FTP, SMTP e IMAP/POP3 durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente;
c) O envio de conteúdo para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

d) A funcionalidade de Sandbox deverá ser implementada em nuvem, appliance físico ou em ambiente virtual.

e) Caso a solução de Sandbox seja disponibilizada em ambiente virtual, é de responsabilidade da contratada providenciar servidores e softwares necessários para o funcionamento da ferramenta.

f) Deve ser capaz de enviar para análise, no mínimo, arquivos tipo Executável, PDF, DLLs, Arquivos de Código e MSI;

g) Suportar a análise de arquivos maliciosos em ambiente emulado e controlado com, no mínimo, os sistemas operacionais Windows 10 ou superior, Mac OS X ou superior;

h) Ser capaz de inspecionar e prevenir *malwares* desconhecidos em tráfego criptografado SSL/TLS;

i) Manter a performance sem degradação, independentemente das funcionalidades ativadas. (Ex.: AntiMalware, IPS, URL Filtering, e demais);

j) Geração de relatórios decorrentes das análises de links em Sandbox em caso de identificação de *malwares* e sites hospedeiros de exploits;

k) Deve ser capaz de classificar sites falsos, e atualizar a base do filtro URL da solução, e;

l) Deve prover análise em tempo real de páginas maliciosas e dessa forma, permitir o bloqueio de páginas maliciosas antes mesmo da atualização das bases de dados de URLs do fabricante da solução.

7. Grupo I Item 3 do Edital – Renovação de solução de Gerenciamento Centralizado para os Itens 1, 2 e 4 do Grupo 1 com serviço de garantia, atualização e suporte técnico em regime 24x7 por 12 meses.

7.1. A solução de Gerência centralizada deve atender às seguintes especificações:

7.2. A solução centralizada deverá gerenciar, de forma integrada, todos os equipamentos dos Grupos I e II que terão a renovação de garantia estendida ou que o órgão vier a adquirir, em qualquer combinação e quantidade dentro dos limites registados.

7.3. A solução de gerenciamento centralizado deverá ser composta por, pelo menos, 1 (um) “appliance virtual” – solução de software baseada em máquina virtual, conforme os padrões estabelecidos pelo DMTF (Distributed Management Task Force), ou sistema operacional desenvolvido pelo próprio fabricante da solução degerenciamento que possa ser instalado e

executado em ambiente virtual.

7.4. Será instalada em ambiente de virtualização e hardware de propriedade do contratante.

7.5. A Licença de Software para administração / gerência deve estar disponível, para uso, integrada com a base de identificação de usuários do contratante, em até 60 dias da comunicação da assinatura do contrato.

7.6. A solução de gerência terá atualização e suporte pelo período de 12 meses a contar do seu recebimento definitivo. Deverá permitir sua utilização por tempo indeterminado, em sua última versão disponível na data do encerramento do período de 12 meses.

7.7. A solução de gerência deverá ser separada dos gateways de segurança, que irão gerenciar políticas de segurança de todos os Firewalls e funcionalidades solicitadas neste documento.

7.8. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.

7.9. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos gerenciados via plataforma de segurança.

7.10. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

7.11. Suportar acesso via SSH para gerência, via cliente do próprio fabricante ou WEB (HTTPS).

7.12. O gerenciamento deve permitir/possuir monitoramento de logs, ferramentas de investigação de logs e acesso concorrente de administradores via contas diferentes.

7.13. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comando.

7.14. A solução deve suportar a criação de regras com agendamento personalizado, permitindo configurar datas e horários de início e término para o uso de cada regra.

7.15. Suportar backup das configurações e reversão (rollback) de configuração, pelo menos, para a última configuração salva.

7.16. Suportar validação de regras antes da aplicação.

7.17. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras já existentes (shadowing).

7.18. Permitir a visualização dos logs em tempo real de uma regra específica, diretamente na mesma tela de configuração da regra selecionada, garantindo uma experiência integrada e facilitando o monitoramento e a análise imediata do tráfego associado.

7.19. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

7.20. Permitir a criação de certificados digitais para autenticação de usuários.

7.21. Geração de relatórios de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança. Deve permitir apresentar eventos em um único portal (dashboard). Também devem existir relatórios e telas de apresentação onde sejam apresentados os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing).

7.22. Permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

7.23. Permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0.

7.24. Permitir que os administradores consigam revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

7.25. Permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

7.26. Registrar logs, correlação de eventos e relatórios de auditoria dos administradores da solução.

7.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados.

7.28. Permitir a criação de relatórios personalizados.

7.29. Permitir criar relatórios com o resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de usuários específicos e grupos de usuários do AD/LDAP. Os relatórios de usuários e grupos devem incluir as aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware) de rede vinculadas a este tráfego.

7.30. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução.

7.31. Possibilitar exportação dos logs em formatos CSV ou TXT.

7.32. Aplicar separadamente proteções relacionadas a ameaças e regras de acesso.

7.33. Para evitar erros na alteração de políticas, a solução deve combinar configuração de políticas e análise de logs em um único painel.

7.34. O visualizador de log deve ter um recurso de pesquisa.

7.35. Possibilitar a geração de relatórios de eventos no formato PDF.

7.36. Possibilitar rotação do log.

7.37. O gerenciamento centralizado deverá ser entregue como appliance virtual em formato compatível/homologado com tecnologia NUTANIX AHV.

7.38. A solução de gerenciamento deve possuir a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estando em ambientes físicos (on premises), virtualizados e nuvens públicas (AWS e Azure).

7.39. Possuir capacidade de integração com soluções de terceiros via API e suportar configurações por meio de RestAPI.

7.40. Consolidar logs e relatórios de todos os dispositivos administrados pela gerência integrada.

7.41. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.

7.42. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real.

7.43. Nas opções de Drill-Down deve ser possível identificar os acessos específicos de cada usuário.

7.44. Permitir que os relatórios possam ser salvos, enviados por e-mail e impressos.

7.45. Deve permitir a criação de filtros na visualização on-line dos relatórios com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

7.46. Permitir visualização via painel de gerência on-line da quantidade de tráfego utilizado de aplicações e navegação para permitir análise avançada de incidentes.

7.47. Gerar relatório dos eventos de ataque de forma completamente visual, contendo, no mínimo, gráficos de consumo de banda utilizado pelos ataques e quantidade de eventos de segurança gerados e também eventos de segurança protegidos.

7.48. Permitir a integração com servidores de autenticação por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory e servidores RADIUS.

7.49. Criar certificados digitais para acesso dos usuários VPN.

7.50. Criar certificados digitais para VPNs Site-to-Site.

7.51. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplada a sua maior capacidade ou a capacidade de criação de certificados deve ser ilimitada.

7.52. Permitir criação de políticas de acesso de usuários autenticados por meio dos serviços de diretório OpenLDAP com protocolo LDAP e Microsoft Active Directory, de forma que os usuários sejam reconhecidos de forma transparente.

7.53. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças classificadas por origens e destinos do tráfego de dados.

7.54. Possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado, permitindo a procura correlacionada de logs em uma única tela, como por exemplo: pesquisar logs

de Antivírus e navegação web simultaneamente na mesma consulta (query de pesquisa).

7.55. O relatório das emulações (sandboxing) deve conter deve conter um dos seguintes conjuntos de informações:

a) Print screen dos arquivos emulados, todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações individualizado para cada SO emulado, ou;
b) Tipo do arquivo, tamanho do arquivo, nome do arquivo, hash do arquivo, usuário que o recebeu, o veredito (um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema).

7.56. Possibilitar a procura por IPs e redes, de forma que os resultados mostrem estes IPs e redes nos campos de origem e destino dos logs na mesma tela de pesquisa;

7.57. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

7.58. Capacidade de personalização de gráficos com os dados dos logs, como barra, linha e tabela;

7.59. Permitir a criação de painéis (dashboards) customizados para visualização do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

7.60. Possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema e dos componentes gerenciados por ele, contendo, no mínimo, licenças ativas, utilização de memória, utilização de discos e uso de CPUs;

7.61. Ser capaz de correlacionar eventos de todas as suas fontes de log em tempo real;

7.62. Fornecer conteúdo de correlação de eventos pré-definido organizado por categoria;

7.63. Monitorar alterações, análise e otimização de regras de políticas de segurança;

7.64. Possibilitar a verificação de regras de acesso por meio de uma consulta de origem, destino e serviço, a solução também deve apresentar se o tráfego está permitido, bloqueado ou parcialmente permitido/bloqueado, demonstrando os dispositivos no caminho, roteamento e interfaces;

7.65. Deve apresentar relatórios de otimização de regras e objetos, no mínimo, contendo as seguintes informações:

a) Regras não usadas;
b) Regras cobertas
c) Consolidar regras
d) Regras desabilitadas
e) Regras temporárias (definição de data e hora de funcionamento)
f) Regras mais usadas;
g) Última vez que uma regra foi usada;
h) Objetos duplicados;
i) Objetos vazios, e;
j) Serviços duplicados.

7.66. Permitir a monitoração de itens de configuração do sistema operacional dos dispositivos gerenciados;

7.67. Enviar alertas configuráveis sobre regras a expirar;

7.68. Emitir alertas em caso de alterações de configuração que não estão em conformidade com os padrões e políticas corporativas vigentes;

7.69. Realizar a comparação das configurações de um mesmo ou entre diferentes dispositivos;

7.70. Permitir o agendamento para a geração de relatórios dos dispositivos gerenciados;

7.71. Ser capaz de fornecer lista de usuários de VPN dos dispositivos gerenciados, no mínimo, baseados nos seguintes critérios:

a) Data de criação;
b) Grupos de usuários;
c) Métodos de autenticação dos usuários, e
d) Data de expiração dos usuários.

7.72. A comunicação entre a solução e os dispositivos de segurança gerenciados deve ser autenticada e criptografada;

7.73. Todas as funcionalidades descritas para a solução de Next Generation Firewall devem estar devidamente licenciadas e disponíveis para uso durante todo o período do contrato.

Sendo elas, Application Control, identificação de usuários, firewall, geolocalização, navegação internet e inspeção de tráfego SSL/TLS, IPS, VPN, ameaças zero-day, sandboxing, logging, gerência centralizada, SD-WAN e demais funcionalidades necessárias para completa utilização dos equipamentos.

8. Grupo I Item 4 do Edital – Renovação de licenças, suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.

8.1. O objeto deste item é a renovação, pelo período de 12 (doze) meses, das licenças de software, das assinaturas de proteção, do direito de atualização de versões e dos serviços de suporte técnico e garantia da solução dedicada de proteção contra ataques de negação de serviço distribuído (DDoS) já instalada e em produção no ambiente da CONTRATANTE. Não se trata de aquisição de novo equipamento, e sim da continuidade da cobertura do ativo existente.

8.2. A solução objeto da renovação é a seguinte:

a) Fabricante: Check Point Software Technologies;
b) Modelo: DDoS Protector 6-2;
c) Código do fabricante (part number): CPAP-DP6-2-SME;
d) Quantidade: 1 (um) appliance;
e) Capacidade máxima de mitigação de ataques: 6 Gbps (seis Gigabits por segundo);

8.3. Capacidade de proteção de tráfego legítimo (clean traffic): 2 Gbps (dois Gigabits por segundo).

8.4. O número de série do equipamento será informado pela CONTRATANTE à CONTRATADA na reunião inicial de alinhamento, para fins de registro da renovação junto ao fabricante.

8.5. A renovação deverá recair sobre o mesmo ativo identificado no item anterior, com o contrato de suporte registrado junto ao fabricante e vinculado ao número de série do equipamento da CONTRATANTE, que figurará como titular (end user) do licenciamento.

8.6. A vigência de 12 (doze) meses deverá iniciar no dia imediatamente subsequente ao término da cobertura atualmente vigente, de forma a não haver qualquer intervalo de descobertura. Caso, na data da contratação, a cobertura anterior já se encontre expirada, eventuais custos de reativação (reinstatement) cobrados pelo fabricante correrão por conta da

CONTRATADA, sem ônus adicional para a CONTRATANTE.

8.7. Durante toda a vigência contratual deverão permanecer licenciadas, ativas e plenamente operacionais todas as funcionalidades de proteção descritas nos itens subsequentes, sem redução de escopo, de capacidade de mitigação, de desempenho ou de nível de serviço em relação à cobertura atualmente vigente.

8.8. A renovação deverá assegurar o direito de atualização de software durante todo o período contratado, contemplando, no mínimo:

8.8.1. novas versões de software (major e minor), correções, patches e hotfixes disponibilizados pelo fabricante para o modelo em uso;

8.8.2. atualização contínua das bases de assinaturas de ataques, de vulnerabilidades e de reputação utilizadas pelos mecanismos de proteção da solução;

8.8.3. acesso ao portal de suporte, à base de conhecimento e à documentação técnica oficial do fabricante.

8.9. O serviço de suporte técnico deverá ser prestado em regime 24x7 (vinte e quatro horas por dia, sete dias por semana, inclusive sábados, domingos e feriados) durante os 12 (doze) meses de vigência, admitindo a abertura de chamados diretamente junto ao fabricante ou por intermédio da CONTRATADA, sem prejuízo dos níveis de serviço estabelecidos neste Termo de Referência.

8.10. A garantia deverá abranger a substituição de partes, peças e do próprio equipamento em caso de defeito, durante toda a vigência contratual, sem custo adicional para a CONTRATANTE.

8.11. A CONTRATADA deverá comprovar o registro da renovação junto ao fabricante em até 10 (dez) dias corridos contados da assinatura do contrato, mediante documento emitido pelo próprio fabricante contendo, no mínimo, o número de série do equipamento coberto, o escopo das licenças e assinaturas renovadas e as datas de início e término da cobertura.

8.12. Por se tratar de renovação de cobertura sobre ativo já instalado, não será admitida, para atendimento deste item, a substituição da solução por serviço de mitigação em nuvem, por módulo ou licença de proteção contra DDoS embarcado em firewall, roteador ou balanceador de carga, nem por equipamento de fabricante ou modelo diverso do identificado neste item,

ressalvada exclusivamente a hipótese prevista no item seguinte.

8.13. Caso o fabricante declare o modelo instalado em condição de End of Sale, End of Support ou End of Life, tornando inviável a renovação nos termos deste item, a CONTRATADA deverá comunicar formalmente a CONTRATANTE em até 5 (cinco) dias úteis contados do conhecimento do fato e apresentar plano de continuidade indicando o modelo sucessor do mesmo fabricante, com capacidade de mitigação de ataques e de tratamento de tráfego legítimo iguais ou superiores às indicadas neste item e com todas as funcionalidades exigidas neste Item 5, cabendo à CONTRATANTE deliberar sobre a solução a ser adotada, observada a legislação aplicável.

9. PROTEÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDO (DDOS)

9.1. O sistema deve proteger contra inundação de anomalias de pacotes. Ao menos:

9.1.1. Unrecognized L2 Format;

9.1.2. Incorrect IPv4 Checksum;

9.1.3. Invalid IPv4 Header or Total Length;

9.1.4. Invalid IP Header or Total Length;

9.1.5. Inconsistent IPv6 Headers;

9.1.6. Invalid L4 Header Length;

9.1.7. TTL Equal to 0;

9.1.8. IPv6 Hop Limit Reached;

9.1.9. Unsupported L4 Protocol;j) Invalid TCP Flags;

9.1.10. Source or Dest. Address same as Local Host;

9.1.11. Source Address same as Dest Address (Land Attack).

9.1.12. Protecão contra ataques DDoS em camada de rede. Ao menos:

9.1.13. TCP-SYN floods;

9.1.14. TCP ACK + fim Flood;

9.1.15. TCP-SYN + ACK floods;

9.1.16. TCP-RESET floods;

9.1.17. TCP fragments flood;

9.1.18. UDP Floods;

9.1.19. UDP Fragmented Floods;

9.1.20. ICMP Floods;

9.1.21. IGMP Floods.

9.2. Proteção de ataques DDoS em camada de aplicação. Incluindo ao menos:

9.2.1. Todos os tipos de ataques de tipo reflection, independente do protocolo camada 7 utilizado;

9.2.2. Todos os tipos de ataques de tipo Amplification, independente do protocolo camada 7 utilizado;

9.2.3. DNS Floods;

9.2.4. HTTP Floods;

9.2.5. Low and SLow.

9.2.6. O sistema deve ter proteção DDoS originada de trás de CDN ou proxies.

9.2.7. O sistema deve ter mecanismos de proteção para ataques de tipo dia zero e ataques conhecidos.

9.3. O sistema deve ter mecanismo de prevenção de falsos positivos DdoS através de desafios e respostas. Como mínimo:

9.3.1. Desafios e respostas para TCP;

9.3.2. Desafios e resposta HTTP: 302 Redirect, Java Script;

9.3.3. Desafios e resposta em DNS.

9.3.4. O sistema deve ter protecão TCP Out-of–State Flood Attack.

9.3.5. O sistema deve ter proteção granular para limitar por PPS e Kbps o tráfego enviado um destino com certos parâmetros definidos.

9.3.6. O sistema deve ter proteção contra ferramentas conhecidas de DoS.

10. ANÁLISE DE COMPORTAMENTO

10.1. O sistema deve proporcionar detecção de ataques DoS/DDoS em tempo real, baseado em Análise de Comportamento ou estatístico. Não se admitem soluções baseadas em limites estáticos de nenhum tipo já que se busca reduzir a quantidade de falsos positivos que possam existir na rede.

10.2. O sistema deve prevenir falsos positivos na detecção causados por flash crowds ou aumentos de tráfego súbito, através da correlação de parâmetros que variem com a taxa de tráfego com aqueles parâmetros que não variam com a taxa de tráfego.

10.3. Em fase de Proteção, O sistema deve atuar de forma automática, mitigando o ataque sem intervenção humana.

10.4. O sistema não deve realizar mitigação através de rate limits. A mitigação do ataque deve ser cirúrgica, unicamente bloqueando o tráfego que corresponda ao ataque e deixando passar o tráfego legítimo, ainda que o endereço IP de origem seja o mesmo do atacante.

10.5. O sistema deve suportar proteção comportamental ou estatística contra o mal uso da aplicação ou da red o contra-ataques de DoS e DDoS. A proteção comportamental deve resultar na criação de uma contra-medida em tempo real para a mitigação dos ataques de forma imediata.

10.6. O sistema deve ter proteção contra vetores de ataques previamente desconhecidos.

10.7. O sistema deve proteger contra-ataques DDoS de tipo Burst utilizando.

10.8. Análise de Comportamento e mitigação cirúrgica automática, em tempo real.

10.9. O sistema deve basear sua decisão de bloqueio na informação de excesso de tráfego contida em Burst prévios e deve ser capaz de readaptar-se em caso de que o vetor de ataques DDoS no Burst varíe.

10.10. O sistema deve detectar e bloquear Comportamentos anômalos próprios de scans de IP e portas à rede, com o fim de prevenir a enumeração de recursos da entidade.

11. PROTEÇÃO DNS

11.1. O sistema deve suportar proteção DDoS DNS baseado em Análise de Comportamento

de aplicação.

11.2. O sistema a nível de Análise de Comportamento ou estatístico DNS deve observar os seguintes parâmetros:

11.3. O sistema deve suportar um método de proteção de DNS mediante mecanismos de segurança positiva e negativa que permitam a proteção de ataques.

11.4. O sistema deve suportar sistemas de proteção de DNS Challenge para limitar o tráfego malicioso mediante mecanismos de descarte de pacotes que reduzam os falsos positivos.

11.5. O sistema deve permitir crear listas brancas de subdomínios de forma manual ou automática.

11.6. A proteção de DNS deve ser completamente Stateless, Ingress-Only e não deve realizar contagens de NXDomains.

12. PROTEÇÃO SSL/TLS

12.1. A solução deve contar com hardware dedicado, o qual poderá ser interno ou externo, para o tratamento de tráfego SSL.

12.2. Proteção contra ataques DDoS Criptografados com SSL / TLS tanto na camada SSL como na camada HTTPS.

12.3. A solução deve poder autenticar sessões SSL com módulo de criptografia SSL para autenticar sessões legítimas e bloquear sessões de ataque criptografados por SSL.

12.4. A proteção SSL contra ataques de Negação de serviços, no deve cifrar/descifrar o tráfego quando não há ataque. A proteção só deve atuar em caso de ataque.

12.5. A proteção SSL deve funcionar em modo Ingress Only, sem necessidade de ver o tráfego que vem do servidor. Em outras palavras, a proteção deve ser Stateless.

12.6. O sistema deve habilitar flexibilidade com certificados wildcard de SSL, com o objeto de simplificar as operações e minimizar o número total de certificados administrados.

13. PERFIS DE GEOLOCALIZAÇÃO

13.1. A solução deve prover proteção de geolocalização que visualize os principais países atacantes de DDoS utilizando um mapa em tempo real.

13.2. A solução deve bloquear o tráfego de países específicos de imediato, com um clique de um botão na console de administração, utilizando um novo mapa de ataque dedicado, que apresente os principais países atacantes.

13.3. A solução de mitigação deve suportar dois modos de ativação de bloqueio:

13.4. Sempre ativo e sob demanda.

13.5. A proteção deve admitir a configuração de listas de bloqueio/lista de permissões por objeto protegido, e que permita aos operadores da entidade a Capacidade de configurar rapidamente o bloqueio de país e as listas de permissões.

14. PROTEÇÃO CONTRA ATAQUES CONHECIDOS

14.1. A solução deve contar com um mecanismo de proteção de ataques DdoS lançados com ferramentas Conhecidas o que utilizem exploits conhecidos. Este mecanismo deve estar baseado em uma base de dados de assinaturas que contenha os parâmetros necessários para identificar estes ataques conhecidos.

14.2. As assinaturas devem ser atualizadas de forma automática através da internet durante a duração do suporte.

14.3. Ao ser a primeira linha de defesa, além de ataques DDoS Conhecidos deve proteger ao menos contra seguintes vulnerabilidades:

14.3.1. Web application vulnerabilities;

14.3.2. Mail server vulnerabilities;

14.3.3. FTP servers vulnerabilities;

14.3.4. DNS Vulnerabilities;

14.3.5. SQL Servers Vulnerabilities;

14.3.6. VoIP (SIP) vulnerabilities;

14.3.7. Buffer overflow.

15. REQUISITOS TÉCNICOS SISTEMA DE ADMINISTRAÇÃO CENTRALIZADA

15.1. O sistema deve suportar administração centralizada para toda a solução de DDoS.

15.2. O sistema deve ser tipo virtual appliance que permita instalar-se sobre Hyper-V ou

VMware ESXi 5 ou superior na infraestrutura do cliente.

15.3. Deve-se incluir as licenças necessárias para poder ter Capacidade completa de realizar alterações e configurações da solução de mitigação de ataques.4.1.9.4. O sistema deve suportar Web User interface para toda a configuração do dispositivo.

15.4. O sistema deve suportar um padrão industrial API para integração com aplicações personalizadas. A API deve ser oferecida sem custos.

15.5. A API deve estar completamente documentada.

15.6. A solução de administração deve prover a opção de personalizar “dashboards” por usuário, por política que mostrem informação em tempo real como: “top attacks view, traffic monitoring view, SLA reports (bandwidth consuming attack) view, etc”.

15.7. O sistema deve suportar Acessos seguros HTTPS, SSH.

15.8. O sistema deve suportar o envio de eventos através de SYSLOG e SNMP.

15.9. O sistema deve suportar a configuração da solução através de scripts.

15.10. O sistema deve suportar RBAC para os administradores de múltiplos dispositivos.

15.11. O sistema deve suportar LDAP, RADIUS, TACACS e autenticação local.

15.12. O sistema deve suportar guardar toda a configuração em um servidor remoto baseado em uma interface GUI.

15.13. O sistema deve suportar múltiplos administradores logados ao tempo na interface GUI.

15.14. O sistema deve suportar NTP.

15.15. O sistema deve gerar um alarme por cada alteração administrativa feita no dispositivo.

15.16. O sistema deve prover os MIBS completos.

15.17. O sistema deve suportar realização de backups por SCP, FTP, SFTP.

15.18. O sistema deve suportar ferramentas de diagnóstico como core dumps, arquivos de configuração, logs, etc.

15.19. O sistema deve suportar REST sobre HTTPS.

15.20. O sistema deve suportar a criação de scripts personalizados pela entidade que podem ser executados sobre múltiplos dispositivos ao mesmo tempo.

15.21. O sistema deve suportar relatórios históricos das soluções Anti DDoS.

15.22. Estes relatórios poderão ser programados e enviados de forma automática.

15.23. Deve contar com os seguintes protocolos para enviar os relatórios programados: via SFTP e SMTP.

15.24. Os seguintes são os formatos de relatórios que deve suportar o módulo de relatórios históricos: PDF, HTML, CSV, TXT.

15.25. Deve contar com filtros granulares para personalizar o tipo e a informação nos relatórios.

15.26. Deve contar com relatórios out of the box, entre relatórios gerais de segurança e relatórios específicos da solução.

15.27. Deve ter capacidade de gerar ao menos os seguintes relatórios:

15.27.1. Ataques por largura de banda;

15.27.2. Ataques por duração.

15.27.3. Ataques permitidos e negados;

15.27.4. Ataques críticos;

15.27.5. Relatórios de tipo TOP:

15.27.6. Destinos;

15.27.7. Origem;

15.27.8. Aplicação.

16. Grupo I - Item 5 do Edital – Solução para proteção de ferramentas colaborativas baseadas no Office 365 na nuvem, Harmony e-mail e collaboration por 12 Meses.

16.1. Requisitos Gerais e Arquitetura

16.1.1. A solução fornecida deve ser através de um serviço SaaS na nuvem.

16.1.2. O serviço SaaS deve contar com pelo menos alguma destas certificações:

16.1.3. SOC 2

16.1.4. ISO 27001

16.1.5. A solução deve ser reconhecida como uma solução líder em segurança de e-mail por analistas terceirizados como Forrester ou Gartner nos últimos 3 anos.

16.1.6. A disponibilidade do serviço SaaS deve ser de pelo menos 99,9%.

16.1.7. A solução deve usar protocolos de criptografia modernos para proteger a organização.

16.1.8. A solução deve ser escalável e nativa na nuvem para proteger centenas de milhares de usuários.

16.1.9. A solução deve proteger contra Ciberameaças para correio eletrônico na nuvem Office 365 e Google Workspace.

16.1.10. A solução deve suportar proteção contra Ciberameaças nas seguintes aplicações SaaS de colaboração e armazenamento de arquivos:

16.1.10.1. Slack

16.1.10.2. Microsoft Teams

16.1.10.3. Microsoft OneDrive

16.1.10.4. Microsoft SharePoint

16.1.11. A solução deve oferecer um serviço para 2.000 (dois mil) usuários/caixas de correio.

16.1.12. A solução deve prover proteção contra os seguintes tipos de ataques:

16.1.12.1. Prevenção contra ataques a correio eletrônico (Phishing, Spoofing, Spam)

16.1.12.2. Prevenção de Malware em e-mail, ferramentas de colaboração e armazenamento

16.1.12.3. Prevenção de Malware de dia zero com Sandboxing (em ferramentas de colaboração) e limpeza de documentos CDR

16.1.12.4. Anomalias de usuários e sinais de sessão anômalos (indicadores de roubo de conta)

16.1.12.5. Uso não autorizado de aplicações SaaS também conhecido como Shadow IT

16.1.12.6. Prevenção de fuga de dados (DLP) em correio eletrônico e ferramentas de colaboração

16.1.12.7. A solução deve permitir gestão, detecção, investigação e reparação de ameaças a partir de um painel de gestão unificado.

16.1.12.8. A plataforma deve ser administrada via HTTPS e ser compatível com os navegadores Chrome, Firefox e Edge.

16.1.12.9. A solução deve ser fácil e rápida de usar, com configurações de políticas prontas para uso.

16.1.12.10. Prevenção de Ataques a E-mail BEC, Phishing, Spam

16.1.12.11. A solução deve bloquear ataques sofisticados de engenharia social, como falsificação de identidade, spam, phishing de dia zero e comprometimento de e-mail corporativo (BEC), utilizando motores de machine learning (ML), Deep Learning e Inteligência Artificial (IA).

16.1.12.12. A solução deve proteger os e-mails de entrada, saída e proteger a comunicação interna em tempo real contra ataques laterais e ameaças internas.

16.1.12.13. A solução deve oferecer prevenção em linha (não apenas detecção e/ou remediação), ou seja, interceptar e-mails antes que cheguem ao usuário final.

16.1.12.14. A solução deve permitir a implantação automática por integração nativa via API sem exigir alterações nos registros MX do DNS para prevenir ataques por e-mail.

16.1.12.15. A integração via API deve ser automática e simples de gerenciar, permitindo regras granulares para usuários e/ou grupos que podem estar em prevenção e/ou remediação, sem necessidade de configurações manuais no serviço de e-mail (Microsoft 365).

16.1.12.16. A solução deve ser invisível para os atacantes e aplicar segurança em profundidade, atuando como uma camada segregada de defesa sem desativar a segurança nativa das soluções de e-mail na nuvem (Office 365).

16.1.12.17. A solução deve contar com um período de aprendizado que realize uma varredura de 12 meses de metadados de e-mail (remetente, destinatário, assunto, hora) nas caixas de correio dos usuários para determinar padrões de comunicação e ajustar os motores de IA.

16.1.12.18. A solução deve ter suporte multilíngue para análise do conteúdo das mensagens de e-mail utilizando Inteligência Artificial, incluindo pelo menos 100 idiomas, entre eles o contemplando, obrigatoriamente, os idiomas português (Brasil), inglês e espanhol.

16.1.12.19. A solução deve inspecionar metadados, arquivos anexos, links e idioma da comunicação, domínios, OCR, códigos QR, bem como todas as comunicações históricas, para determinar relações de confiança prévias entre remetente e destinatário e identificar falsificação de identidade ou mensagens fraudulentas.

16.1.12.20. A solução deve classificar (etiquetar) os e-mails de acordo com o tipo de ameaça identificada, contemplando, no mínimo, as seguintes categorias:

16.1.12.21. Extorsão

16.1.12.22. Falsificação de identidade

16.1.12.23. Fraude financeira

16.1.12.24. Engenharia social

16.1.12.25. Faturas falsas

16.1.12.26. Roubo de credenciais

16.1.12.27. Sextorsão

16.1.12.28. Texto ofuscado em HTML

16.1.13. A solução deve analisar cada e-mail como um todo e de forma individual, permitindo estabelecer pelo menos os seguintes pontos:

16.1.13.1. No nível de contexto do e-mail analisado:

a) Este remetente já escreveu para a organização antes?

b) Alguns usuários internos já tiveram contato prévio com este endereço ou domínio?

c) Qual é a relação entre o endereço externo ou domínio externo e a organização?

d) Quão comum é para esses destinatários da organização receberem o mesmo e-mail?

e) Este remetente já foi mencionado por usuários internos em algum e-mail anterior?

f) O endereço do remetente se parece com algum endereço interno ou externo

conhecido (endereço/domínio)?

16.1.13.2. No nível de conteúdo do e-mail analisado:

a) A estrutura do link é suspeita?

b) Os links contidos no e-mail são semelhantes aos usados em e-mails de phishing?

c) O link está ofuscado por algum método conhecido?

d) O link foi projetado para redirecionar o destinatário para um domínio diferente do sugerido pelo link original?

e) O anexo contém conteúdo potencialmente malicioso, como links ou macros?

f) Há sinais de tentativa de extorsão no corpo deste e-mail?

g) A linguagem do e-mail sugere que é um e-mail típico de phishing ou spam?

16.2. A solução deve ser capaz de analisar tanto o cabeçalho quanto o conteúdo da mensagem para detectar e identificar ataques de falsificação de domínio e falsificação de nome.

16.3. A solução deve realizar a verificação de mais de 200 indicadores de ataque sobre o e-mail, como a verificação DMARC, SPF ou DKIM, para confirmar se o e-mail se origina do suposto domínio de origem e, por meio de inteligência artificial, evitar ataques evasivos e sofisticados.

16.4. A solução deve ser totalmente compatível com os seguintes mecanismos de autenticação de e-mail:

16.4.1. Sender Policy Framework (SPF),

16.4.2. Domain Keys Identified Mail (DKIM),

16.4.3. Domain-based Message Authentication, Reporting & Conformance (DMARC).

16.5. A solução deve contar com a opção de configuração de listas brancas e listas negras.

16.6. A solução deve detectar quando os cibercriminosos utilizam o domínio de uma empresa para se passar pela marca ou seus funcionários.

16.7. A solução deve utilizar a integração com o diretório para criar automaticamente listas de usuários VIP para protegê-los contra-ataques de impersonação.

16.8. A solução deve inspecionar links quando o usuário clicar na URL, ou seja, reescrever

o(s) link(s) no e-mail.

16.9. A solução deve emular (sandboxing) os links reescritos para expor indicadores ocultos de phishing.

16.10. A solução deve permitir que os administradores detectem os usuários que clicaram em links maliciosos e que necessitam de maior educação e treinamento para evitar novos cliques.

16.11. A solução deve interagir com a Microsoft via API, sem gerar interferência quando MS ATP ou Defender inspecionam a URL antes da reescrita. Assim, pode ser usada como camada adicional de proteção.

16.12. A solução deve reescrever links no corpo do e-mail e também em links dentro de documentos anexos.

16.13. A solução deve permitir que os administradores configurem listas de exceções para e-mails detectados como maliciosos ou suspeitos.

16.14. A solução deve suportar a reescrita de URLs incorporadas, mesmo que sejam códigos QR, substituindo a imagem do QR no corpo do e-mail por um novo QR que aponte para um link reescrito.

16.15. A reescrita de links da solução deve ter a opção de ofuscar a rota completa da URL, deixando visível apenas o domínio, permitindo que os usuários compreendam aproximadamente para onde o link aponta, sem comprometer a segurança.

16.16. A solução deve ser capaz de colocar em quarentena e-mails, arquivos e mensagens conforme políticas de segurança e configuração dos motores de segurança.

16.17. A solução deve permitir, conforme política, que usuários finais enviem solicitações de restauração para e-mails em quarentena, e que administradores autorizados possam aprovar ou não essas solicitações.

16.18. A solução deve permitir que os administradores configurem notificações sobre solicitações de restauração para qualquer endereço de e-mail, como parte da equipe de suporte ou SOC, que receberá notificações e as gerenciará conforme seu SLA.

16.19. A solução deve permitir aos administradores configurar um remetente personalizado para as notificações enviadas aos usuários finais sobre a aprovação ou rejeição de solicitações de restauração de e-mails em quarentena e os relatórios sobre e-mails de phishing,

sendo possível configurar pelo menos os seguintes parâmetros:

16.19.1. Endereço do remetente

16.19.2. Nome do remetente

16.19.3. Endereço de resposta

16.20. Quando a organização utilizar soluções de Simulação e Treinamento de Phishing, nas quais são enviadas campanhas falsas para avaliar a resposta dos usuários e educá-los, a solução de segurança de e-mail deve detectar automaticamente esses relatórios e distingui-los de outros e-mails. Quando os usuários reportarem esses e-mails simulados, deve ser possível enviar uma resposta automatizada para reconhecer sua conscientização.

16.21. Para casos de spam, que são uma ameaça que principalmente desperdiça tempo e/ou impacta a produtividade do usuário, o spam pode ser válido para um funcionário ou não. Para evitar frustração do usuário final ao colocar algo desnecessário em quarentena ou movê-lo para a pasta de spam, e para evitar carga adicional para o suporte técnico devido à necessidade de criar exceções manuais, a solução deve permitir que os administradores autorizem os usuários finais a marcar remetentes e domínios como confiáveis, garantindo que os e-mails desses remetentes cheguem à caixa de entrada, mesmo se forem classificados como spam. E-mails classificados como phishing ou contendo malware devem continuar em quarentena.

16.22. Ao revisar os e-mails de resumo de quarentena diários ou visitar o portal de quarentena do usuário final, os usuários finais podem confiar nos remetentes. Dessa forma, os e-mails enviados por esses remetentes e marcados como Spam ou Graymail chegarão à caixa de entrada e não à pasta de lixo eletrônico ou quarentena.

16.23. A solução deve permitir aos administradores monitorar e gerenciar a lista de remetentes confiáveis pelo portal de gestão de Exceções de Anti-Spam.

16.24. Os administradores podem confiar nos remetentes globalmente para toda a organização. Eles devem poder editar ou adicionar remetentes confiáveis para destinatários específicos pelo portal da solução. Também devem poder adicionar remetentes confiáveis não apenas para um destinatário específico, mas para toda a organização. Assim, os e-mails desses remetentes confiáveis, mesmo se classificados como spam ou Graymail, chegarão à caixa de entrada do destinatário, independentemente de quem seja o destinatário.

16.25. Para e-mails de Graymail, que estão entre spam e e-mails profissionais do dia a dia, a solução deve permitir que organizações que utilizam Microsoft 365 Exchange Online movam automaticamente esses e-mails para uma pasta dedicada. A solução deve criar e manter a pasta de Graymail na caixa de entrada de todos os usuários finais, para que todos saibam exatamente onde encontrar esses e-mails.

16.26. A solução deve permitir que e-mails incluídos na lista de permitidos da solução também sejam permitidos pelo Microsoft/Google.

16.27. A solução deve contar com ações automatizadas como alertar o usuário no e-mail, mover para a pasta Spam/Junk, colocar o e-mail em quarentena e/ou adicionar um cabeçalho no e-mail.

16.28. A solução deve contar com ações automatizadas diferenciadas para phishing, malware, spam e e-mails de marketing.

16.29. A solução deve permitir que o administrador autorize os usuários finais a confiar nos remetentes para que e-mails classificados como spam sejam entregues na caixa de entrada. Em contrapartida, se os e-mails forem classificados como phishing ou contiverem malware, devem permanecer em quarentena.

16.30. A solução deve permitir que o administrador personalize os modelos usados para notificar os usuários finais sobre as ameaças.

16.31. A solução deve ter um período de retenção dos e-mails originais colocados em quarentena de pelo menos 180 dias.

16.32. A solução deve ter um período de retenção dos metadados dos e-mails analisados como maliciosos por pelo menos 180 dias.

16.33. A solução deve permitir conservar os e-mails colocados em quarentena pelo Microsoft por um período maior que a retenção padrão do Microsoft, podendo ser configurado até 180 dias.

16.34. A solução deve ter um período de retenção de todos os e-mails originais analisados por pelo menos 14 dias, mesmo que sejam classificados como limpos.

16.35. A solução deve permitir opcionalmente armazenar localmente os e-mails/arquivos em quarentena como backup.

16.36. A solução deve ter capacidade de remediação das ameaças que chegam às caixas de entrada dos usuários. A partir da interface de gestão, deve ser possível realizar identificação, análise e correção. Se um e-mail ou arquivo chegar, devem ser tomadas medidas imediatas em milhares de caixas de entrada com poucos cliques, sem PowerShell ou qualquer tipo de codificação.

16.37. A solução deve permitir que usuários e administradores forneçam comentários sobre e-mails suspeitos para ajudar na classificação de phishing.

16.38. A solução deve permitir que os usuários ajudem a detectar ataques não identificados e permitir que os administradores de segurança bloqueiem ataques detectados e previnam ataques semelhantes no futuro.

16.39. A solução deve se integrar com o mecanismo de relatório de spoofing do MS Outlook.

16.40. A solução deve permitir a adição de banners educacionais em e-mails usando inteligência artificial para os e-mails recebidos, permitindo à organização conscientizar sobre cibersegurança e lembrar os usuários de seguir a política. Os banners devem ser totalmente personalizáveis quanto à cor (para indicar gravidade) e ao texto, informando o destinatário sobre e-mails com conteúdo como:

16.40.1. Solicitação de pagamento via serviço de pagamento

16.40.2. E-mails com faturas / ordens de compra

16.40.3. E-mails com links para recursos restritos

16.40.4. Nome do remetente diferente do endereço

16.40.5. Domínio de resposta criado recentemente e diferente do domínio do remetente

16.40.6. Erro no SPF do remetente

16.40.7. Domínio do remetente criado recentemente

16.40.8. E-mails recebidos de remetentes externos

16.41. A solução deve permitir ao administrador realizar personalizações ou configurar exceções nas regras de segurança com base em pelo menos as seguintes opções:

16.41.1. Hosts

16.41.2. Endereços IP

16.41.3. Usuários

16.41.4. Domínios

16.41.5. Cabeçalhos / Headers

16.41.6. Assunto

16.41.7. Links

16.41.8. Anexos

16.42. O diagrama de fluxo de segurança do e-mail no painel principal deve mostrar quantos e-mails foram enviados pelo Microsoft para caixa de entrada, quarentena, lixo eletrônico e quantos foram detectados e colocados em quarentena pela solução de segurança oferecida.

16.43. A solução deve permitir aos administradores, a partir da mesma console de gestão de segurança de e-mail, visualizar e restaurar todos os e-mails em quarentena, seja colocados pelo Microsoft ou pela solução de segurança oferecida baseada em API – Possuir uma quarentena unificada.

16.44. A solução deve permitir aos administradores bloquear automaticamente URLs provenientes de fontes de indicadores de comprometimento (IOC).

16.45. Revisão de e-mails de phishing reportados pelo usuário

16.46. Os usuários podem ajudar a detectar ataques não identificados, permitindo que os administradores de segurança corrijam os ataques detectados e ajustem as políticas para evitar ataques semelhantes no futuro.

16.47. A solução deve ingerir automaticamente esses relatórios, alertar os administradores sobre eles e apresentar um painel dedicado que permita aos administradores investigar e tomar as medidas necessárias.

16.48. A solução deve poder se integrar com o complemento nativo Report Message para Microsoft 365, para marcar como phishing no Outlook. Quando um usuário clicar nessa opção.

16.49. Responder automaticamente e corrigir os relatórios dos usuários finais sobre e-mails de phishing. Para reduzir a carga de trabalho das equipes de SOC e Help Desk, isso deve ser significativamente simplificado.

16.50. Cada vez que um usuário envia um relatório de e-mail de phishing, a solução deve reavaliar o e-mail, utilizando reputação atualizada, motores de segurança atualizados e IA para adicionar indicadores adicionais.

16.51. O resultado será um veredicto reavaliado: limpo, phishing ou inconclusivo.

16.52. Para cada veredicto reavaliado, os administradores podem configurar um fluxo de trabalho (colocar o e-mail em quarentena ou mantê-lo na caixa de entrada), além de definir notificações personalizáveis tanto para administradores quanto para usuários finais.

16.53. A solução deve permitir que os administradores configurem um comentário automatizado para ser enviado aos usuários finais quando eles reportarem e-mails de treinamento de phishing.

16.54. A solução deve permitir que os administradores configurem um remetente personalizado para as notificações enviadas aos usuários finais sobre solicitações de restauração de quarentena aprovadas ou rejeitadas e os relatórios sobre e-mails de phishing.

16.55. A solução deve permitir que os administradores enviem notificações sobre os usuários que enviam solicitações de restauração para qualquer endereço de e-mail.

16.56. A solução deve permitir o envio de um relatório diário por e-mail aos usuários finais sobre e-mails em quarentena e lixo/spam nas últimas 24 horas.

16.57. A solução deve permitir que os administradores configurem a liberação automática de e-mails da quarentena do Microsoft se forem classificados como limpos pelo sistema de segurança, ou seja, falsos positivos nas detecções de phishing de alta confiança, evitando que os administradores dediquem muito tempo para liberar esses e-mails da quarentena.

16.58. Como última linha de defesa e camada de segurança, a solução deve poder ser configurada para liberar automaticamente os e-mails em quarentena pelo Microsoft como phishing de alta confiança se o sistema os classificar como limpos.

16.59. Os e-mails que Microsoft entregam erroneamente na pasta de lixo eletrônico podem ser redirecionados para a caixa de entrada do usuário.
A solução permite corrigir essas detecções de falsos positivos, para que as equipes de SOC não dediquem tempo ajudando os usuários finais a localizar seus e-mails legítimos perdidos.

16.60. Portal dedicado para gestão de e-mails em quarentena pelos usuários finais

As organizações precisam que seus usuários finais tenham acesso aos seus e-mails para manter o funcionamento do negócio. Em casos raros em que um e-mail é colocado em quarentena erroneamente pelo sistema de segurança ou pelo Microsoft e não é liberado automaticamente, é crucial que o usuário possa recuperá-lo rapidamente.

16.61. O portal de segurança de e-mails para usuários finais deve permitir que os usuários vejam todos os seus e-mails em quarentena, filtrem, pré-visualizem e restaurem ou enviem solicitações de restauração, tudo conforme as políticas organizacionais definidas.

16.62. Os usuários podem fazer login no portal de quarentena do usuário final via Microsoft, aplicando os mesmos controles de segurança, incluindo login único, através da conta corporativa do Microsoft.

16.63. A solução deve permitir que os usuários solicitem ao administrador a liberação dos e-mails em quarentena a partir desse relatório diário.

17. Requisitos de Interação e análise de ferramentas de IA Generativa:

17.1. A solução deverá prover arquitetura de monitoramento contínuo para aplicações de Inteligência Artificial Generativa, contemplando acessos web, aplicações e agentes, com aplicação de políticas de acesso, prevenção contra vazamento de dados (DLP) e controle de agentes em tempo real no ambiente corporativo.

17.2. A solução deve possuir arquitetura em nuvem com gerenciamento centralizado e gerenciamento por interface web.

17.3. A solução deve monitorar aplicações web, aplicações, desktop e ferramentas de desenvolvimento compatíveis.

17.4. A solução deve permitir descoberta automática de aplicações de IA utilizadas pelos usuários.

17.5. A solução deve identificar aplicações de inteligencia artificial generativa gerenciadas e não gerenciadas (Shadow AI).

17.6. A solução deve identificar utilização de aplicações de IA generativa não autorizadas.

17.7. A solução deverá classificar as interações com aplicações de Inteligência Artificial Generativa com base no risco da aplicação, no contexto de uso e na sensibilidade dos dados processados, identificando, no mínimo, níveis de risco baixo, médio, alto e crítico.

17.8. A solução deve permitir políticas distintas para aplicações, conteúdo e agentes de IA.

17.9. Suportar integração com provedores de identidade (IdP), com suporte mínimo para Microsoft ADFS, Microsoft Entra ID, Okta, servidores SAML genéricos, Google Workspace, radius.

17.10. A solução deve permitir criação de políticas de acesso baseadas por usuários e grupos, permitindo visibilidade sobre interação dos usuários com os aplicativos de IA generativa.

17.11. A solução deverá manter inventário atualizado das aplicações e agentes de Inteligência Artificial identificados no ambiente, permitindo visualizar sua utilização, responsáveis e classificação de risco.

17.12. A solução deverá identificar a utilização de agentes de Inteligência Artificial acessados por meio de credenciais não corporativas (Shadow AI), permitindo identificar usuários, aplicações, nível de risco e priorizar ações de governança e remediação.

17.13. A solução deverá apresentar visibilidade das integrações, dependências externas e capacidades operacionais dos agentes de Inteligência Artificial, permitindo identificar os sistemas acessados, os tipos de ações executadas e os riscos associados.

18. Add-in Oulook

18.1. A Ferramenta deve propiciar a opção de utilizar botões (Add-in) próprios no outlook dos usuários que será utilizado para:

18.2. Correção e alerta de envios de e-mails quando:

a) Dominio semelhante

b) Endereço do remetente incorreto

c) Contato externo

d) Dominio de remetente criado recentemente

e) Remetende se assemelha a alguém dentro da organização

f) Emails com faturas / POs

g) Emails parece ser de um serviço de assinatura eletrônica

h) Fautra de um novo fornecedor

i) Primeira vez do remetente

j) Nome de remetente com um diferente endereço

k) O remetente se assemelha ao contato

l) Requisição de pagamento via serviço de pagamento

m) Remetente falhou no SPF

n) Solicitação de atualização de detalhes de pagamento

o) Reportar Phishing possibilitando ao usuário verificar o veredito da IA diretamente no outlook, assim ajudando na conscientização e treinamento dos usuários em tempo real.

18.3. Portal de segurança da Check point, onde vai ser capaz de ter visibilidade inicial do portal unificado de quarentena, possibilitando ver:

a) Quantos emails ele possui em quarentena até 7 dias para trás

b) Requisições enviadas ao administrador para restaurações

c) Link integrado para visualizar via browser o Portal unificado completo

18.4. Prevenção de Malware em E-mail e Ferramentas de Colaboração e Armazenamento SaaS

18.5. Deve escanear malware por meio de análise estática.

18.6. A solução deve ter proteção antivírus/malware baseada em assinaturas.

18.7. A solução deve permitir que os administradores configurem a lista de bloqueio para qualquer tipo de arquivo marcado como malware e, para tipos de arquivos (PDF, EML, HTML), optar por bloquear esses arquivos dependendo se contêm links ou não.

18.8. A solução deve detectar arquivos protegidos por senha com pelo menos as seguintes extensões:

18.8.1. Documentos: Word, Excel, PowerPoint e PDF.

18.8.2. Arquivos: ZIP, 7Z, RAR, CAB, TAR, TAR.GZ, TGZ, GZ, BZ2, XZ, TXZ, TBZ2, TB2, TBZ, ISO, TAR.XZ, TAR.BZ2, CHM, IZH, RPM, WIM, ARJ, CPIO, CRAMFS, QCOW2, UDF, AR e IMG, ISO, AR.

18.9. Se um arquivo estiver protegido por senha, a solução deve tentar extrair a senha usando várias técnicas, como buscar a senha no corpo do e-mail. Se a senha for encontrada, deve

usá-la para descriptografar o arquivo e inspecioná-lo em busca de malware.

18.10. Se a senha não for encontrada, o administrador deve poder selecionar uma das seguintes ações:

18.10.1. Solicitar que o usuário final insira uma senha.

18.10.2. O usuário recebe o e-mail com um aviso.

18.10.3. Colocar em quarentena.

18.10.4. Identificar o e-mail como suspeito de malware.

18.11. A solução deve permitir que os administradores excluam remetentes externos do fluxo de trabalho padrão para lidar com e-mails com anexos protegidos por senha, evitando solicitações repetidas de senha para sistemas automatizados ou domínios confiáveis que enviam muitos anexos protegidos. As exclusões devem permitir que endereços de remetentes ou domínios específicos sejam excluídos do fluxo de trabalho, garantindo que seus e-mails continuem sendo inspecionados para malware. Se o sistema não conseguir ler as senhas, os anexos serão considerados permitidos (limpos).

18.12. Escaneia todos os arquivos trocados interna e externamente em busca de links maliciosos, códigos ou outros componentes de ataques avançados: Google Drive, ShareFile, OneDrive, SharePoint, Box, Dropbox — incluindo malware, ransomware e ataques laterais.

18.13. A solução deve escanear e analisar cada arquivo em busca de links maliciosos e depois bloqueá-los em todas as suas aplicações para compartilhamento de arquivos.

18.14. A solução deve detectar diretamente o comportamento malicioso e colocar os arquivos em quarentena antes que a ameaça se espalhe.

18.15. Oferece proteção contra links de phishing, código ou arquivos maliciosos e vazamento de dados em plataformas de chat corporativo.

18.16. A solução deve permitir aos administradores bloquear URLs exatas e domínios completos em mensagens do Teams e Slack.

18.17. Para aplicações como OneDrive e SharePoint, deve permitir por política dois tipos de ações de remediação: Quarentena e Vault Folder (Pasta Cofre).

18.18. Prevenção de Malware de Dia Zero (sandboxing) em E-mail e Ferramentas de

Colaboração e Armazenamento SaaS e Limpeza de Documentos

18.19. A solução deve incluir capacidades de “Sandboxing” resistentes à evasão para bloquear malware de dia zero, com análise dinâmica em um ambiente virtual isolado e escalável baseado na nuvem.

18.20. A solução deve incluir o uso da análise de sandboxing para revisar anexos e recursos web associados a hiperlinks incluídos nas mensagens. Deve também permitir visualizar um vídeo do resultado da emulação.

18.21. A análise de sandboxing deve obter um veredicto sobre um anexo ou recurso web associado a um hiperlink em no máximo 5 minutos.

18.22. A solução deve contar com uma página de bloqueio para impedir o acesso dos usuários a sites maliciosos associados aos hiperlinks contidos nos e-mails analisados.

18.23. A solução deve ser capaz de aplicar sandboxing a pelo menos os seguintes tipos de arquivos: EXE, DLL, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, SWF, JAVA (.jar, .js/.jse), VBS, scripts e arquivos PowerShell (.ps1).

18.24. A solução deve permitir que os administradores selecionem os sistemas operacionais que usarão o sandbox do Anti-Malware para emular arquivos. A emulação deve suportar Win7, Win8.1, Win10 e até Win11.

18.25. A solução deve suportar capacidades CDR (Content Disarm and Reconstruction), ou seja, limpar documentos ou imagens anexadas nos e-mails de conteúdo malicioso.

18.26. A solução CDR deve ser capaz de lidar com pelo menos os seguintes tipos de arquivos: PDF, FDF, XLSX, XLSB, XLSM, XLTX, XLTM, XLAM, XLSB, XLS, PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM, PPT, PPS, POT, PPA, DOCX, DOCM, DOTX, DOTM, DOC, DOT.

18.27. A solução deve emular arquivos atrás de links de download direto antes de entregá-los aos usuários finais, aplicando proteção contra arquivos desconhecidos ocultos atrás de links.

18.28. Além disso, deve prevenir ataques nos quais o arquivo atrás do link é alterado após o envio do e-mail, aplicando proteção de reescrita do link e inspeção quando os usuários clicam nos links reescritos. Se for detectado que o arquivo é malicioso, o acesso ao arquivo deve ser bloqueado.

18.29. A solução deve fazer sanitização de arquivos limpando e entregando o arquivo sem

nenhum executável ou macro para o usuário em OneDrive e SharePoint.

18.30. O relatório de Sandboxing deve apresentar as técnicas detectadas na ameaça de acordo com a matriz MITRE ATT&CK.

18.31. Todos os arquivos escritos no sistema de arquivos serão monitorados e analisados estaticamente. Se forem considerados potencialmente maliciosos, os arquivos serão emulados mediante um ambiente de testes e colocados em quarentena se forem considerados maliciosos.

18.32. A solução mostrará capturas de tela de emulação de arquivos maliciosos e vídeos no ambiente Sandbox.

18.33. A solução deve incluir um relatório com o resultado da emulação que inclua: componentes do ataque, vídeo da emulação, atividades suspeitas, quadro de análise forense.

18.34. Anomalias de Usuários e Detecção de Contas Comprometidas

18.35. A solução deve evitar ataques avançados de apropriação de contas, aumentando os processos de autenticação, evitando que usuários não autorizados e dispositivos comprometidos acessem seu e-mail na nuvem ou aplicativos SaaS.

18.36. A solução deve contar com um motor que analise o comportamento utilizando um algoritmo de aprendizado automático, criando um perfil baseado em eventos históricos que incluem localizações e horários de login, comportamento de transferência de dados e padrões de mensagens de e-mail.

18.37. A solução deve detectar comportamentos e ações que pareçam anormais quando observados no contexto da organização e da atividade histórica do usuário.

18.38. Para identificar contas potencialmente comprometidas, deve incluir um motor de inteligência artificial para inspecionar todos os parâmetros dos eventos de login e identificar ações realizadas por atores mal-intencionados, como:

18.38.1. Exclusão de todos os e-mails da caixa de entrada

18.38.2. Usuários que enviam e-mails maliciosos

18.38.3. Mover todos os e-mails para uma subpasta

18.38.4. Detecção baseada em IA de logins anômalos

18.38.5. Login a partir de um endereço IP malicioso

18.38.6. Primeira vez em um novo país

18.38.7. Encaminhamento automático para um endereço de e-mail externo

18.38.8. Acesso incomum a partir de um país

18.38.9. Acesso a partir de uma localização suspeita (viagem impossível)

18.38.10. Erro de login suspeito em MFA

18.38.11. Cliente usando navegador vulnerável

18.39. A solução deve gerar um evento de segurança que forneça contexto e informações necessárias para investigação, classificando-o como crítico ou suspeito.

18.40. A solução deve ter capacidade de executar as seguintes ações de resposta quando detectar contas potencialmente comprometidas ou sequestradas:

18.40.1. Bloquear a conta

18.40.2. Redefinir a senha

18.41. As anomalias críticas e logins identificados de usuários comprometidos devem ser bloqueados automaticamente.

18.42. A solução deve permitir que os administradores configurem uma caixa dedicada para enviar alertas sobre contas comprometidas.

18.43. Bloqueio de contas que iniciem sessão a partir de IPs conhecidos como maliciosos, com base em inteligência do fabricante (TIP).

18.44. Entre os eventos que a solução deve analisar para identificar contas sequestradas (“account takeover”) devem incluir:

18.44.1. O início de sessão

18.44.2. A localização de onde ocorreu o início de sessão

18.44.3. Anomalias recentes

18.44.4. E-mails recentes

18.44.5. Ações recentes do usuário

18.45. Os administradores podem configurar para adicionar automaticamente uma lista

de bloqueio para todo o tráfego de saída das contas detectadas como comprometidas ou suspeitas de estarem comprometidas, como uma camada adicional de segurança em cenários como:

18.46. Mensagens maliciosas programadas: o atacante pode programar o envio de e-mails em uma etapa posterior que se adapte ao seu ataque, sabendo que o usuário comprometido pode ser bloqueado a qualquer momento.

18.47. Ambientes híbridos: nos casos em que o Active Directory local invalida o Azure Active Directory, é possível que os usuários bloqueados sejam desbloqueados. Nesse caso, todos os e-mails enviados pelo usuário comprometido continuarão bloqueados.

18.48. Shadow IT & Controle de Aplicações

18.49. A solução, baseada na análise de e-mails (Office 365 e/ou Gmail), deve identificar os e-mails das aplicações na nuvem que os usuários sugerem estar utilizando, para oferecer visibilidade das aplicações em nuvem usadas na empresa.

18.50. A solução deve detectar e fornecer relatórios sobre aplicações de Shadow IT e os principais usuários.

18.51. A solução deve fornecer um relatório de avaliação de riscos da aplicação.

18.52. A solução deve indicar o uso das aplicações ao longo do tempo.

18.53. A solução deve apresentar as aplicações utilizadas conforme sua categoria.

18.54. A solução deve permitir testar uma aplicação ou criar uma lista branca para a aplicação.

18.55. Prevenção contra Perda de Dados (DLP) para e-mail e ferramentas de colaboração e armazenamento SaaS

18.56. A solução deve contar com um motor de prevenção contra perda de dados (DLP) para proteger os dados da organização contra possíveis violações ou transmissões de dados sensíveis.

18.57. O motor DLP deve analisar e-mails, arquivos anexos, arquivos compartilhados e mensagens de texto publicadas em plataformas de colaboração, detectando padrões de dados que não devem ser compartilhados com pessoas ou destinos não autorizados.

18.58. O motor DLP deve permitir criar políticas para controlar como os arquivos são

compartilhados entre usuários internos e externos. Deve identificar e marcar arquivos que contenham informações confidenciais, financeiras ou de identificação pessoal, como números de cartão de crédito, números de seguro social, números de contas bancárias ou dados protegidos por HIPAA.

18.59. A solução DLP deve suportar expressões regulares, dicionários e termos personalizados definidos pelo cliente.

18.60. Políticas DLP devem permitir:

18.60.1. Filtrar e-mails enviados para garantir que dados confidenciais não cheguem a destinatários não autorizados.

18.60.2. Filtrar e-mails recebidos para garantir que dados confidenciais não sejam armazenados nas caixas de correio da organização ou compartilhados por métodos não autorizados.

18.61. Para e-mails enviados, a solução DLP deve permitir pelo menos as seguintes ações:

18.61.1. Bloquear o e-mail e alertar o usuário.

18.61.2. Bloquear o e-mail e solicitar reenvio criptografado.

18.61.3. Adicionar cabeçalho ao e-mail.

18.61.4. Enviar criptografado

18.62. Para os e-mails recebidos, a solução DLP deve permitir pelo menos as seguintes ações:

18.62.1. Bloquear o e-mail e alertar o usuário.

18.62.2. Bloquear o e-mail e solicitar que seja reenviado criptografado.

18.62.3. Permitir o e-mail adicionando um cabeçalho.

18.63. A solução deve permitir que os administradores coloquem em quarentena e-mails recebidos que violem a política de Prevenção de Perda de Dados (DLP) sem notificar os usuários finais.

18.64. A solução deve permitir configurar alertas por e-mail para administradores e usuários sobre e-mails recebidos ou enviados que contenham uma infração de DLP.

18.65. A solução deve permitir que os administradores configurem sua diretiva DLP para que os e-mails sejam enviados criptografados pelo Microsoft 365.

18.66. O sistema deve permitir que os administradores definam políticas DLP não apenas baseadas em tipos de dados predefinidos ou personalizados, mas também nas Etiquetas de Sensibilidade do Microsoft Purview associadas a e-mails, anexos, arquivos compartilhados ou mensagens.

18.67. A seção de critérios DLP deve permitir escolher as etiquetas de sensibilidade do Microsoft, com opções para selecionar qualquer etiqueta, etiquetas específicas, toda exceto algumas ou nenhuma etiqueta.

18.68. A solução deve permitir correspondência segura por e-mail com parceiros e clientes, onde partes externas visualizam e-mails confidenciais por meio de um portal autenticado, e a organização controla a disponibilidade da mensagem para a parte externa.

18.69. A solução deve permitir que os administradores personalizem o portal de correspondência segura adicionando imagens ou logotipos.

18.70. A solução deve ter capacidade de integração com criptografia do Microsoft 365, garantindo que qualquer e-mail detectado não seja entregue ao destinatário até que seja seguro, e permitindo que o usuário reenvie o e-mail como criptografado pelo Microsoft.

18.71. A solução deve permitir lista de remetentes/destinatários individuais ou domínios completos para granularidade na inspeção DLP.

18.72. Para aplicativos como OneDrive e SharePoint, deve permitir por política dois tipos de ações de remediação: Quarentena e Vault Folder (Pasta Cofre).

18.73. A solução deve definir sensibilidades personalizadas para as regras DLP, de modo que seja ativado um fluxo de trabalho diferente dependendo da quantidade de dados confidenciais filtrados.

18.74. A solução deve permitir que os administradores configurem alertas por e-mail para que gerentes recebam notificações em tempo real quando seus funcionários enviarem ou tentarem enviar dados classificados que coincidam com as regras da política DLP do Microsoft 365.

18.75. Essas notificações devem poder ser configuradas para qualquer regra de política DLP, seja o e-mail bloqueado ou não, inclusive para regras que apenas monitoram.

19. Gestão de Eventos, Painéis, Relatórios e Auditoria

19.1. A solução deve permitir gerenciar os eventos de segurança, sejam detectados/prevenidos automaticamente ou identificados posteriormente por administradores/usuários finais, abrangendo diversas ameaças, desde e-mails maliciosos e spam até contas comprometidas e parceiros arriscados.

19.2. A solução deve contar com uma visão detalhada de todos os eventos de segurança em tempo real. Por meio de busca e filtros, deve ser possível visualizar eventos relacionados a qualquer período, estado, nível de gravidade e SaaS.

19.3. A solução deve oferecer uma visão centrada nas ameaças de e-mail com informações como:

19.3.1. Categorias de phishing detectadas

19.3.2. Ação sobre o e-mail malicioso (se está em quarentena, na caixa de entrada ou na pasta de lixo eletrônico)

19.3.3. Usuários envolvidos no evento (destinatários, remetentes, proprietários de arquivos compartilhados)

19.3.4. Informação sobre quem realizou a remediação (administrador, ferramenta de segurança ou provedor de e-mail em nuvem)

19.3.5. A solução deve fornecer painéis com análises detalhadas de eventos maliciosos para cada aplicação SaaS.

19.3.6. Os painéis (dashboards) devem detalhar eventos de segurança por cada aplicação SaaS de armazenamento e/ou colaboração, registrando:

19.3.7. Quantidade de usuários, arquivos, recursos compartilhados, links, logins e detecções de ameaças.

19.3.8. A solução deve fornecer relatórios executivos de eventos de segurança da última semana, últimas duas semanas e últimos 30 dias.

19.3.9. Deve permitir que os administradores programem relatórios de segurança para envio em diferentes fusos horários e para diferentes destinatários.

19.3.10. A solução deve fornecer capacidades de investigação que apoiem os

processos de caça a ameaças da organização, permitindo realizar consultas a toda a metadata (e-mails, arquivos, logins de usuários etc.) capturada e armazenada no tenant.

19.3.11. As capacidades de investigação devem permitir os seguintes tipos de filtros:

19.3.12. Múltiplos valores em uma consulta: listas extensas de até 200 valores em um único campo de busca que aceita texto livre, com condições disponíveis (Contém Qualquer, Coincide com Qualquer, Excluir Contém, Excluir Coincide).

19.3.13. Múltiplas condições para o mesmo campo: aplicar filtros a um campo, definir múltiplas condições para ajustar a busca de forma mais precisa, gerenciar o operador (E/OU) entre cada condição.

19.3.14. A solução deve fornecer uma quarentena unificada com a Microsoft 365, assim gerenciando as duas quarentenas no mesmo portal

19.3.15. A solução deve fornecer um painel de resumo que proporcione aos administradores visibilidade instantânea de todas as tarefas pendentes de revisão, incluindo:

19.3.15.1. Usuários comprometidos

19.3.15.2. Parceiros arriscados

19.3.15.3. Solicitações abertas de restauração de quarentena por usuários finais

19.3.15.4. Relatórios abertos de phishing por usuários finais

19.3.15.5. Ataques BEC, incluindo um indicador que mostra se as contas comprometidas foram bloqueadas automaticamente ou não

19.3.16. A solução deve ter a possibilidade de exportar eventos para arquivos CSV, JSON, XLSX.

19.3.17. A solução deve fornecer relatórios de eventos por até 180 dias, em formato CSV ou XLSX.

19.3.18. A solução deve permitir filtrar e-mails com base na sua direção: entrada, saída e interno.

19.3.19. A solução deve permitir que os administradores filtrem e-mails pelo campo Message ID.

19.3.20. Os administradores devem poder filtrar e-mails usando instruções no idioma nativo, com suporte à IA generativa e ao Assistente de IA.

19.3.21. Com o Assistente de IA, deve ser possível buscar e-mails usando instruções no idioma nativo e obter resultados instantâneos, permitindo buscas baseadas em múltiplos campos.

19.3.22. A solução deve contar com um painel que mostre:

19.3.22.1. Número de relatórios de phishing dos usuários

19.3.22.2. Solicitações de restauração

19.3.22.3. Parceiros de risco

19.3.22.4. Indicação se contas comprometidas foram bloqueadas automaticamente ou não.

19.3.23. A solução deve permitir que os administradores tenham visibilidade do risco dos parceiros com quem se comunicam, usando um motor de IA, e recebam alertas sobre parceiros potencialmente comprometidos.

19.3.24. A solução deve permitir que os administradores desencadeiem uma ação específica quando o domínio do remetente for muito semelhante ao domínio de um parceiro, para evitar ataques de parceiros comprometidos.

19.3.25. A solução deve permitir que os administradores possam ver a justificativa dos usuários finais antes de aprovar/rejeitar as solicitações antes de liberar um e-mail da quarentena.

19.3.26. Os administradores da solução devem ter visibilidade em tempo real de como o Microsoft 365 classificou cada e-mail e qual ação foi tomada pelas soluções EOP ou Defender, ou seja, a solução deve trabalhar com segurança em profundidade e em camadas.

19.3.27. Os eventos e cada e-mail devem ter a classificação (SCL, BCL) e a ação de conformidade (quarentena, mover para pasta de lixo eletrônico) tomada sobre o e-mail de acordo com a classificação.

19.3.28. A solução deve permitir filtrar e-mails com base nas ações tomadas pelas ferramentas ou pelas decisões de conformidade do Microsoft.

19.3.29. A solução deve fornecer detalhes da análise de um arquivo identificado como malicioso, incluindo os comportamentos de risco que foram detectados e as técnicas identificadas. O resultado da emulação de um arquivo malicioso deve incluir um vídeo indicando o resultado da emulação.

19.3.30. O painel principal deve fornecer uma visão geral de como a solução classificou os e-mails que o Microsoft decidiu deixar passar para os usuários finais.

19.3.31. A solução deve permitir filtrar e-mails por esta e pelas decisões de conformidade do Microsoft.

19.3.32. A solução deve incluir um relatório diário de quarentena (Resumo), permitindo enviar um relatório por e-mail diariamente aos usuários finais sobre os e-mails em quarentena e lixo/spam.
Os usuários finais recebem um relatório detalhado contendo informações sobre os e-mails enviados e colocados em quarentena nas últimas 24 horas.

19.3.33. Os usuários finais podem gerar um novo relatório de quarentena (Resumo) para as últimas 24 horas a qualquer momento.

19.3.34. A solução deve permitir que os administradores possam personalizar:

19.3.35. Quando e quantas vezes por dia os usuários finais recebem o relatório de quarentena (Resumo).

19.3.36. O endereço de resposta do relatório diário de quarentena enviado aos usuários finais.

19.3.37. Os textos no corpo e no assunto do relatório diário de quarentena do usuário final (Resumo).

19.3.38. O texto do link no qual os usuários clicam para gerar um relatório.

19.3.39. A solução deve permitir que os administradores possam configurar, para cada detecção do Microsoft 365, se os usuários finais podem solicitar uma restauração, restaurar por conta própria ou não restaurar os e-mails.

19.3.40. Todas as solicitações de restauração enviadas pelos usuários finais estarão disponíveis para os administradores no painel Solicitações de Restauração.

19.3.41. A solução deve permitir que os administradores possam carregar um logotipo personalizado para adicionar às notificações por e-mail, páginas do navegador e relatórios.

19.3.42. A solução deve permitir que os administradores possam buscar na console de segurança de e-mail os e-mails detectados devido a uma regra de transporte do Microsoft, seja que tenham sido entregues ao usuário final, movidos para a pasta de lixo eletrônico ou colocados em quarentena pela solução de segurança ou pelo Microsoft.

19.3.43. A solução deve permitir que, a partir do portal de gestão, os administradores se mantenham atualizados sobre as atividades de manutenção e o status do serviço.

19.3.44. A solução deve permitir que os administradores possam definir caixas de correio dedicadas para receber alertas sobre o status do serviço.

20. Portal de Gestão

20.1. Controle de acesso granular baseado em funções no portal web de gestão, pelo menos para: Administrador, Somente Leitura, Help Desk.

20.2. Usuários do Help Desk e usuários com acesso somente leitura podem receber permissões de visualização apenas para a seção de Políticas.

20.3. Usuários do Help Desk e usuários com acesso somente leitura podem receber permissões para visualizar e editar a seção de Políticas.

20.4. Por padrão, os usuários do Help Desk e de somente leitura não têm permissão para visualizar ou editar as regras de políticas.

20.5. A solução deve permitir que os administradores restrinjam o acesso ao portal da organização a um endereço IP ou CIDR específico.

20.6. Integrações com SIEMs e API

20.7. A solução oferecida deve permitir integração com soluções SIEM via syslog (TCP) ou JSON via HTTP.

20.8. A solução deve suportar API REST para administrar e atuar sobre os eventos de segurança detectados.

21. Gestão de DMARC

21.1. Deve permitir centralizar os logs de DNS no mesmo Portal

21.2. Possibilitar uma melhor visibilidade dos reportes resumidos por IA com as seguintes informações:

21.2.1. Resumo

21.2.2. Sugestão

21.2.3. Informação do domínio

21.2.4. Reportante

21.2.5. Informação do Source

21.2.6. Cabeçalhos

21.2.7. Resultado da autenticação SPF

21.2.8. Resultado da autenticação DKIM

21.2.9. Ação da política

21.3. Deve ter a possibilidade de exportar as informações em formato CSV

21.4. Permitir configurar o DKIM e SPF diretamente do Portal da ferramenta

21.5. Criar e customizar alertas e eventos para a funcionalidade DMARC como:

21.5.1. Erro no SPF

21.5.2. Erro no DMARC

21.5.3. Queda da porcentagem de aceitação do DMARC

21.5.4. Parada de recebimento dos reportes de DMARC

21.5.5. Novo source falhando

21.6. A gestão de DMARC ajuda as organizações a garantir que todos os remetentes legítimos estão autorizados, permitindo aplicar com confiança uma política restritiva no registro DNS de DMARC da organização. Inclui:

21.6.1. Visibilidade de todos os serviços que enviam e-mails em nome dos seus domínios e subdomínios.

21.6.2. Busca de todos os e-mails que falharam na autenticação DMARC enviados em nome da organização.

21.6.3. Recomendações acionáveis para alteração do registro DMARC.

21.6.4. Vazamento de credenciais

21.6.5. Deve permitir visualizar as credencias que estão sendo vazadas em Deep, Dark web, forúns e malware database até 6 meses para trás em mesmo portal da proteção de e-mail.

21.6.6. Possibilitar uma melhor visibilidade das credenciais:

21.6.6.1. Email cooporativo

21.6.6.2. Aplicação que usuário perdeu sua credencial

21.6.6.3. Senha

21.6.6.4. Confiança da informação

21.6.6.5. Data de Observação

21.6.6.6. Deve ter a possibilidade de exportar as informações em formato CSV

21.6.6.7. Deve ser capaz de trocar a senha ou bloquear o usuário no Workspace.

22. Treinamento sobre Phishing baseado em GenAI

22.1. Personaliza os ataques simulados para cada usuário com base em seu departamento, cargo e setor.

22.2. As campanhas de treinamento são criadas automaticamente pelo GenAI, com os devidos permissos para que não sejam bloqueadas pela ferramenta HEC, reduzindo o tempo e os recursos necessários para criar as campanhas e garantir que os e-mails cheguem aos usuários.

22.3. Criação de regras com base em usuário, grupos ou departamentos

22.4. Possibilita utilizar GenAI para simular impersonificação de identidade internamente

22.5. A solução deve fornecer a opção de customizar templates para simulação de phishing

22.6. Deve ter a possibilidade de inscrever o usuário que caiu o no phishing diretamente para um treinamento

22.7. Deve ser possível colocar smartbanners nas simulações de phishing

22.8. Deve ser gerado automaticamente em Portugues (Brazil) para simulações e possibiliar fazer campanhas também em português.

22.9. Deve ser possível customizar e criar campanhas customizadas para os usuarios

22.10. Deve ser possível customizar a % de acerto que vai ser exigido para o usuário.

22.11. Possuir mais de 20 campanhas de treinamento já criadas no portal

22.12. Visualizar dashboard por Política ou departamentos

22.13. Visibilidade granular de cada ação tomada nas simulações de phishing como:

22.13.1. Lida

22.13.2. Clicou no phishing

22.13.3. Não leu

22.13.4. Deletou

22.13.5. Reportou como phishing

22.13.6. Visibilidade granular nas ações das campanhas

22.13.7. Invitado

22.13.8. Começou

22.13.9. Passou

22.13.10. Falhou

22.13.11. Não começou

22.13.12. Em progresso

23. Grupo I Item 6 do Edital – Solução de Acesso Remoto Seguro Harmony Sase Internet Access por 12 Meses.

23.1. Características Gerais

23.1.1. A solução deve permitir que os usuários se conectem à Internet de forma segura através de instalação de agente;

23.1.2. Durante a instalação, deve permitir indicar qual o usuário, a fim de aplicar a

segurança da Internet imediatamente após a instalação do agente, sem exigir nenhuma interação do usuário final;

23.1.3. Apenas o tráfego de interesse da máquina do usuário deve ser desviado para o serviço de firewall em nuvem do fabricante;

23.1.4. Deve permitir o desvio do tráfego para a nuvem de forma inteligente, possibilitando selecionar objetos pré-configurados como: “Office 365 Services”. Permitindo assim que todo o tráfego do Office passe pela nuvem do fornecedor e todo o restante do tráfego saia localmente;

23.1.5. Mesmo sem direcionar todo o tráfego para a nuvem, a solução deve ser capaz de aplicar alguns controles de segurança, como:

23.1.6. Impedir com que o usuário acesse sites proibidos pela organização (Web Filter);

23.1.7. Bloquear a tentativa de download de conteúdo malicioso conhecido através de assinaturas (Anti-malware) ou desconhecidos através de Sandbox (Threat Emulation);

23.1.8. Bloquear comunicação de máquina infectada com uma C&C (Anti-bot);

23.1.9. Controlar de maneira granular o acesso às aplicações (App Control);

23.1.10. Impedir o acesso não autorizado a contas pessoais ou contas corporativas não aprovadas (Tenant Restrictions), ao menos nas seguintes aplicações: Microsoft Office 365, Google Workspace, Dropbox, ChatGPT, Claude, GitHub e Slack;

23.1.11. Os acessos não autorizados devem ser registrados, permitindo habilitar ou não o log através da política;

23.1.12. O serviço de firewall em nuvem deve possuir PoP (Point of Presence) no Brasil a fim de garantir uma baixa latência e uma melhor experiência na navegação do usuário;

23.1.13. Se o usuário estiver em outro país, a solução deve ser capaz de selecionar o PoP mais próximo através de uma lista de locais previamente aprovados para conexão pelo administrador;

23.1.14. A solução deve permitir que os administradores criem políticas de segurança de forma unificada para ser aplicada para diferentes usuários remotos;

23.1.15. A solução deve gerenciar todos os acessos de forma centralizada, permitindo maior visibilidade nas conexões e controle de acesso à internet e no combate de

prevenção de ameaças;

23.1.16. Deve ser possível criar e administrar as políticas de acesso a internet da solução através da Gerência dos Firewalls, garantindo maior consistência, visibilidade e eficiência operacional;

23.1.17. A solução deve permitir a instalação de agentes nos computadores remotos, permitindo uma conexão segura através de engines de prevenção de ameaças e controle de navegação WEB;

23.1.18. O agente instalado deve ser capaz de identificar quando estiver conectado à internet de maneira remota, ou por dentro da infraestrutura do escritório remoto. Para com isso ser ativado/desativado de acordo com a política.

23.2. Funcionalidade de Segurança

23.2.1. A solução deve ter gerência baseada em nuvem e permitir que os administradores gerenciem os usuários através de agentes permitindo fazer toda inspeção de navegação Web;

23.2.2. A solução deve permitir que os administradores criem políticas granulares para usuários para liberar ou bloquear a navegação para URL's e Aplicações;

23.2.3. Controle de políticas por URL, grupos de URLs e categorias de URLs;

23.2.4. Controle de políticas por Aplicações, permitindo configurações granulares como: Permitir o uso do Google Drive, mas restringir o Upload dentro da aplicação;

23.2.5. Controle de políticas através de geolocalização, bloqueando tráfego com destino a países que não tem relação direta com o negócio;

23.2.6. Controle de políticas por usuários e grupos de usuários;

23.2.7. Controle de políticas por tempo, permitindo ou negando acesso a uma URL em um determinado dia e horário;

23.2.8. A solução deve possuir funcionalidade de inspeção do tráfego SSL;

23.2.9. A inspeção do tráfego SSL deve ser feita no dispositivo sem a obrigatoriedade de instalar um certificado na máquina;

23.2.10. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 80 categorias de aplicações WEB pré-definidas pelo fabricante;

23.2.11. Possuir mecanismo de controle de URL que permite o bloqueio apenas de uma URL específica, por exemplo o facebook.com, ou seja, não deve ser bloqueado toda a categoria como "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc.

23.2.12. Suportar a criação de categorias de URLs customizadas;

23.2.13. No caso de bloqueio de acesso, o usuário deve receber um retorno informando que o acesso foi bloqueado;

23.2.14. A solução deve apresentar em tempo real a quantidade de alterações que estão sendo realizadas pela sessão do administrador;

23.2.15. A solução deve possuir recurso de descartar as configurações realizadas pelo administrador antes de ser aplicado nos GW's de segurança;

23.2.16. A solução deve permitir que o administrador consiga ter visibilidade em tempo real de todas as alterações que estão sendo realizadas na ferramenta antes de ser aplicadas. Assim, ele terá controle e permissão para desfazer qualquer configuração durante o período de criação/alteração;

23.2.17. A solução deve possuir painel de auditoria para ser analisado todas as alterações realizadas pelos administradores, contendo no mínimo campos como:

23.2.18. Usuários administrador;

23.2.19. Dia e horário da mudança;

23.2.20. Descrição das mudanças de forma individual.

23.2.21. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulos de proteção contra malwares e reputação de URL;

23.2.22. A solução deve sincronizar todas as assinaturas de prevenção de ameaças de forma automatizada, sem a necessidade da intervenção do administrador;

23.2.23. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS;

23.2.24. Suportar a criação de regras de exceção para as funcionalidades de

Prevenção de Ameaças;

23.2.25. As regras de exceção devem ser baseadas em URLs ou Hash de arquivos;

23.2.26. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

23.2.27. O nome da assinatura, origem (usuário e dispositivo) e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

23.2.28. Proteção contra vazamento de dados

23.2.29. A solução deve possuir recursos de prevenção contra vazamento de dados (DLP) para o tráfego web, baseado no navegador;

23.2.30. O recurso de DLP deve detectar e impedir a transmissão não autorizada de informações confidenciais, como números de CPF, números de cartão de crédito, números de contas bancárias, dentre outros.

23.2.31. A solução deve fornecer Data Types predefinidos, a fim de prover uma configuração inicial sem a necessidade de customização;

23.2.32. Deve possuir ao menos 700 Data Types predefinidos, disponíveis para uso na regra;

23.2.33. Deve permitir a criação de Data Types customizados utilizando ao menos: Dicionário de palavras, palavras-chaves, expressões regulares e atributo do arquivo (nome, tamanho e tipo);

23.2.34. Deve ser capaz de analisar e criar regras baseadas nos eventos de “outbound” (Upload de arquivos) e “inbound” (Download de arquivos);

23.2.35. Possibilitar a criação de regras de DLP por usuário ou grupo de usuários;

23.2.36. Deve permitir ao menos configurar as seguintes ações nas regras do DLP:

23.2.37. Detectar: Executa a varredura de dados sensíveis, mas não bloqueia a ação.

23.2.38. Prevenir: Executa a varredura DLP e impede a transferência de dados se encontrar um dado sensível.

23.2.39. Os logs devem ser registrados no portal administrativo para ações de

prevenção, detecção e notificação.

23.2.40. controle de acesso ao ambiente corporativo para usuários remotos

23.3. Características Gerais

23.3.1. A solução deve permitir que os usuários se conectem facilmente por meio de um portal unificado a uma ampla gama de aplicativos sem cliente e através de instalação de software (client).

23.3.2. A solução deve permitir que os administradores de segurança implantem facilmente a solução através de datacenter em ambientes físicos e nuvem publica.

23.3.3. A comunicação entre DC, nuvem pública, ambientes corporativos e usuários devem implementar uma arquitetura full-mesh.

23.3.4. Para que o usuário remoto consiga se comunicar de forma segura com os ambientes corporativos internos é necessário a instalação de um conector dentro do ambiente corporativo.

23.3.5. Deve permitir alta disponibilidade (HA) para os Conectores;

23.3.6. Além dos conectores, também deve possibilitar, estabelecer um túnel IPsec usando um gateway local existente e o gateway do SASE;

23.3.7. O gateway SASE deve possuir IP público dedicado, não deve compartilhar IPs entre clientes do fabricante.

23.3.8. A solução deve habilitar a Zero Trust Architecture definindo uma política de acesso granular para fornecer às pessoas certas no contexto certo, o acesso menos privilegiado aos aplicativos e reduzir a superfície de ataque.

23.3.9. A solução deve autenticar primeiro e se conectar depois - cada dispositivo e usuário que tenta acessar um aplicativo deve primeiro ser autenticado e autorizado pelos provedores de identidade em nuvem.

23.3.10. A autenticação deve ser baseada em atributos contextuais do usuário, como credenciais (usuário, senha e duplo fator de autenticação).

23.3.11. Com o client instalado na máquina, a solução deve possuir validação de postura periódica e granular, de forma que o administrador consiga criar regras de postura por

tipo de sistema operacional.

23.3.12. A validação de postura para máquinas Windows deve comtemplar pelo menos a validação de:

23.3.12.1. Anti-virus instalado;

23.3.12.2. Certificados;

23.3.12.3. Criptografia de disco;

23.3.12.4. Arquivos existentes;

23.3.12.5. Processos em execução;

23.3.12.6. Chaves de registro;

23.3.12.7. Domínio;

23.3.12.8. Versão de SO;

23.3.13. A validação de postura também deverá se aplicar ao acesso agentless (sem agentes), não apenas ao acesso com cliente instalado no dispositivo do usuário.

23.3.14. A validação de postura para o acesso agentless deve comtemplar no mínimo as seguintes validações:

23.3.14.1. Grupo;

23.3.14.2. Data e hora de acesso;

23.3.14.3. IP;

23.3.14.4. Localização (País de acesso);

23.3.14.5. Navegador;

23.3.14.6. Sistema Operacional;

23.3.15. O acesso aos aplicativos não deve exigir o acesso a toda a rede. Os usuários devem ter conectividade granular para aplicativos apenas com base na necessidade da empresa.

23.3.16. Usuários externos, bem como usuários internos, não devem estar cientes de aplicativos não autorizados. Os recursos não autorizados não devem apenas ser inacessíveis, mas também completamente invisíveis.

23.3.17. A solução deve trazer o monitoramento da atividade da rede, dando às equipes de TI uma maneira de monitorar e gerenciar facilmente todas as atividades da rede.

23.3.18. O client deve estar disponível para o seguintes Sistemas Operacionais:

23.3.18.1. Windows (exe e msi), Windows on ARM (ARM64);

23.3.18.2. Mac;

23.3.18.3. Linux (Ubuntu, Red Hat e Fedora);

23.3.18.4. Android / Chromebook;

23.3.18.5. iOS;

23.3.18.6. Detalhes da Solução:

23.3.19. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

23.3.20. Deve ser licenciada pelo número de usuários que utilizarão a plataforma de acesso remoto seguro;

23.3.21. Deve prover acesso a recursos internos (on-premise) ou em múltiplas nuvens de forma segura;

23.3.22. Deve permitir acesso com permissões granulares para cada recurso corporativo baseado em permissões dinâmicas e contextuais;

23.3.23. Para o acesso agentless, deve suportar no mínimo, os seguintes tipos de aplicações:

23.3.23.1. Web;

23.3.23.2. SSH;

23.3.23.3. RDP;

23.3.23.4. VNC;

23.3.24. O acesso RDP deve permitir a conexão através do navegador e usando o Remote Desktop nativo;

23.3.25. Cada usuário poderá ver, em seu portal, somente as aplicações para as quais possui acesso;

23.3.26. Caso o usuário possua endereço de acesso para uma aplicação para o qual não tem permissão, o acesso deve ser bloqueado pela solução;

23.3.27. A solução não deve depender de cliente instalado na máquina do usuário;

23.3.28. A solução deve permitir a criação de usuários em base de usuários interna;

23.3.29. A gestão interna de usuários deve permitir a criação de usuários e grupos e a configuração de políticas.

23.3.30. A autenticação do usuário da base interna de usuários deve ser feita, no mínimo, por usuário e senha;

23.3.31. A solução deve se integrar com bases de identificação externas;

23.3.32. Deve ser possível utilizar usuários da base interna e usuários de um provedor de identidades externo na mesma tenant;

23.3.33. Deve ser possível personalizar a aplicação adicionada permitindo o envio de logo da mesma;

23.3.34. Ao adicionar uma aplicação SSH, deve ser possível escolher entre, pelo menos, os seguintes métodos de autenticação:

23.3.34.1. Usuário e senha;

23.3.34.2. Chave privada: o usuário deverá baixar a chave para ter acesso ao recurso;

23.3.35. Deve ser possível configurar a forma como a solução se conectará ao servidor SSH, de, pelo menos, as seguintes formas:

23.3.35.1. Direta: permitir que usuários conectem ao servidor diretamente através da seleção de sua conta e senha;

23.3.35.2. Conta específica: adicionar o servidor com uma conta específica em que todos os usuários serão logados automaticamente;

23.3.35.3. A solução deve manter logs de atividade de uso das aplicações;

23.3.35.4. Os dados de logs devem ser armazenados em ambiente criptografado e sem exposição para a internet;

23.3.36. Os logs de atividade devem cobrir, pelo menos, as seguintes atividades:

23.3.36.1. Logins efetuados com sucesso;

23.3.36.2. Logout efetuados com sucesso;

23.3.36.3. Conexão com sucesso às aplicações;

23.3.36.4. Falha em conexão às aplicações;

23.3.36.5. Os logs devem gravar data e hora de cada ocorrência;

23.3.36.6. Toda a comunicação entre o usuário e a plataforma deve ser realizada através de conexões TLS;

23.4. Módulo de Gerência

23.4.1. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

23.4.2. A solução de gerência deverá ser separada dos gateways de segurança;

23.4.3. A solução de gerência irá gerenciar as políticas de segurança de todos Gateways e funcionalidades solicitadas neste documento;

23.4.4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

23.4.5. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

23.4.6. Deve possuir a capacidade de proteção contra sign out do usuário autenticado e desinstalação do agente instalado por meio de código.

23.4.7. O gerenciamento da solução deve suportar acesso via web através do portal do próprio fabricante;

23.4.8. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

23.4.9. A solução deve possuir relatório de segurança correlacionado onde consta todo os principais eventos das funcionalidades de URL e prevenção de ameaças:

23.4.10. Tentativa de download de arquivos maliciosos que foram bloqueados;

23.4.11. Tentativa de acesso a sites maliciosos e bloqueados pela organização;

23.4.12. A solução deve permitir o login de múltiplos usuários administradores com perfil de escrita;

23.4.13. A solução deve possuir logs de acessos e logs de auditoria dos administradores da solução;

23.4.14. Prover painel com informações sumarizadas de navegação de usuários contendo quantidade de sessões ativas e consumo de banda através de uma linha do tempo.

23.4.15. A gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação, web e prevenção de ameaças.

23.4.16. Todos os logs gerados pela solução devem ser armazenados por pelo menos 90 dias;

23.4.17. A solução deve se integrar com bases de identificação externas;

23.4.18. A solução deve ser compatível com, no mínimo, os seguintes provedores de identidade:

23.4.18.1. Okta;

23.4.18.2. AzureAD;

23.4.18.3. Active Directory / LDAP;

23.4.18.4. Google Workspace;

23.4.18.5. SAML 2.0 Identity Providers.

23.4.18.6. A solução deve oferecer gerenciamento por API;

23.4.19. O gerenciamento por API deve permitir ao menos executar tarefas como:

23.4.19.1. criar usuários, grupos e listar Networks.

---------- FIM DO APÊNDICE “A” ----------