Outlook

TELETEX | DILIGÊNCIA | PE 90017-2024 | LOTE 3 | TRF6

De Setor de Licitação <licitacao@teletex.com.br>
Data Sex, 28/03/2025 15:57
Para LICITAÇÃO/SELIT-MG: Licitação e Compras <licitacao@trf6.jus.br>
Cc Daniel Augusto <daniel.augusto@teletex.com.br>; Cristian Fruchting <cristian@teletex.com.br>

3 anexos (11 MB)
ATESTADO - HAVAN - CISCO - SEGURANÇA assinado.pdf; Proposta_Comercial_-_HAVAN_-_Projeto_Security_2024_-_V4.2_-_SE.pdf; Diligência - TRF6 Atestado HAVAN v.final(1)(1).pdf;

Sr. Pregoeiro, boa tarde!

REF.: PREGÃO ELETÔNICO N° 90017/2024 – TRF6

Em atenção ao pedido de diligência, a Teletex Computadores e Sistemas Ltda, inscrita no CNPJ n° 79.345.583/0001-42, vem, respeitosamente, apresentar as devidas comprovações referente ao atestado da HAVAN LOJAS DE DEPARTAMENTOS LTDA.

Favor confirmar o recebimento.

At.te
Maria da Conceição Oliveira Silva
Coordenadora de Licitações

Setor de Licitação
Commercial Dept.
licitacao@teletex.com.br
+554121697714 | +5541992710182
www.teletex.com.br

AO TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO/MG
AO ILUSTRÍSSIMO PREGOEIRO OFICIAL E A RESPECTIVA EQUIPE DE APOIO
REF.: PREGÃO ELETRÔNICO 90017/2024

TELETEX COMPUTADORES E SISTEMAS LTDA., pessoa jurídica de direito privado, inscrita no CNPJ/MF sob nº. 79.345.583/0001-42, sediada na Rod. BR 116 N° 12.500, Linha Verde, CEP 81690-200, Curitiba/PR vem, respeitosamente, por seu procurador que adiante subscreve, à presença de Vossa Senhoria, expor, conforme segue.

Em atenção à diligência, referente ao complemento da análise dos recursos e informações contidas no atestado de capacidade técnica emitido pela empresa HAVAN LOJAS DE DEPARTAMENTOS LTDA., vimos por meio deste ofício apresentar uma justificativa quanto à não possibilidade de apresentarmos a íntegra da nossa proposta, conforme diligência.

Entendemos que a transparência e o respeito às normas que regem o processo licitatório são fundamentais. No entanto, gostaríamos de esclarecer que a divulgação da proposta na sua totalidade, conforme solicitado, resultaria na exposição pública de informações estratégicas de nossa empresa, as quais são de natureza confidencial e essencial para a nossa competitividade no mercado.

O acesso irrestrito a esses dados sensíveis, especialmente à composição de custos, preços e margens de lucro,

comprometeria nossa estratégia comercial, bem como caracterizar infração às políticas de compliance e confidencialidade, assim, nossa relação de confiança com o cliente HAVAN.

Adicionalmente, gostaríamos de destacar que, em compras realizadas no mercado privado, é prática comum que a proposta seja aceita com a devida ordem de compra, sem a necessidade de um contrato formal, o que reforça a natureza comercial de nossa estratégia, que se vê, assim, protegida de forma simples e eficaz.

Além disso, gostaríamos de destacar que a apresentação integral da proposta exporá o ambiente do cliente, comprometendo a confidencialidade e a integridade das informações estratégicas, tanto da nossa empresa quanto de nossos parceiros comerciais. A divulgação desses dados pode prejudicar a segurança das operações e a confiança mútua, uma vez que envolve detalhes sensíveis que são fundamentais para a preservação da competitividade e da proteção dos interesses de todas as partes envolvidas.

Por esse motivo, estamos encaminhando *prints* de partes da proposta que podemos disponibilizar, resguardando, assim, as informações confidenciais que estão diretamente relacionadas à nossa estratégia comercial. Ressaltamos que, caso o procedimento licitatório seja homologado, nos comprometemos a apresentar a íntegra da proposta no momento oportuno, de acordo com as orientações da Comissão de Licitação.

Joinville, 23/07/2024

A/C HAVAN

Ref.: Proposta Projeto Security 2024

Prezado Senhor,

Conforme conversamos, apresentamos nossa Proposta Comercial para soluções Cisco Secure, para que seja apreciada.

Desde já agradecemos seu interesse por nossas soluções e nos colocamos ao seu inteiro dispor para a discussão do que expomos aqui.

1 Descição do Projeto

Projeto de renovação e expansão de soluções Cibersegurança, redes e datacenter. Através de dados coletados junto a equipe da HAVAN e através de análise do ambiente, elaborou-se uma proposta técnica e comercial para manter a aprimorar a segurança de dados no ambiente da HAVAN Lojas, CDs, ADM, Datacenter e Cloud.

1.1 Objetivo

Esta proposta tem como resultado esperado Implementar 10 novas capacidades de segurança no ambiente da HAVAN e melhorar/expandir 12 capacidades já existentes. Melhorar no sentido de licenças mais avançadas e expandir em relação ao número atual de licenças contratadas. O projeto ainda prevê a renovação de soluções avançadas de redes com Cisco SD-ACCESS e Cisco ACI para manter a operação atual de datacenter. Prevê a renovação de capacidades existentes de segurança, como proteção de DNS, Microsegmentação e Proteção de e-mail. Abaixo imagem com as capacidades de segurança cobertas neste projeto como resultado da metodologia SAFEX da TELETEX.

4 Valores detalhados

Abaixo valores para todas as soluções do projeto, incluindo renovação e novos produtos:

USER + BREACH ADV + CLOUD ADVANTAGE		
SOLUÇÃO	LICENÇAS	3 ANOS
CISCO SECURE ACCESS ADVANTAGE	12.000	
CISCO SECURE ENDPOINT PREMIER	12.000	
DUO PREMIER	12.000	
EMAIL THREAT DEFENSE & CES ADVANTAGE	12.000	
CISCO XDR ADVANTAGE	12.000	
THOUSANDEYS EXPERIENCE INSIGHTS	12.000	
SECURE NETWORK ANALYSTICS SW	52.500 flows/SEC	
SECURE WORKLOAD SaaS TETRATION	700	
MULTICLOUD DEFENSE PREMIER	14 Gateways	
VULNERABILITY MANAGEMENT PREMIER (KENNA)	14.000 ASSETS	
PANOPTICA (CNAPP)	700	
ASM - ATTACK SURFACE MANAGEMENT Jupiter one	17.500 entidades	[redacted]
CISCO CDO - Gerenciamento Cloud dos Firewalls	6	
CISCO FIREWALL FIREPOWER 3120	2	
CISCO SECURE FIREWALLS - Licenças	6	
ISE + ANYCONNECT	3000	
ISE LOJAS	12000	
DNA WIRELESS + SWITCHING + ROUTING - Renovação	Todo parque	
SUPORTE CISCO ENHANCED	Produtos SEC	
TENABLE NESSUS PROFESSIONAL	1	
ACI - Renovação	Todo parque	
TREINAMENTO OFICIAL DO FABRICANTE	8	
SERVIÇO TELETEX NOVAS SOLUÇÕES	1	
TOTAL GERAL		[redacted]
TOTAL GERAL		[redacted]
VALOR POR ANO		[redacted]
VALOR POR USUÁRIO/MÊS		[redacted]

Informamos ainda que, para garantir a transparência e o cumprimento das exigências do processo licitatório, apresentamos um atestado mais detalhado, contendo todas as informações necessárias para a comprovação da nossa capacidade técnica e qualificação. Este documento visa oferecer um panorama completo, resguardando, ao mesmo tempo, as informações confidenciais que não podem ser divulgadas integralmente.

Caso haja necessidade de verificar a proposta ou obter maiores esclarecimentos, é possível o contato à empresa HAVAN, através do contato Diego Aguirre (diego.machado@havan.com.br). Estamos comprometidos em colaborar

com o processo licitatório, garantindo a transparência e a veracidade das informações, sempre respeitando a confidencialidade das nossas estratégias comerciais.

Agradecemos desde já a compreensão e nos colocamos à disposição para quaisquer esclarecimentos adicionais, a fim de garantir o pleno cumprimento das exigências do processo licitatório, sem comprometer os interesses comerciais da empresa.

Nestes termos, pede deferimento.

Curitiba, 28 de março de 2025.

MARIA DA CONCEICAO OLIVEIRA SILVA:66500630106

Assinado de forma digital por MARIA DA CONCEICAO OLIVEIRA SILVA:66500630106
Dados: 2025.03.28 15:53:41 -03'00'

TELETEX COMPUTADORES E SISTEMAS LTDA.

Maria da Conceição Oliveira Silva

Representante

Projeto HAVAN Security 2024

HAVAN

OP00001525 | Versão 4.2

PROPOSTA COMERCIAL

JOINVILLE | 23/07/2024

Joinville, 23/07/2024

A/C HAVAN

Ref.: Proposta Projeto Security 2024

Prezado Senhor,

Conforme conversamos, apresentamos nossa Proposta Comercial para soluções Cisco Secure, para que seja apreciada.

Desde já agradecemos seu interesse por nossas soluções e nos colocamos ao seu inteiro dispor para a discussão do que expomos aqui.

Atenciosamente,

Luiz Henrique de Lima
Account Manager
Luiz.lima@teletex.com.br
(47) 9 9929 0021
Joinville | SC

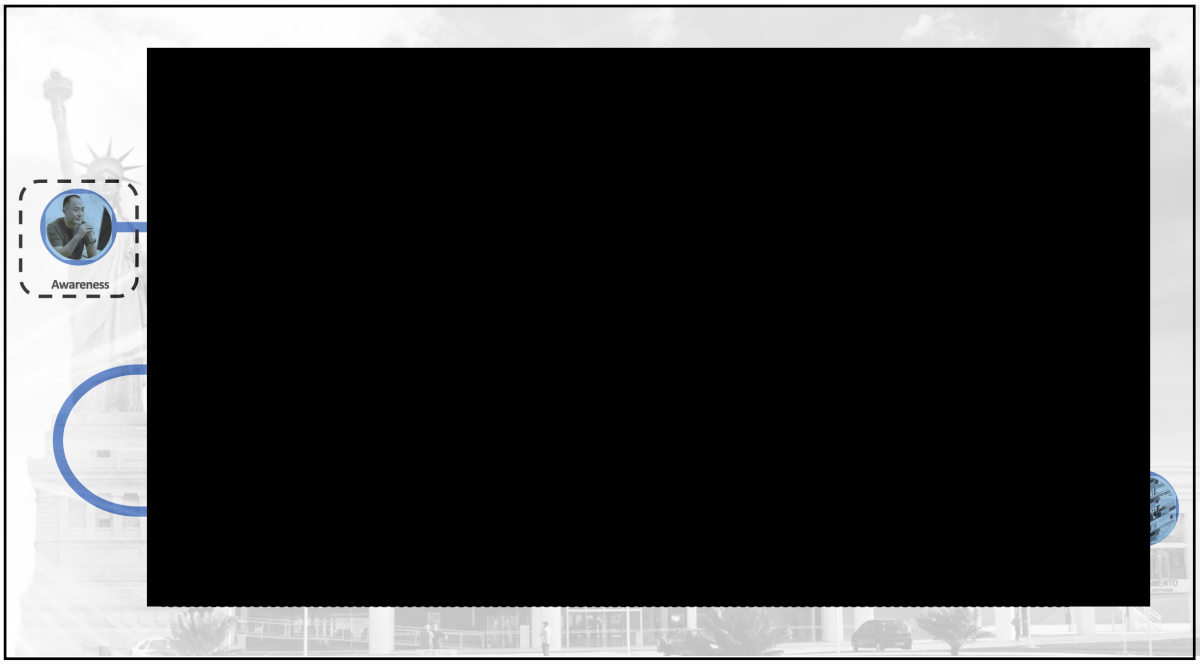
Jean Cachoeira
Technical Account Manager
Jean.cachoeira@teletex.com.br
(47) 9 9904 7719
Joinville | SC

1 Descição do Projeto

Projeto de renovação e expansão de soluções [redacted]

1.1 Objetivo

[redacted] de redes com Cisco SD-ACCESS e [redacted]



[redacted] *1 - S[redacted]2024*

1.2 Etapas/Entregas do Projeto

Neste projeto teremos os seguintes macros de entrega, que posteriormente estará detalhado em produtos e no escopo de serviços de implementação:

- Renovação de licenciamento Cisco DNA para WIRELESS + SWITCHING + ROUTING.
- Renovação de licenciamento Cisco AC
- Renovação da solução Cisco Umbrella DNS
- Renovação de licenciamento Cisco Secure Firewall para todos os firewalls do ambiente
- Renovação e ampliação da solução de Antispam Cisco CES – 12 mil licenças
- Renovação de licenciamento Cisco Anyconnect
- Renovação de licenciamento Cisco ISE
- Renovação e ampliação da solução de microsegmentação Cisco Secure Workload – 700 licenças
- Renovação e ampliação do licenciamento EDR Cisco Secure Endpoint para licença Premier – 12 mil licenças
- Renovação e ampliação da solução de MFA Cisco DUO para licença Premier – 12 mil licenças
- Implantação da solução Cisco Secure Access (CASB/SSE/SASE) – 12 mil licenças
- Implantação de solução de proteção avançada de e-mail Cisco ETD
- Implantação de EDR Cisco para encontrar e corrigir ameaças mais rapidamente
- Implantação do módulo de Observabilidade ThousandEyes Experience Insights – 12 mil licenças de endoint
- Implantação de solução de NDR Cisco Secure Analitics – 52.500 flows/SEC
- Implantação de camada de proteção cloud com Cisco MULTICLOUD DEFENSE – 14 cloud gateways
- Implantação da solução Cisco Vulnerability mManagement Premier (Kenna) – 14.000 Assets
- Implantação de camada de proteção cloud com CNAPP Cisco Panoptica – 700 Assets
- Implantação da solução Cisco Defense Orquestrator para gerenciamento núvem de todos os Firewalls Cisco no ambiente
- Implantação de 1 Cluster de Firewall Cisco Firepower 3120
- Implantação de solução de NAC para as lojas com Cisco ISE Essentials – 12 mil endpoints
- Fornecimento de licença Tenable Nessus Professional – 1 licença
- Implantação da solução Tenable Identity Exposure – 12.300 usuários
- Disponibilização de treinamentos oficiais do fabricante Cisco
- Documentação e repasse de todas as soluções implementadas

1.3 Solução Proposta

O projeto foi desenhado seguindo a metodologia de arquitetura de segurança integrada Cisco, oferecendo uma série de benefícios que são cruciais para proteção eficiente e eficaz de infraestrutura de TI:

- VISIBILIDADE E CONTROLE UNIFICADOS
- MELHOR DETECÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA
- REDUÇÃO DA COMPLEXIDADE E CUSTOS OPERACIONAIS
- AUTOMAÇÃO E EFICIÊNCIA
- MAIOR RESILIÊNCIA E REDUÇÃO DE RISCOS
- CONFORMIDADE REGULAMENTAR SIMPLIFICADA

Os pacotes de segurança da Cisco fortalecem a postura de segurança com uma abordagem consolidada, protegendo a empresa de uma só vez, para que ela possa crescer e se adaptar com eficiência e segurança. A Cisco é reconhecida como líder em cibersegurança e vem investindo significativamente em inteligência artificial (IA) e automação para melhorar a segurança cibernética.

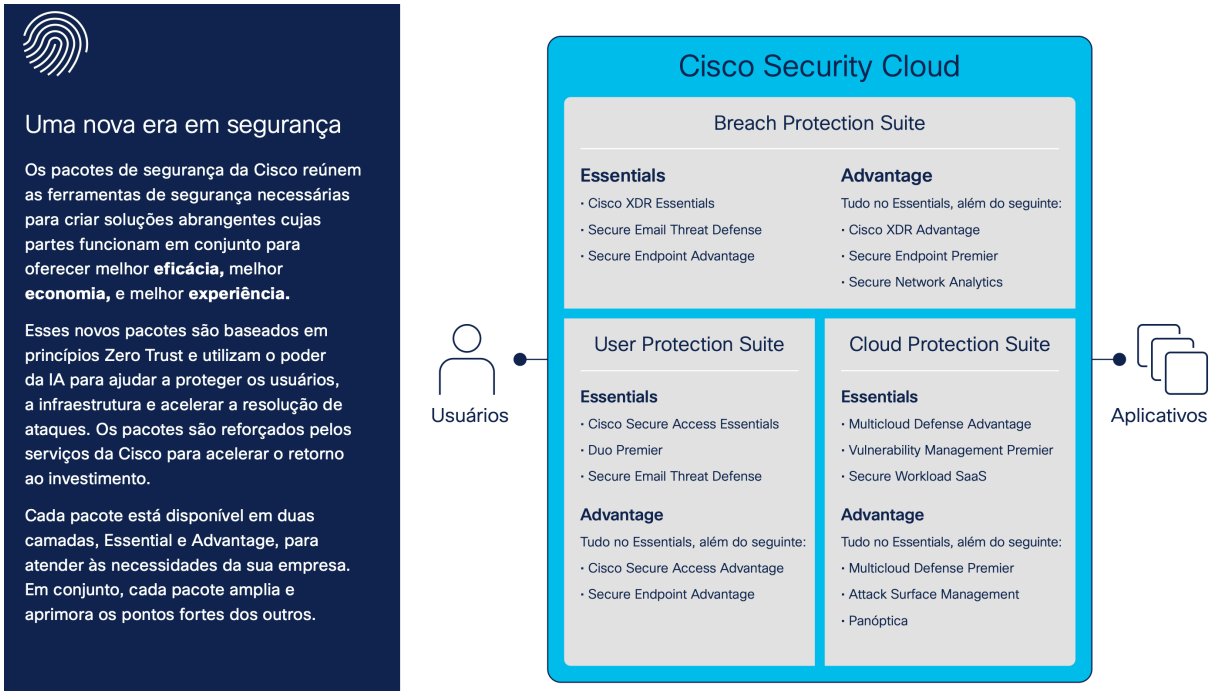


Figura 2 - Abordagem Cisco de proteção de Usuário, Cloud e brechas de segurança

2 Produtos

2.1 Produtos Cisco Secure

Os produtos ofertados nesta proposta são das Suites de segurança da Cisco, conforme apresentado abaixo:

Figura 3 - Cisco Security Suites Composition

- User Protection Suite: Ofereça aos usuários acesso seguro e contínuo a qualquer aplicativo, a qualquer momento, em qualquer dispositivo.
- Cloud Protection Suite: Proteja ambientes híbridos e multicloud com segurança de ponta a ponta para aplicações, cargas de trabalho, redes e nuvens.
- Breach Protection Suite: Capacite as equipes de segurança para simplificar as operações e acelerar a resposta.

2.1.1 Cisco Secure Access

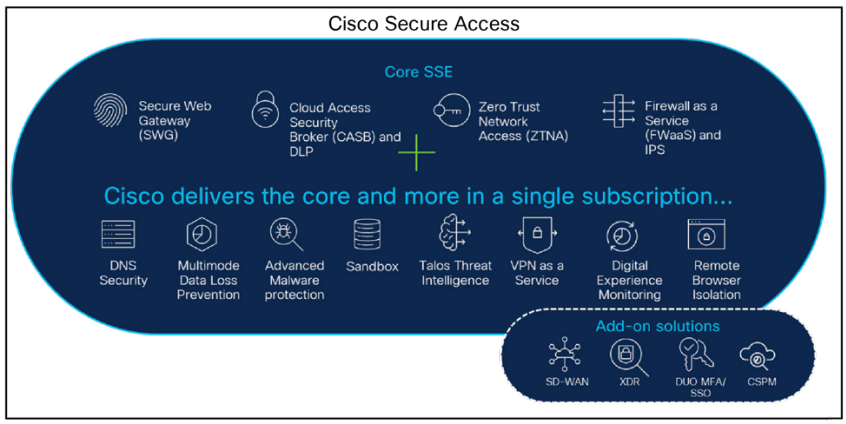
A nova era de trabalho híbrido requer uma abordagem revisada de segurança, e SSE (Security Service Edge) é um facilitador chave da estratégia de trabalho híbrido de qualquer organização. O SSE combina múltiplas funções de segurança na nuvem para proteger funcionários, contratados ou parceiros que trabalham de qualquer localidade, bem como salvaguardar recursos críticos. Quer as sessões envolvam aplicações em data centers privados, locais de SaaS, peer-to-peer, IaaS ou sites da Internet, o SSE atua como um 'intermediário de segurança' para identificar e prevenir múltiplos tipos de atividades maliciosas. Os usuários finais têm a garantia de uma experiência de usuário segura e transparente, em qualquer lugar que trabalhem - escritório, casa ou na estrada. As soluções de SSE devem atender a três requisitos principais: proporcionar uma experiência superior ao usuário, reduzir a complexidade de TI e melhorar a eficácia da segurança.

Visão geral do produto

O Cisco Secure Access é uma solução de segurança na nuvem SSE convergente, baseada em zero trust, que fornece acesso seguro, contínuo e transparente de qualquer coisa para qualquer lugar. A premiada solução de acesso seguro à Internet da Cisco Umbrella foi expandida sob o nome mais amplo de Secure Access para cobrir um conjunto maior de funções relacionadas ao SSE. Agora inclui todos os componentes principais do SSE (SWG, CASB, ZTNA e FWaaS) além de um conjunto expandido de capacidades (DLP multimodal, Segurança DNS, RBI, sandboxing, insights DEM, inteligência de ameaças Talos e medidas para garantir o uso de IA.) em uma licença e plataforma de gerenciamento. Ao aproveitar essas capacidades, todas sob uma plataforma entregue na nuvem, as organizações podem resolver uma variedade de desafios de segurança. Os usuários podem agora acessar com segurança e sem problemas todos os recursos e aplicativos de que precisam, independentemente do protocolo, porta ou nível de personalização.

O Cisco Secure Access é projetado com controles administrativos comuns, estruturas de dados e gerenciamento de políticas que facilitam a interoperabilidade com outros componentes sinérgicos. Por exemplo, uma ampla variedade de provedores de identidade (IDPs), incluindo qualquer serviço baseado em SAML (incluindo AD, Azure AD, Okta, Ping, etc.) para fornecer confirmação de identidade e contexto. Esta solução funciona com outras ofertas da Cisco, incluindo SD-WAN, XDR e monitoramento de experiência digital, bem como tecnologias de terceiros para melhorar os resultados dos clientes.

O Secure Access aplica cibersegurança moderna, enquanto reduz fundamentalmente o risco, simplifica radicalmente a complexidade operacional de TI e minimiza as tarefas realizadas pelos usuários finais.



Funcionalidades:

- Zero Trust Network Access (ZTNA)
- VPNaaS
- Secure Web Gateway (full proxy)
- Cloud access security broker (CASB)
- Data Loss Prevention (DLP)
- Firewall as a Service (FWaaS)
- Intrusion prevention system (IPS)
- Cisco Secure Malware Analytics
- Remote Browser Isolation (RBI)
- DNS-layer security
- Talos threat intelligence
- Cloud malware detection
- Single management and reporting console
- AI Assistant
- Experience Insights: Digital Experience Monitoring (DEM) – 1 APP por endpoint
- Mobile device ZTA support

Datasheet: https://www.cisco.com/c/en/us/products/collateral/security/secure-access/hybrid-workforce-cloud-agile-security-ds.html

2.1.2 [redacted]

[redacted]

- Autenticação multifatorial (MFA) com suporte a Duo Verified Push e FIDO2
- Single Sign-On (SSO)
- Verificação de endpoints confiáveis
- Autenticação sem senha
- Visibilidade dos dispositivos
- Integrações ilimitadas de aplicações
- Autenticação baseada em risco
- Verificações de saúde do dispositivo
- Políticas adaptativas de acesso
- Detecção de ameaças impulsionada por aprendizado de máquina
- Painéis completos e relatórios abrangentes
- Acesso remoto seguro sem VPN
- Verificação de proteção de endpoints

Datasheet: https://duo.com/editions-and-pricing/duo-premier

2.1.3 Cisco E-mail Threat Defense

O Email Threat Defense é uma solução nativa em nuvem que utiliza inteligência superior de ameaças do Cisco Talos. Ela possui uma arquitetura habilitada por API para tempos de resposta mais rápidos, visibilidade completa de e-mails, incluindo e-mails internos, uma visualização de conversas para melhor informação contextual e ferramentas para remediação automática ou manual de ameaças ocultas nas caixas de correio do Microsoft 365.

As organizações de hoje enfrentam um desafio assustador. O e-mail é simultaneamente a ferramenta de comunicação empresarial mais importante e o principal vetor de ataque para violações de segurança. As perdas causadas por ransomware e Comprometimento de E-mail Empresarial são assustadoras e continuam a aumentar. Em 2023, o FBI IC3 recebeu 21.489 queixas de Comprometimento de E-mail Empresarial (BEC) com US$ 2,9 bilhões em perdas relatadas. E os incidentes de ransomware aumentaram para mais de 2.825 queixas, um aumento de 18% em relação a 2022.

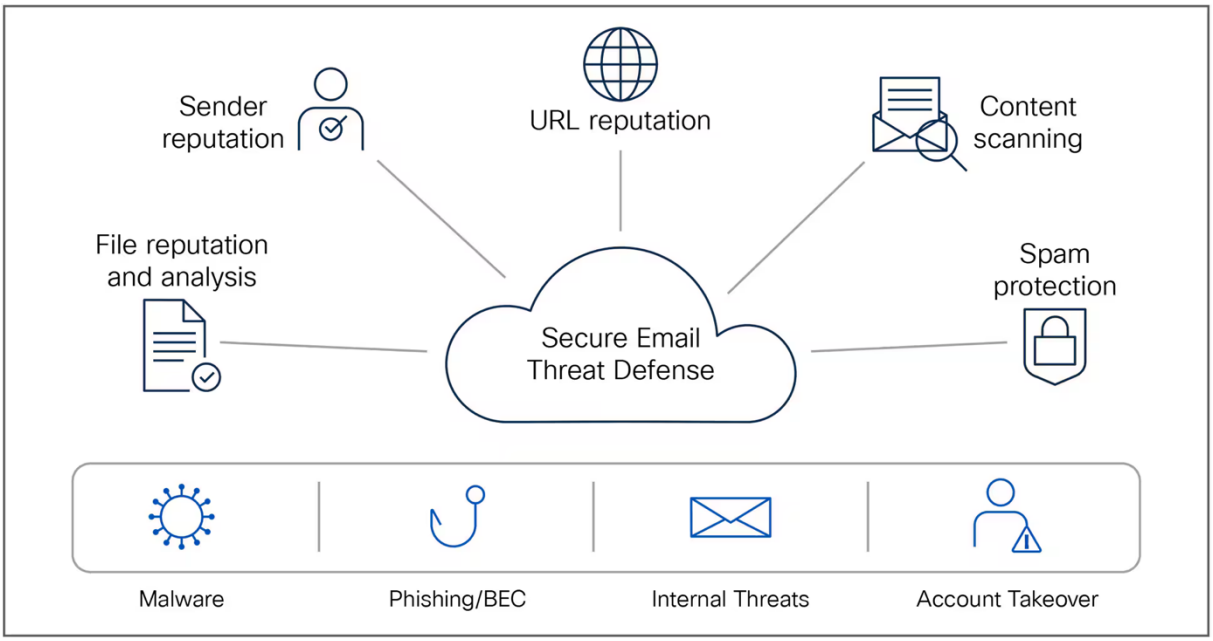
A adoção de e-mail baseado em nuvem, como o Microsoft 365, continua a aumentar. A segurança de e-mail em nuvem é menos dispendiosa e mais escalável em comparação com os dispositivos on-premises e essa tendência está impulsionando o crescimento no mercado de segurança de e-mail SaaS. Porque o e-mail é vulnerável a ameaças avançadas, nos últimos anos a Gartner tem recomendado adicionar segurança suplementar de e-mail em nuvem para proteger sua caixa de correio na nuvem com segurança em camadas e inteligência de ameaças diversificada. O Cisco Secure Email Threat Defense protege sua organização contra o vetor de ameaça número um: o e-mail.

Visão geral do produto

O Email Threat Defense aumenta a segurança nativa do Microsoft 365 e fornece visibilidade completa para mensagens de entrada, saída e internas entre usuários.

Com o Email Threat Defense, os clientes podem:

- Detectar e bloquear ameaças com inteligência superior de ameaças do Cisco Talos, uma das maiores equipes de pesquisa e eficácia de ameaças.
- Combater ameaças avançadas usando Secure Endpoint e Secure Malware Analytics.
- Obter visibilidade completa para mensagens de entrada, saída e internas.
- Aproveitar a remediação rápida baseada em API de mensagens com conteúdo malicioso.
- Usar um painel integrado para busca, relatórios e rastreamento, incluindo visualização de conversas e trajetória de mensagens.
- Melhorar a segurança do Microsoft 365 em menos de 5 minutos sem alterar o fluxo de e-mails.
- Prevenir usuários contra os ataques mais recentes baseados em e-mail, como códigos QR, falsificação de marcas, falsificação de usuários e muitos mais.



Datasheet: https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/secure-email-threat-defense-ds.html

2.1.4 [redacted]

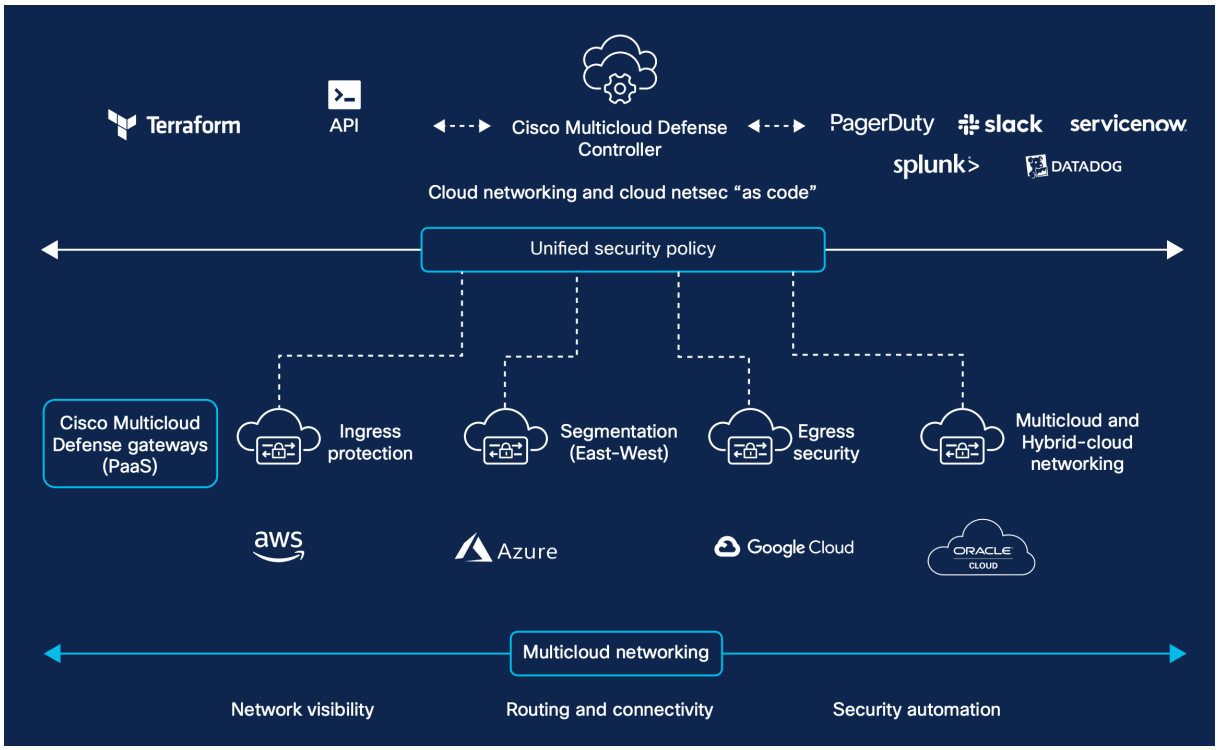
[redacted]

[redacted]

- [redacted]
- [redacted] 4 e DL[redacted]
- [redacted]
- [redacted]

- Modelos de Implementação: Suporta modelos de segurança centralizados e distribuídos, escalando automaticamente conforme necessário para atender às demandas de tráfego.

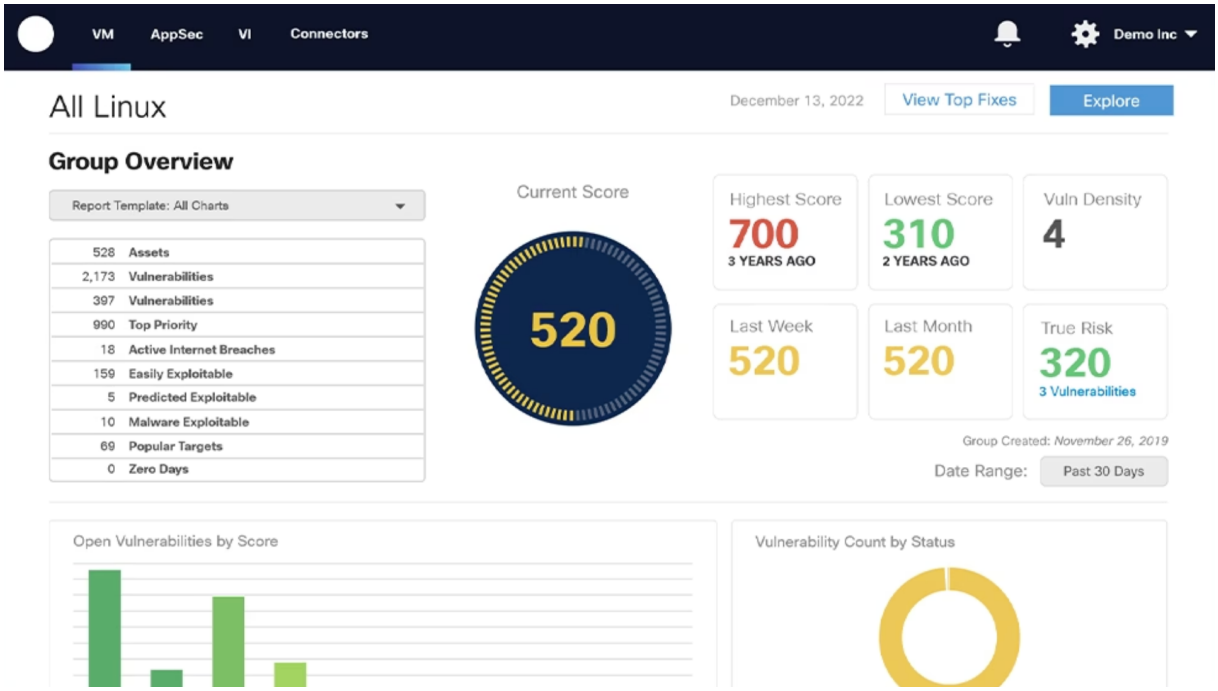
A solução é projetada para fornecer segurança robusta e otimizada em ambientes multicloud, oferecendo visibilidade aprimorada e controle sobre o tráfego, e simplificando a implementação de políticas de segurança.



https://www.cisco.com/site/us/en/products/security/multicloud-defense/index.html

2.1.5 [redacted]

[redacted]



[redacted] o risco

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

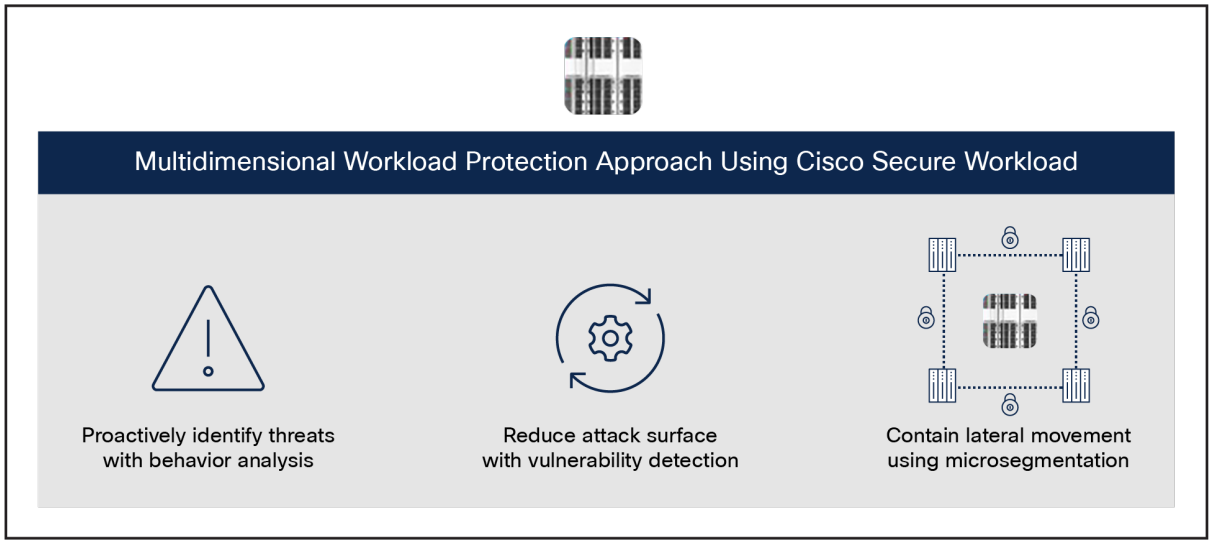
[redacted]

Melhore a eficiência e a comunicação

Uma única fonte de verdade verificada por dados alinha segurança e TI, eliminando atritos e liberando recursos. Além disso, pontuações de risco intuitivas e simplificadas ajudam você a gerar relatórios que qualquer pessoa pode entender.

2.1.6 Cisco Secure Workload

O Cisco Secure Workload (anteriormente Tetration) oferece microsegmentação de confiança zero de forma contínua em qualquer carga de trabalho, ambiente ou localização a partir de um único console. Com visibilidade abrangente de todas as interações de cargas de trabalho e automação poderosa guiada por IA/ML, o Secure Workload reduz a superfície de ataque ao prevenir movimentos laterais, identifica anomalias no comportamento das cargas de trabalho, ajuda a remediar rapidamente ameaças e monitora continuamente a conformidade.



Casos de uso da proteção de Workloads

O Secure Workload oferece microsegmentação de confiança zero para proteger aplicativos, reduzir riscos e manter a conformidade com:

- Políticas de microsegmentação geradas automaticamente através de uma análise abrangente dos padrões de comunicação e dependências de aplicativos.

- Definição de políticas dinâmicas baseadas em atributos com um modelo de política hierárquico para fornecer controles abrangentes em vários grupos de usuários com controle de acesso baseado em funções.

- Aplicação consistente de políticas em larga escala através do controle distribuído de firewalls nativos de hosts e infraestruturas, incluindo ADCs (Application Delivery Controllers) e firewalls.

- Monitoramento de conformidade quase em tempo real de todas as comunicações para identificar e alertar sobre violações de políticas ou possíveis comprometimentos.

- Estabelecimento de padrões de comportamento de cargas de trabalho e detecção proativa de anomalias.

- Detecção de vulnerabilidades comuns com mitigação dinâmica e quarentena baseada em ameaças.

2.1.7 Cisco XDR

O Cisco XDR simplifica as operações de segurança, acelera respostas e capacita as equipes do Centro de Operações de Segurança (SOC) com detecção e resposta a ameaças proativas e orientadas por IA. Ele é projetado para enfrentar os desafios enfrentados pelos analistas de segurança e oferece uma solução extensível, nativa da nuvem, que integra dados de várias ferramentas de segurança e aplica aprendizado de máquina e análises para chegar a detecções correlacionadas.

Ao ir além das abordagens centradas em detecção e resposta de endpoint (EDR) ou em gerenciamento de informações e eventos de segurança (SIEM), o Cisco XDR muda o foco de investigações intermináveis para a remediação dos incidentes de maior prioridade com automação respaldada por evidências, ajudando as equipes do SOC a agir com mais rapidez, eficiência e confiança. Enquanto a tecnologia SIEM tradicional gerencia dados centrados em logs e mede resultados em dias, o Cisco XDR foca em dados centrados em telemetria e entrega resultados em minutos.

O Cisco XDR analisa e correlaciona nativamente as seis fontes de telemetria que os operadores do SOC dizem ser críticas para uma solução de detecção e resposta estendida (XDR): endpoint, rede, firewall, e-mail, identidade e DNS. Com o Cisco XDR, as equipes de segurança podem detectar ameaças além do endpoint, tornando a telemetria e os insights de outras fontes, incluindo a rede, igualmente fundamentais. Através de integrações turnkey e curadas com produtos de segurança de terceiros, bem como o extenso portfólio de soluções de segurança da Cisco, o Cisco XDR oferece uma instalação perfeita em arquiteturas existentes e entrega resultados consistentes, independentemente do fornecedor ou solução.

O [redacted] e insights sobre ativos, garantindo que você sempre veja o quadro completo.

Ao [redacted] de segurança podem responder a ataques com confiança, aumentar a eficiência do SOC e automatizar tarefas para uma abordagem mais proativa à segurança.

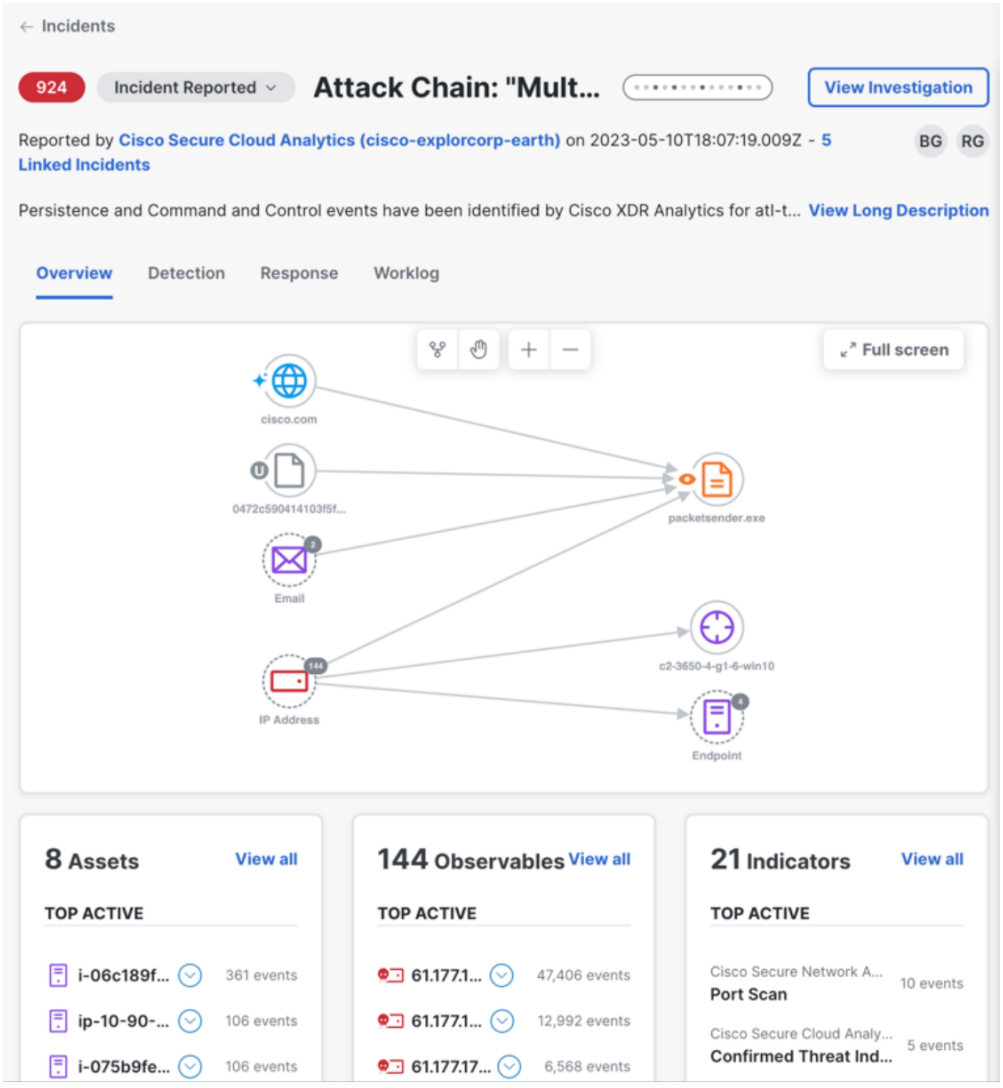


Figura 4 - Cisco XDR Attack Chain

2.1.8 [redacted]

[redacted]

[redacted]a para reduzir drasticamente o tempo médio de detecção e resposta a ameaças.

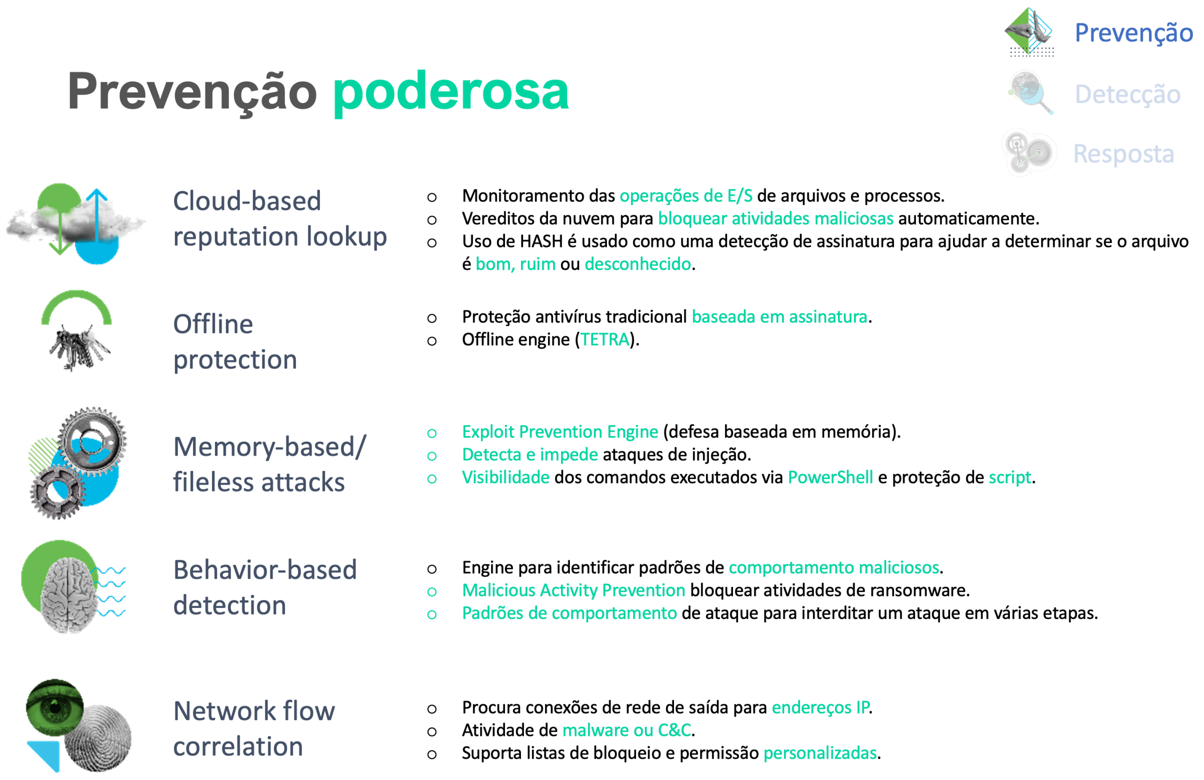
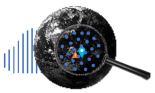


Figura 5 – Cisco Secure Endpoint - Prevenção

Detecção contínua através do tempo

Prevenção
Detecção
Resposta

 Vulnerable surfaces	○ Identifica aplicativos/doftwares em execução com vulnerabilidades conhecidas. ○ Fornece links para descrições e classificações de gravidade no banco MITRE CVE. ○ Resposta proativa, incluindo o bloqueio de versões vulneráveis.
 Prevalence analysis	○ Identifica aplicações incomuns no ambiente; ○ Envio automaticamente do aplicativo/arquivo para o Cisco Secure Malware Analytics. ○ Com base em milhares de indicadores de comportamento, o aplicativo pode ser classificado de volta ao endpoint como evento retrospectivo.
 Indications of compromise	○ Eventos de arquivo, telemetria e intrusão são correlacionados e priorizados. ○ Ajudar as equipes de segurança a identificar incidentes de malware.
 Global Threat Alerts (Cognitive Intelligence)	○ Monitora/investiga o tráfego web-based suspeitos que entra e sai dos endpoints; ○ Propósito é detectar e responder atividades de C&C e malwares utilizando machine learning e análise de comportamento.
 API integrations	○ API bidirectional habilitada no endpoint. ○ Integrações mais fáceis com ferramentas de segurança de terceiros e SIEMs. ○ Acesso a eventos e dados do endpoint diretamente via API.

Tempo de detecção da Cisco é de **14 horas**, contra a média do setor de **100 a 200 dias**.

Figura 6 - Cisco Secure Endpoint - Detecção

Resposta – não se trata apenas do endpoint

Prevenção
Detecção
Resposta

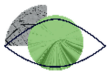
 Retrospective events	○ Monitoramento contínuo e resposta rápida a novas informações de ameaças. ○ Secure Malware Analytics analisa o comportamento de um arquivo em relação a milhões de amostras e bilhões de artefatos de malware.
 Endpoint isolation	○ Endpoints podem ser isolados do restante da rede. ○ Não interrompe a solução de problemas e a investigação forense. ○ Pode ser ativada com um clique ou resposta automática com base na gravidade do evento.
 Automated actions	○ Isolamento de endpoints. ○ Envio automático de amostras para análise, com captura instantâneas forenses. ○ Mover o endpoint para um grupo com políticas diferentes.
 SecureX integration	○ Possibilita ações de resposta em outros produtos (bloqueio de DNS no Umbrella por exemplo), diretamente da console do SecureX. ○ Ações de orquestração do SecureX com fluxos de trabalho otimizados. ○ Dashboard centralizado com informações relevantes do cenário atual do ambiente.
 Cross-platform policy view	○ Produtos como Secure Firewall, Secure Email, etc, podem se conectar ao console do Secure Endpoint. ○ Lista de bloqueios e/ou permissões em um só lugar.

Figura 7 - Cisco Secure Endpoint - Resposta

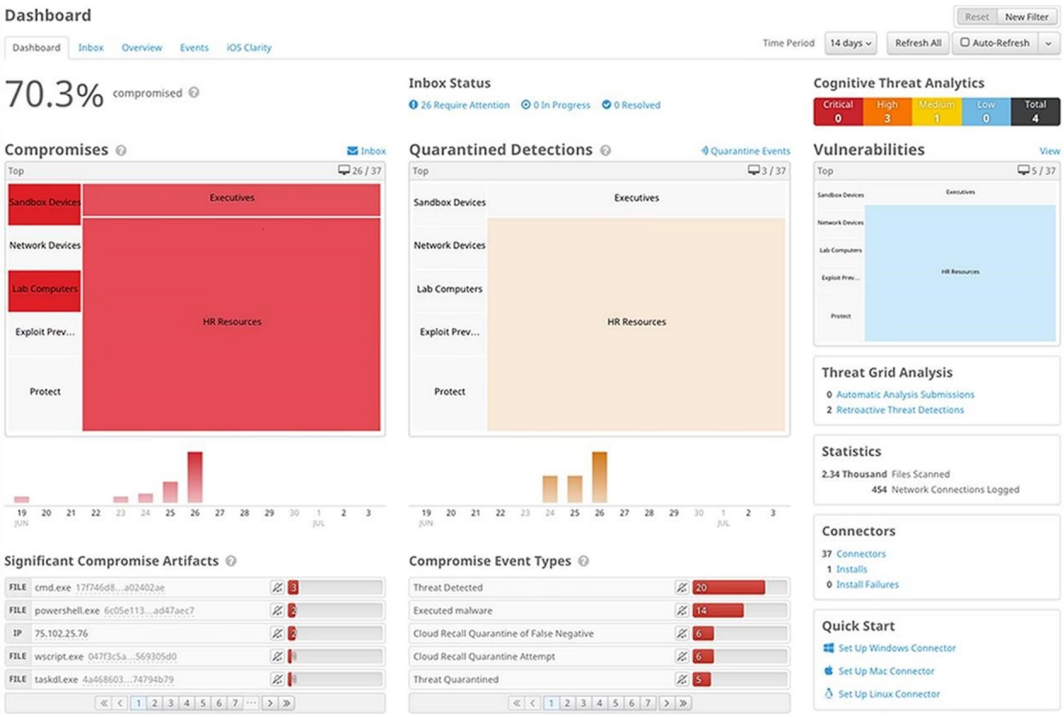


Figura 8 - Dashboards Alerts

Datasheet:https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html

2.1.9 [redacted]

[redacted]

As organizações já investiram muito em sua infraestrutura e segurança de TI. No entanto, as ameaças continuam encontrando maneiras de penetrar. Além disso, muitas vezes leva meses ou até anos para detectar violações. Essa falta de visibilidade é uma função da crescente complexidade da rede e das ameaças em constante evolução. As equipes de segurança com recursos limitados e ferramentas desarticuladas só podem fazer até certo ponto. Praticamente todas as organizações possuem soluções de segurança, como firewalls, mas como sabem se essas ferramentas estão funcionando, gerenciadas e configuradas corretamente? Como sabem se essas ferramentas estão fazendo o trabalho que precisam fazer?

Decidimos virar o problema de cabeça para baixo — por que não aproveitar seu investimento existente, a rede, para proteger sua organização? A telemetria da rede é uma fonte rica de dados que pode fornecer insights valiosos sobre quem está se conectando à organização e o que estão fazendo. Tudo toca a rede, então essa visibilidade se estende desde a sede até a filial, o data center, os usuários itinerantes e os dispositivos inteligentes, abrangendo nuvens privadas e públicas. Analisar esses dados pode ajudar a detectar ameaças que podem ter encontrado uma maneira de contornar seus controles existentes antes de causarem um grande impacto.

A solução é o Secure Network Analytics, que utiliza a rede para fornecer visibilidade do tráfego de ponta a ponta, tanto localmente quanto em nuvens privadas e públicas. Essa visibilidade inclui conhecer todos os hosts e ver quem está acessando quais informações a qualquer momento. A partir daí, é importante entender qual é o comportamento normal para um usuário ou "host" em particular e estabelecer uma linha de base a partir da qual você pode ser alertado sobre qualquer mudança no comportamento do usuário no instante em que ocorre.

O Secure Network Analytics oferece dois modelos de implantação diferentes — no local como um appliance de hardware, ou como uma máquina virtual. O Secure Cloud Analytics (anteriormente Stealthwatch Cloud) é a versão Software como Serviço (SaaS) do Secure Network Analytics. Além de monitorar a rede privada, o Secure Cloud Analytics também pode ser implantado para detectar ameaças e problemas de configuração na nuvem pública.

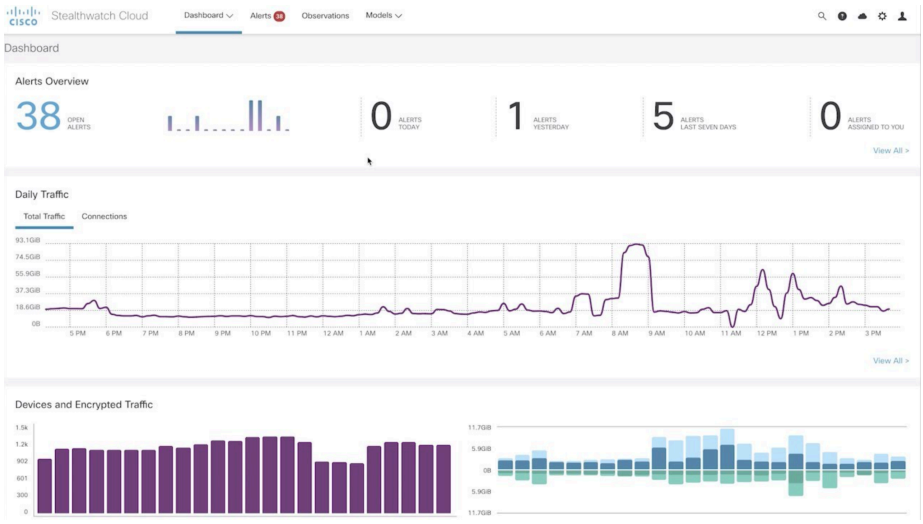


Figura 9 - Cisco Stealtwatch Dashboard

2.2 Suporte Cisco Incluído

Juntamente com a suite de produtos Cisco Secure, está incluso o suporte no modelo Solution Support Enhanced, onde teremos os seguintes diferenciais:

	Deliverables	SWSS Enhanced Included with Suites
	Solution Support (Reactive Technical Support)	24*7 with 30-min response times Primary point of contact Multi product, vendor issue resolution
Adoption Services	Onboarding Guidance	Y
	Digital Adoption Journey	Y
	Annual Security Health Check's	Y

Figura 10 - Entregáveis Suporte Cisco

Enhanced	Onboarding Guidance	• Getting started: Kick-off, Overview & Planning, Pre-requisites, Security Success Plan, Licensing Management Demo, Onboarding collateral Resources. • Deployment Guidance: Architecture/Policy Guidance, integration guidance as applicable • Deployment validation use cases as applicable • Outcome validation as applicable
	Digital Adoption	• Unlimited 1 to many adoption sessions • Enrollment in Digital Journey to receive adoption & best practices information • Access to digital learning, knowledge base and community best practices • Reactive technical adoption guidance (hand-raiser)
	Annual Security Health Check's	• Annual Security Health Check for customer environment • Targeting elements that impacts security posture and performance. • Validation of improvement

Figura 11 - Serviços de Adoção

2.3 Cisco Secure Firewall

A Série Cisco Secure Firewall 3100 é uma família de dispositivos de segurança focados em ameaças que oferece resiliência empresarial e defesa superior contra ameaças. Cada modelo oferece um desempenho excepcional para vários casos de uso de firewall, mesmo quando funções avançadas de proteção contra ameaças estão ativadas. Essas capacidades de desempenho são possibilitadas por uma arquitetura moderna de CPU combinada com hardware desenvolvido especialmente para otimizar funções de firewall, criptografia e inspeção de ameaças.

Figura 12 - Cisco Secure Firewall 3100 Series

2.4 Cisco Defense Orchestrator

O Cisco Defense Orchestrator é uma solução de gerenciamento baseada em nuvem que permite gerenciar políticas de segurança e configurações de dispositivos com facilidade em várias plataformas de segurança Cisco e nativas da nuvem.

O Cisco Defense Orchestrator gerencia centralmente elementos de políticas e configurações em:

- Cisco Multicloud Defense;
- Cisco Secure Firewall ASA;
- Cisco Secure Firewall Threat Defense (FTD);
- Cisco Meraki™ MX;
- Dispositivos Cisco IOS;
- Grupos de segurança AWS.

O Cisco Defense Orchestrator também incorpora a versão em nuvem do Firewall Management Center (FMC), proporcionando uma experiência totalmente unificada entre o gerenciamento de firewalls on-premises e baseados na nuvem. Isso expande o gerenciamento de políticas e configurações.

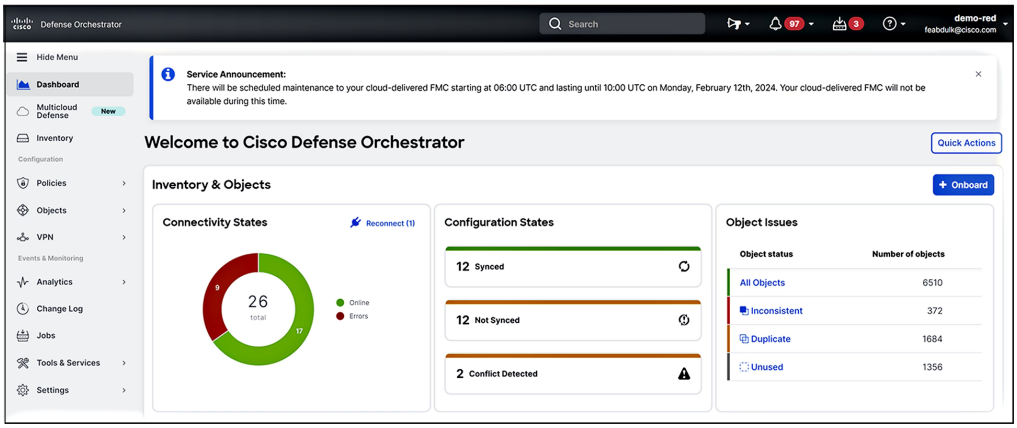
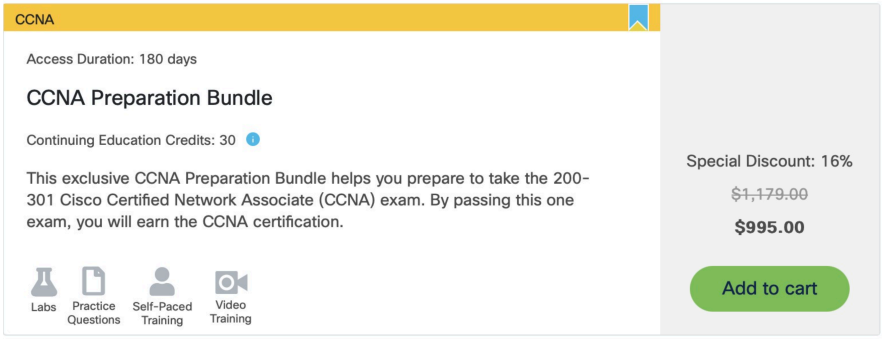


Figura 13 - Cisco Defense Orchestrator

2.5 Treinamento oficial Cisco

Essa proposta contempla 80 Learning Credits Cisco, que podem ser utilizados para treinamentos oficiais no site https://learningnetworkstore.cisco.com/. Essa quantidade é possível comprar 8 treinamentos oficiais para certificação CCNA, incluindo conteúdo, LAB e simulados.



Os learning credits podem ser utilizados para qualquer outro treinamento disponível na página da Cisco.

2.6 [redacted]

[redacted]

- [redacted]
- [redacted]

- Licenças Cisco [redacted]
- [redacted] e Premier);
- Licenças Cisco [redacted]
- Licenças Cisco [redacted]
- Licenças Cisco [redacted]

OBS: Não [redacted]

3 Serviços TELETEX

O escopo de serviços ofertado para a HAVAN contempla a implementação das soluções ofertadas assim como o suporte. A seguir, está descrito o escopo de serviço de implementação e sustentação da estrutura de soluções Cisco na HAVAN:

3.1 Cisco Secure Access (Advantage)

A implementação do Cisco Secure Access para o ambiente HAVAN será realizado pela TELETEX em conjunto com as equipes de infraestrutura da HAVAN. Serão configurados os recursos de ZTNA, VPNaaS, Proxy SWG, CASB, FWaaS, DNS, DLP, AMP e Monitoramento da experiencia digital, trazendo as configurações da solução atual e adaptando para o Secure Access. Abaixo seguem as etapas macro do plano de implementação:

Planejamento;

- Atividades de planejamento para migração da atual solução de SASE/SSE para a nova solução Cisco Secure Access;

Implementação;

- Configuração das conexões entre HAVAN e Cloud Cisco;
- Configuração dos recursos de conexão;
- Configuração de conectividade para os usuários;
- Configuração dos endpoints (Workstations e Mobile) e recursos de rede;
- Configuração do Experience Insights;
- Reports e Logging.

Documentação As Built;

Monitoramento;

Repasse de conhecimento;

Não fazem parte dos serviços:

- Alteração na topologia com as Lojas (SD-WAN Meraki);
- Alteração na topologia com o CDH (SD-WAN Viptela);
- Configuração de equipamentos não fornecidos pela TELETEX;
- Deployment manual de agentes em estações de trabalho de usuários;
- Suporte a estação de trabalho de usuários em caso de falha no S.O. não causado pelo produto implementado;
- Qualquer configuração na estrutura do Microsoft 365.

3.2 [redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted] **Built;**

Monitoramento;

Repasse de conhecimento;

Não fazem parte dos serviços:

- Instalação de novos agentes em novas workstations/servidores;
- Tratativa dos incidentes e alertas recebidos no Secure Endpoint;

3.3 [redacted]

[redacted], Device Health, Risk-Based Authentication, Threat Detection e Remote Access.

Planejamento;

- Atividades de planejamento implementação dos novos recursos disponíveis no licenciamento premier no ambiente HAVAN;

Implementação;

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted] detecta tentativas de ataque em andamento usando o Duo Trust Monitor;

Documentação As Built;

Monitoramento;

Repasse de conhecimento;

Não fazem parte dos serviços:

- Qualquer configuração na estrutura do Microsoft 365
- Instalação manual dos agentes em workstations;

[redacted]

Planejamento;

[redacted]

- Atividades de planejamento implementação do Cisco Multicloud Defense no ambiente HAVAN;

Implementação;

- Setup inicial do tenant SaaS;
- Integração com as clouds (AWS e AZURE);
- Ativação da feature de Visibility nas clouds;
- Configuração dos Ingress e Egrees Gateways;
- Configuração da comunicação entre Cloud vs On-prem via IPsec;
- Enforcement de regras para os recursos em cloud (limitado a 5 VNs);

Documentação As Built;

Monitoramento;

Repasse de conhecimento;

Não fazem parte dos serviços:

3.6 [redacted]

[redacted] e segurança da HAVAN. Abaixo a lista de atividades a serem executadas no projeto:

Planejamento;

- Atividades de planejamento implementação do Cisco Cloud Application Security (Panoptica) no ambiente HAVAN;

Implementação;

- [redacted]

- Integrações com outros produtos;

Documentação As Built;

Repasse de conhecimento;

Não fazem parte dos serviços:

- Resolução de problemas identificados pela solução nos produtos HAVAN;
- Resolução de vulnerabilidades identificadas pela solução no ambiente HAVAN;

3.7 [redacted], que ainda não estão cobertos pela solução.

Planejamento;

- Atividades de planejamento implementação do Cisco Secure Worklolad no ambiente HAVAN;

Implementação;

- Instalação dos agentes nos servidores;
- Ajustes nos escopos de aplicações;
- Execução do ADM RUN para validação das politicas;
- Enforcement das novas politicas;

Documentação As Built;

Repasse de conhecimento;

Não fazem parte dos serviços:

- Manter as políticas atualizadas no ambiente HAVAN;

3.8 [redacted]

[redacted]

- Disponibilização da tenant SaaS;
- Integração dos scanners externos;
- Configurar os Risk Meters (limite de 5);
- Análise no gerenciamento de vulnerabilidades;
- Priorização de vulnerabilidades e patches de segurança;

Documentação As Built;

Repasse de conhecimento;

Não fazem parte dos serviços:

- Resolver as vulnerabilidades no ambiente HAVAN;

3.9 [redacted]

[redacted]

- [redacted]nejamento [redacted];

Implementação;

- Disponibilização da tenant SaaS;

- [redacted]

Documentação As Built;

Repasse de conhecimento;

Não fazem parte dos serviços:

- Realizar respostas a incidentes de segurança via XDR;

3.10 [redacted] recebimento de Flows.

Planejamento;

- Atividades de planejamento implementação do Cisco Network Analytics no ambiente HAVAN;

Implementação;

- [redacted]

Documentação As Built;

Repasse de conhecimento;

Não fazem parte dos serviços:

- Instalação de agentes de forma manual nas workstations HAVAN;

Este é um escopo geral que pode ser personalizado para atender às necessidades específicas da HAVAN. Importante frisar que a TELETEX suporta ambientes e sistemas que possuem garantia e/ou suporte ativo com a fabricante, não se responsabilizando em suportes de produtos em estágio de fim de vida (EOL).

4 Valores detalhados

Abaixo valores para todas as soluções do projeto, incluindo renovação e novos produtos:

USER + BREACH ADV + CLOUD ADVANTAGE		
SOLUÇÃO	**LICENÇAS**	**3 ANOS**
CISCO SECURE ACCESS ADVANTAGE	12.000	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	R$ [redacted]
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]e	
SUPORTE CISCO ENHANCED	Produtos SEC	
[redacted]	[redacted]	
[redacted]	[redacted]	
TREINAMENTO OFICIAL DO FABRICANTE	8	
SERVIÇO TELETEX NOVAS SOLUÇÕES	1	
TOTAL GERAL		[redacted]
TOTAL GERAL		[redacted]
VALOR POR ANO		[redacted]
VALOR POR USUÁRIO/MÊS		[redacted]

Abaixo fluxo de pagamento para itens Cisco + SRV de Implantação.

FLUXO DE PAGAMENTO - 3 ANOS		
VENCIMENTO	**VALOR Cobrança**	**VALOR ANO**
[redacted]	[redacted]	R$ [redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	

5 Condições comerciais

5.1 Gerência de Projetos

A metodologia de gestão do projeto será baseada nas melhores práticas definidas pelo PMBOK Guide – Project Management Body of Knowledge – documento mantido e publicado pelo "PMI – Project Management Institute", organização internacional que define os padrões e metodologias para melhores para práticas de gerenciamento de projetos.

5.2 Equipe técnica

Gerente de Projetos (TELETEX), responsável por:

- Planejamento geral do projeto de forma compartilhada com a equipe HAVAN;
- Preparação e manutenção do Plano de Projeto;
- Coordenação de atividades do dia-a-dia visando cumprimento dos prazos estabelecidos;
- Reunião de Revisão de Status semanal para acompanhamento do cronograma;
- Antecipação e comunicação com HAVAN de quaisquer desvios no cronograma e adoção de medidas corretivas;
- Atuação como ponto único de contato com HAVAN para todas as atividades da TELETEX;
- Gerenciamento dos recursos humanos necessários para a realização das atividades da TELETEX;
- Gerenciamento dos procedimentos de Requisição de Mudança.

Consultor de TI, responsável por:

- Análise dos requerimentos;
- Instalação, configuração e customização dos produtos e serviços que compõem a solução, de acordo com o escopo;
- Execução dos testes.

Coordenador do Projeto (HAVAN), responsável por:

- Gerenciar o projeto e as atividades sob sua responsabilidade;
- Aprovar o Plano de Projeto e gerenciar as Requisições de Mudança;
- Obter as informações que se façam necessárias para o bom andamento do projeto;
- Participar ativamente das reuniões de revisão do programa;
- Informar eventuais desvios no cronograma do projeto e adotar medidas corretivas;
- Atuar como ponto único de contato para a TELETEX e outros fornecedores, que vierem a ser envolvidos no projeto ou em atividades correlatas;
- Gerenciar os recursos humanos do projeto;
- Gerenciar e prover os testes de aceitação previstos.

Os serviços serão executados por um ou mais analistas da equipe técnica da TELETEX, definido(s) pelo gerente de projetos com base nas aptidões e conhecimentos técnicos necessários para realização de cada atividade específica.

5.3 Horário de trabalho

Os serviços serão realizados preferencialmente no horário comercial, de segunda a sexta-feira, exceto feriados locais e nacionais.
Serviços que necessitem ser realizados fora do horário e que não estiverem relacionados no escopo apresentado serão objeto de proposta complementar ou inclusão em nova versão.

5.4 [redacted]

5.5 Melhor esforço

A TELETEX empregará sempre seu melhor esforço na execução dos serviços contratados, independentemente do seu grau de complexidade, respeitando os prazos previstos e os parâmetros técnicos de qualidade definidos pelos fabricantes envolvidos. Para tanto, a TELETEX vale-se de processos modernos e de mercado no gerenciamento de tempo, recursos humanos, qualidade, comunicação, integração, custo, riscos, escopo e suprimentos.

5.6 Garantias

Será assegurado aos serviços prestados pela TELETEX, garantia contra falhas de implantação, desde que imputáveis à equipe técnica disponibilizada, pelo período de 90 (noventa) dias a partir da assinatura do termo de aceite.
Esta garantia se limita exclusivamente a implantação das soluções sob a execução e/ou supervisão técnica da TELETEX ou terceiros expressamente por ela autorizados.

5.7 Atendimento em garantia

Os atendimentos em garantia serão realizados nos dias úteis, de segunda a sexta-feira, durante o horário comercial das 8h às 18h, exceto feriados locais e nacionais.
O tempo de resposta para chamados em garantia será de 4 (quatro) horas úteis.
Não-afetos à garantia serão cobrados na mesma base dos atendimentos pós-garantia.

Os chamados em garantia deverão ser abertos através do **Service Desk Teletex**, por e-mail (servicedesk@teletex.com.br), por telefone **(41) 2169-7717** para Curitiba/PR e Região Metropolitana e 0800 703 1122 para demais localidades no Brasil.

5.8 Atendimento pós-garantia

Todo e qualquer atendimento necessário depois de decorrido o prazo de garantia dos serviços de instalação dos equipamentos, será objeto de proposta complementar e só será realizado após seu aceite.

Não estão contempladas na presente proposta taxa de deslocamento para visitas relacionadas com serviços de reprogramação ou decorrentes de falhas não constatadas nos equipamentos.

Os atendimentos serão faturados com base na quantidade de horas utilizadas e nos valores praticados pela TELETEX na data da prestação do atendimento.
Os chamados fora de garantia deverão ser abertos através do **Service Desk Teletex**, por e-mail (servicedesk@teletex.com.br), por telefone **(41) 2169-7717** para Curitiba/PR e Região Metropolitana e **0800 703 1122** para demais localidades no Brasil.

5.9 Exclusão de garantia

A garantia não abrange danos causados pela HAVAN, por acidentes decorrentes de operação indevida ou negligente, manutenção ou armazenagem inadequadas, operação anormal ou em desacordo com as especificações, obras civis mal acabadas, influências de natureza química, eletroquímica, elétrica, climática ou atmosférica, tais como: enchentes, inundações, descargas elétricas e raios, incêndio, terremoto, sabotagem, vandalismo ou por fornecimento de energia elétrica e outros casos fortuitos ou de força maior, previstos na legislação. Neste caso, uma vez comprovado o fato, todo e qualquer serviço fornecido pela TELETEX na reparação dos danos será realizado mediante aprovação de Proposta Técnica Comercial correspondente.

Despesas de deslocamento, mão-de-obra, diárias e estadias de visitas técnicas ao local de instalação, fretes, embalagens e seguro de transportes ocorrerão por conta da HAVAN.

A garantia não implica em reconhecimento de quaisquer despesas adicionais ou de danos indiretos ou lucros cessantes.

5.10 Aceite de entrega dos serviços

O Aceite de Entrega dos Serviços poderá ser feito através da assinatura da HAVAN e carimbo com CNPJ no documento constante dessa proposta, enviando digitalizado por e-mail e posteriormente entregue em mãos.

Em caso de não haver nenhuma das respostas supracitadas em até 15 dias do recebimento de um destes dois documentos, considerar-se-á ocorrida nessa data a aceitação tácita dos serviços, tomando-se referida data como base para a emissão do faturamento correspondente.

Quando da execução de serviços em mais de uma fase, haverá aceites de entrega parciais para cada uma, com o faturamento correspondente à proporção de horas realizadas em relação ao total previsto para o projeto final. Caracterizar-se-á “serviços em fases”, quando houver intervalo de mais de 30 dias entre a execução de tarefas do escopo proposto.

Os Termos de Aceite parciais, se darão através de documento de Close-Out ou por resposta à mensagem eletrônica (e-mail) enviada pela TELETEX com esta finalidade. Para tanto, a mensagem eletrônica conterá em seu título: primeiro o número da proposta e a fase referida para a execução dos serviços e a informação "Aceite de Entrega dos Serviços – Fase X".

5.11 Restrições e recursos não previstos

Preços e condições comerciais válidos para os itens e quantidades especificados. Qualquer mudança nas descrições representará alterações nos valores propostos.

5.12 Formação de preços

Para o faturamento os valores em dólares americanos serão convertidos para moeda nacional corrente na data do faturamento utilizando a taxa BACEN PTAX800 publicada no website do Banco Central do Brasil do dia útil imediatamente anterior à data da emissão da fatura. http://www4.bcb.gov.br/pec/taxas/batch/taxas.asp?id=txdolar&id=txdolar

Estes valores incluem todos os impostos incidentes (CIF) com as alíquotas vigentes na data da emissão desta proposta, sendo eventuais alterações entre esta data e a data do faturamento, repassadas ao valor informado nesta. Qualquer imposto criado, alterado ou extinto, após a assinatura do Contrato/Ordem de Compra, cuja base de cálculo afete o preço contratado, implicará na revisão dos preços, em igual medida, para mais ou para menos, conforme o caso. A alteração ou criação de tributos de repercussão indireta, assim como encargos sociais e trabalhistas, não repercutem nos preços contratados.

Os valores de licenciamento contemplados neste projeto tratam-se de aquisição de subscrição 3 ou 5 anos sem possibilidade de cancelamento. Entende-se o parcelamento sugerido como prazo de pagamento do projeto conforme condições especiais desta negociação.

5.13 Prazo de entrega

A TELETEX, o(s) fabricante(s), ou distribuidor(es) enviará(ão) os produtos ao endereço indicado formalmente pela HAVAN em um prazo médio de 60 dias contados após a assinatura do contrato, recebimento da ordem de compra ou formalização de aceite desta proposta.

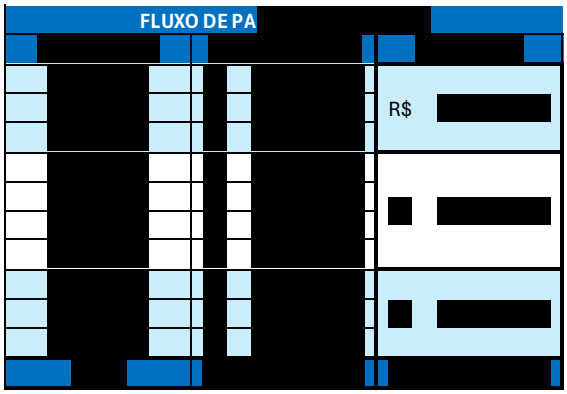
Atrasos por motivos alheios à gerência da TELETEX, como problemas na fabricação, logística do material pelo fabricante, trâmites alfandegários e outros eventos poderão afetar a entrega efetiva. Neste caso, a TELETEX não poderá assumir nenhum tipo de penalidade pelo não atendimento das previsões de entrega contidas nesta proposta.

5.14 Frete

Frete

6 Pagamentos

Pagamento para cada cenário confo



A **HAVAN LOJAS DE DEPARTAMENTOS LTDA, com sede em Brusque (SC), situado na Rodovia Antonio Heil, nº 200, inscrito no CNPJ/MF sob o nº 79.379.491/0001-83**, atesta para os devidos fins, que a empresa **TELETEX COMPUTADORES E SISTEMAS LTDA**, inscrita no CNPJ 79.345.583/0001-42, com matriz estabelecida à Rodovia BR 116, nº 12.500, CEP 81.690-200, bairro Parolin, na cidade de Curitiba, Estado do Paraná, e suas filiais de: **Santa Catarina** – CNPJ 79.345.583/0003-04, localizada na Rua Dona Francisca, 8300 Bl. L, sala 5, Joinville| **Rio Grande do Sul** – CNPJ 79.345.583/0004-95, localizada na Av. Praia de Belas, 1212, Sala 1311 andar 13, Porto Alegre | **Paraíba** - CNPJ 79.345.583/0008-19, localizada na Rua João Câncio, n.º 620, sala 1301, Bairro Manaíra, CEP sob n.º 58.038-340, João Pessoa | **Distrito Federal** – CNPJ 79.345.583/0011-14, localizada na SCN Quadra 5 Bloco A, EN 50, Sala 1322, Asa Norte, CEP sob o nº 70.715-010, Brasília | **São Paulo** CNPJ 79.345.583/0010-33, localizada na Avenida Doutor Cardoso de Melo, n.º 1308, Sala 71, Bairro Vila Olímpia, CEP sob n.º 04.548-004, São Paulo | **Espírito Santo** – CNPJ 79.345.583/0015-48, localizada na Avenida Acesso Rodoviário, s/nº, Sala B5,Quadra 9, Módulos 2/3, Bairro Terminal Intermodal da Serra, CEP sob o nº 29.161-376, Serra | **Foz do Iguaçu** – CNPJ 79.345.583/0016-29, localizada na Avenida José Maria de Brito, 1707, Bairro Polo Centro, CEP sob o nº 85.863-730 , através de contrato firmado para o Projeto de Segurança entre as partes, forneceu os produtos e serviços abaixo descritos:

- Fornecimento de licenças e subscrições
- Implementação, parametrização e acompanhamento técnico
- Capacitação on-site
- Suporte Técnico on-site
- Suporte Técnico remoto

ITEM	DESCRIÇÃO	QDE
1	**SECURITY EA3.0 CLOUD PROTECTION ADVANTAGE.** Marca: **Cisco** Modelo: E3S-SS-CPA	610
2	**SECURITY EA3.0 COMBO BREACH A & USER A PROTECTION.** Marca: **Cisco** Modelo: E3S-SS-CBPAUPA	10500
3	**SECURITY EA 3.0 UMBRELLA SECURE INTERNET GATEWAY ADVANTAGE** Marca: **Cisco** Modelo: E3S-UMB-SIGA	5000

Atestamos por fim, que a mesma demonstra capacidade técnica adequada aos serviços executados de acordo com os parâmetros técnicos de qualidade exigidos e no prazo pactuado, não existindo, em nossos registros, até a presente data, fatos que desabonem sua conduta e responsabilidade com as obrigações assumidas.

Brusque (SC), 15 de fevereiro de 2025.

DocuSigned by:
Diego Aguirre Machado
4A08FC8B35944BF...

Diego Aguirre Machado
Coordenador de Segurança