

Observer Apex

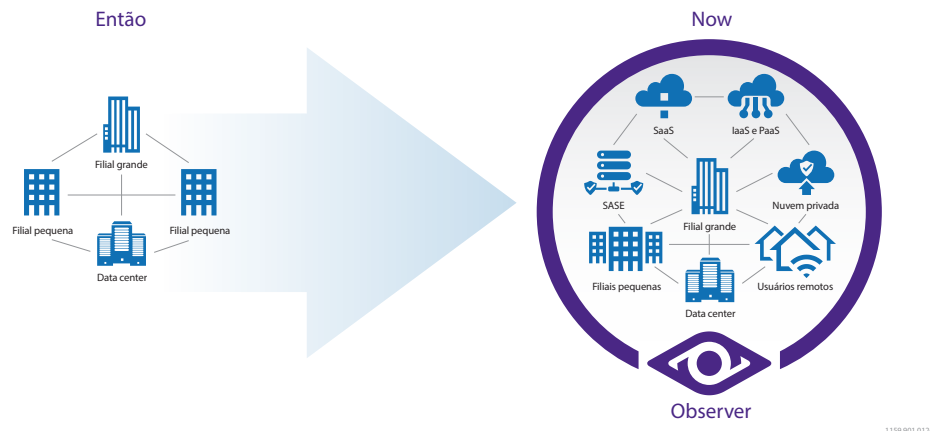
**Criado para NetSecOps: Veja mais. Resolva mais rápido.
Proporcionando visibilidade abrangente da rede e da segurança
por meio de análises avançadas.**



A REDE ESTÁ EM TODO LUGAR

Aplicações complexas de vários níveis são hospedados in loco ou em recursos baseados em nuvem; incluindo SaaS, IaaS, PaaS e SASE. Usuários que acessam aplicativos em qualquer lugar são o novo normal. A rede de hoje não conhece fronteiras, mas todos os serviços de TI ainda dependem disso.

Se qualquer componente da rede ou da arquitetura de serviço falhar, a entrega de aplicações pode se degradar rapidamente, resultando em baixa satisfação do cliente e redução da lucratividade do negócio. Para evitar isso, a observabilidade abrangente do serviço é essencial.



O Observer Apex oferece visibilidade onde você mais precisa e é a primeira solução de gestão de desempenho a gerar uma pontuação de experiência do usuário final (EUE) em cada transação. O Apex oferece adaptabilidade e visibilidade por meio de várias fontes de dados: pacotes, metadados e fluxo enriquecido. Assim, os usuários da ferramenta podem selecionar as fontes que melhor se encaixam em seus orçamentos.

O Apex fornece conscientização global sobre a integridade e o status dos serviços de TI, alinhando-se com seu compromisso de fornecendo uma visibilidade abrangente. Quando surgem anomalias de serviço ou são detectadas possíveis violações de segurança, fluxos de trabalho eficientes capacitam os grupos de NetOps, DevOps e SecOps a descobrir a causa raiz e corrigi-la rapidamente.

CENTRO DE COMANDO PARA NETSECOPS

- A pontuação EUE é automatizada e alimentada por aprendizado de máquina, convertendo vários KPIs em uma única métrica fácil de entender. Quando combinada com as deduções detalhadas de pontuação que isolam automaticamente o(s) domínio(s) do problema, fornecem as informações necessárias para priorizar uma correção rápida
- Opções flexíveis de fonte de dados, incluindo pacotes, metadados e fluxo enriquecido, oferecem a visão certa para todas as partes interessadas, desde o engenheiro de rede até a linha de proprietário do negócio
- Painéis personalizáveis para inteligência operacional global, com fluxos de trabalho eficientes, permitem rápida identificação e resolução de problemas para NetOps, SecOps e DevOps
- O mapeamento de dependências de aplicações sob demanda permite visibilidade rápida e precisa de aplicações de várias camadas, sem necessidade de configuração
- Gestão integrada de desempenho e perícia para uma resposta rápida a anomalias e violações de segurança cibernética

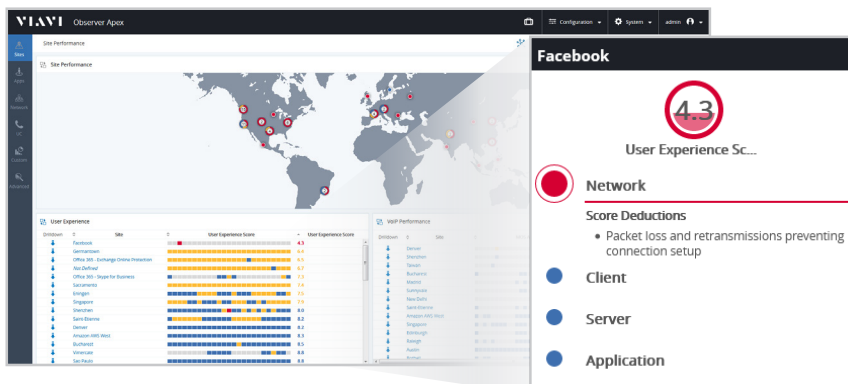
- Os recursos de inspeção profunda de pacotes (DPI) abordam o desafio de entender a composição do tráfego de rede e determinar se o tráfego não crítico está afetando negativamente os principais serviços de negócios e usuários finais
- O Observer Threat Forensics com Threat Intelligence desenvolvido pela CrowdStrike® combina informações em nível de pacote com contexto adversário incorporado para enriquecer investigações, apoiando triagem mais rápida, validação de alta confiança e visibilidade de ameaças acionáveis em ambientes híbridos
- Análise de certificado digital, identifica certificados que expiraram ou estão prestes a expirar e destaca protocolos desatualizados, ajudando a garantir a conformidade e o serviço ininterrupto para os usuários
- Fluxos de trabalho de comunicações unificadas orientam especialistas em UC de resumos globais e visualizações específicas do local a detalhes de chamadas interativas. Os pacotes e dados de fluxo são perfeitamente integrados para visualizar um único caminho de chamada ponto a ponto ou multiponto complexo por meio da infraestrutura de rede
- A ingestão e análise de registros de fluxo na nuvem proporciona a visibilidade necessária no tráfego na nuvem, auxiliando na detecção de ameaças à segurança, na identificação de anomalias e na aderência à conformidade para ambientes na nuvem, como Amazon Web Services (AWS) e Microsoft Azure
- Opções flexíveis de implantação, desde dispositivos específicos para data center até imagens de máquinas virtuais para implantações de nuvem simples e eficientes

GESTÃO DE DESEMPENHO

Pontuação da experiência do usuário final (EUE)

A Apex elimina as suposições na avaliação de satisfação do usuário com análises patenteadas alimentadas por aprendizado de máquina para analisar e avaliar com precisão todas as comunicações. Cada pontuação é classificada de 0 a 10 utilizando um código de cores e uma classificação para representar o desempenho da perspectiva do usuário, levando em conta o comportamento exclusivo do ambiente e de aplicação para eliminar falsos positivos.

As pontuações fornecem visibilidade da experiência de um único usuário ou podem ser expandidas para um site, um serviço ou uma visão empresarial global. O Apex vai um passo além, isolando o problema na rede, no cliente, no servidor ou no domínio da aplicação com descrições de problemas fáceis de entender.



8 a 10 = Bom

5,1 a 7,9 = Marginal

0 a 5 = Crítico

Painéis personalizados no nível de negócios

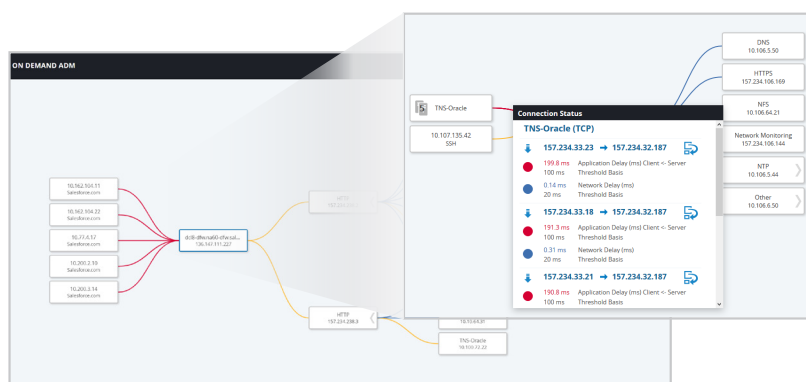
Painéis definidos pelo usuário e baseados em geolocalização permitem a conscientização situacional integrada em toda a empresa sobre a integridade da prestação de serviços.

Troubleshooting de fluxos de trabalho

Fluxos de trabalho orientados por sites e serviços integrados à pontuação da experiência do usuário final significam que as equipes de TI podem obter consciência situacional instantânea de todos os recursos em todo o mundo e, em seguida, detalhar rapidamente um usuário individual para resolução rápida de problemas.

Inteligência de aplicações multinível sob demanda

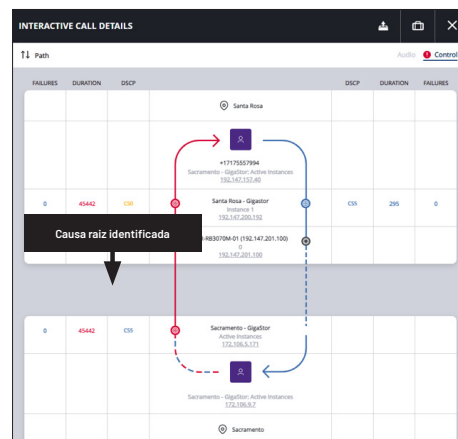
O mapeamento de dependências de aplicações sob demanda oferece reconhecimento de serviços de multicamadas, descoberta rápida de interdependências de aplicações e renderização ad hoc de mapas que visualizam esses relacionamentos complexos com clareza. Com um único clique, o Apex gera todo o mapa e automaticamente, identificando e destacando as piores conexões para que os usuários possam atribuir rapidamente a prioridade de troubleshooting.



Mapas de dependência de aplicações automatizados com pontuação da experiência do usuário final integrada

Comunicações Unificadas (UC)

Os dashboards e fluxos de trabalho do Apex UC orientam com eficiência os especialistas em VoIP e UC, desde resumos globais e vistas específicas do local até visualizações exclusivas e interativas de detalhes da chamada. Somente o Observer combina perfeitamente pacotes e dados de fluxo para visualizar o caminho de uma única chamada ponto a ponto ou multiponto complexa por meio da infraestrutura de rede, identificando as origens da degradação de qualidade e oferecendo acesso com um clique aos dados de pacote relevantes, quando necessário.



Detalhes interativos da chamada identificam as causas raízes das degradações de qualidade.

Os principais benefícios incluem:

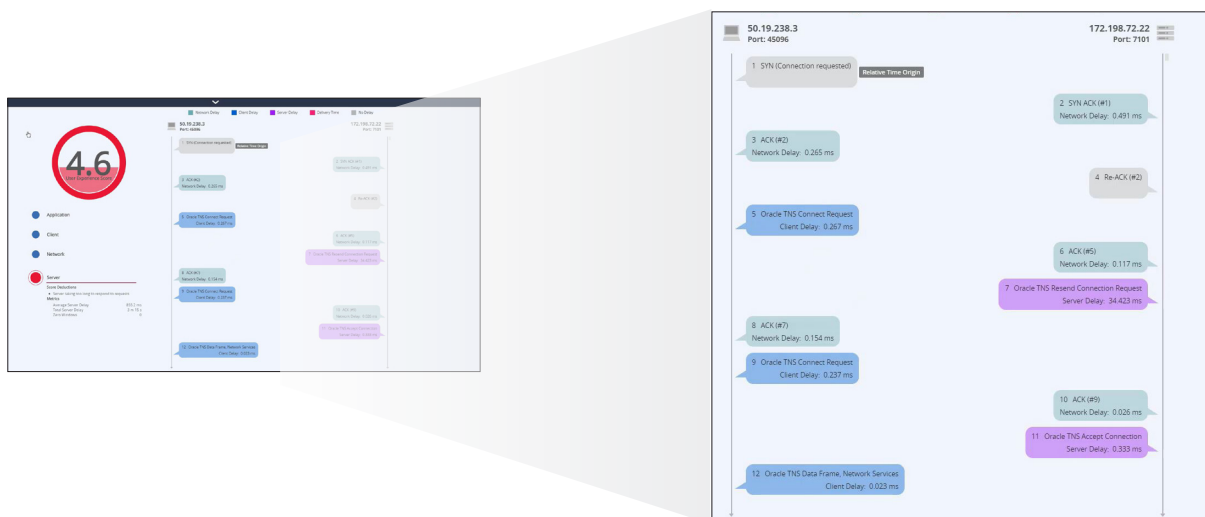
- **Mapeamento visual da jornada:** transformação de pacotes e dados de fluxo em visualizações intuitivas para o caminho das chamadas identificam as causas raízes das degradações de qualidade.
- **Resolução rápida de problemas:** reduza significativamente o MTTR com fácil identificação da causa raiz para problemas de desempenho de UC
- **Interface fácil de usar:** interface fácil de usar e entender, que permite capacitar não especialistas com representações simplificadas de chamadas complexas de UC multiponto e ponto a ponto



ANÁLISE FORENSE DE REDES E SEGURANÇA

A perícia da rede do Observer integra duas fontes de dados complementares: pacotes e fluxo enriquecido, além da capacidade de reter esses dados por longos períodos de tempo. As opções de implantação de imagem de máquina virtual permitem a coleta e a análise de pacotes e fluxos enriquecidos para aplicações hospedadas na nuvem. Chegar à causa raiz de muitos problemas de desempenho e violações de segurança cibernética começa com metadados e painéis intuitivos, mas frequentemente termina com fluxos de trabalho lógicos que levam à visibilidade dos dados subjacentes, às vezes dias após o evento. É por isso que o Observer continua apoiando os detalhes por longos períodos.

Conforme descrito acima, muitas anomalias de desempenho são rapidamente isoladas com pontuação da experiência do usuário final. No entanto, quando são necessários detalhes de maior fidelidade, os dados de suporte ficam instantaneamente disponíveis.



Pontuação da experiência do usuário final com a conexão associada ao intervalo de comunicações dinâmicas

Perícia da conversa

Com os dados do pacote capturados pelo Observer, cada transação, do início ao fim, está disponível para revisão e ações de investigação. Fluxos de trabalho eficientes orientam os usuários do painel global para pacotes individuais, sempre que necessário, em apenas algumas etapas.

Com a visibilidade adicional proporcionada pela identificação de aplicações orientadas por DPI, o Observer fornece informações avançadas sobre o tráfego de rede. Essa recurso permite que os engenheiros de rede identifiquem facilmente o tráfego em execução nas portas não padrões, quantificando o tráfego não crítico e analisando mais profundamente protocolos como HTTP e HTTPS. Os recursos de DPI do Observer permitem identificar mais de 4.300 aplicações, proporcionando clareza imediata se uma comunicação é uma transação comercial ou de outro tipo.

Perícia de fluxo enriquecido

USER	DEVICE	IP	SWITCH	ROUTER	BANDWIDTH	APPS	BANDWIDTH	HOSTS
 Mike	 2	 2	 1	 1		 10		 50
	Dell Inc.	88.151.80.178	SG200-26 (gig 6, vlan: 1)	Head Office Primary		HTTPS TCP/443		52.97.146.162
	Apple, Inc.	172.21.21.72				TCP/8013		cloudfront
						DNS TEST		13.107.42.15
						MS Web Discovery		52.114.77.34
						HTTP TCP/80		40.100.174.194
						More		More

Visualização do Observer GigaFlow IP Viewer da atividade do usuário na infraestrutura de rede para cada comunicação

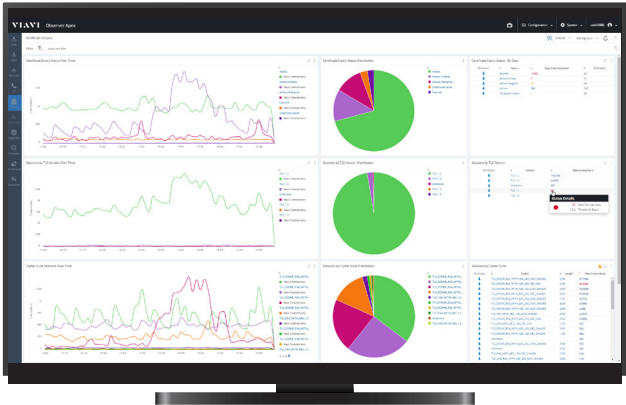
Ao compilar informações de Camada 2 a Camada 3 em um único registro de fluxo enriquecido, o Observer pode produzir visualizações interativas exclusivas que ilustram as relações entre usuário, endereço IP, endereço MAC e uso de aplicações em toda a rede. Os usuários podem simplesmente inserir um nome/ User ID de usuário ou endereço IP e encontrar imediatamente todos os dispositivos, interfaces e aplicações associados a ele. Descobrir o que está conectado e quem está se comunicando em toda a sua rede nunca foi tão fácil.



Gerenciamento de certificados digitais

O Observer monitora handshakes SSL/TLS enquanto analisa o tráfego da rede, identificando certificados digitais que expiraram ou estão prestes a expirar e fornecendo notificações proativas. Ele identifica servidores que publicam sessões inseguras, destaca protocolos desatualizados, valida a conformidade e ajuda a garantir um serviço ininterrupto para os usuários.

Para os engenheiros e administradores de rede, garantir o tempo de atividade e a satisfação do cliente é essencial para o fornecimento de serviços baseados na Web. A transição de métodos de relatórios manuais, como planilhas, para uma abordagem proativa de análise de certificados simplifica o processo, protegendo sua empresa contra possíveis interrupções relacionadas a certificados.



O painel de análise de certificados fornece a versão TLS, o status de expiração do certificado e as distribuições do Cipher Suite.

Os principais benefícios incluem:

Monitoramento proativo: análise, relatórios e notificações em tempo real mantêm você à frente da expiração do certificado

Informações de segurança aprimoradas: obtenha uma visão clara das versões SSL ou TLS em operação, permitindo a rápida desativação de protocolos desatualizados ou inseguros

Serviço ininterrupto: ao identificar e corrigir problemas relacionados a certificados, possíveis interrupções são evitadas, garantindo uma experiência perfeita ao usuário

Quando se trata de segurança cibernética, a melhor proteção contra ameaças exige uma estratégia de três etapas de prevenção, detecção e resposta.

Prevenção		Detecção	Resposta
• Firewalls • Prevenção de DDoS • Prevenção de perda de dados • Prevenção de intrusão • Antivírus e malware	• Criptografia • Anti-spam/Phishing • Controles de acesso • Segurança de endpoint	• Detecção de intrusão • Gerenciamento de eventos de segurança (SIEM) • Descoberta de endpoint	• Perícia de rede • Gerenciamento de eventos de segurança (SIEM)

Para muitas organizações, o foco frequentemente é a prevenção e detecção; até que uma violação seja confirmada e a war room comece a responder à ameaça. É neste momento que ter acesso imediato a todas as atividades da rede, incluindo o histórico, é fundamental para limitar os danos e garantir que tudo esteja bem com confiança.

É aqui que a perícia da rede é inestimável. O Observer oferece o poder combinado de tráfego com a perícia de fluxo enriquecido, permitindo que seus negócios voltem a funcionar respondendo como, quem, o que e onde de cada violação de segurança cibernética.

Perícia do tráfego



Como os dispositivos
estão ou estavam
conectados?



Quem está
ou estava se
comunicando?



O que é ou foi
transmitido?



Até onde as ações
questionáveis se estenderam?

Ao responder a essas perguntas, as equipes de TI podem determinar rapidamente o “vetor de ataque” (como o malfeitor contornou as medidas de prevenção e detecção para conseguir entrar) e quais serviços de TI, dispositivos ou dados confidenciais de clientes/negócios foram comprometidos. Assim que isso for realizado, é possível fazer a contenção e financiar avaliação de danos.



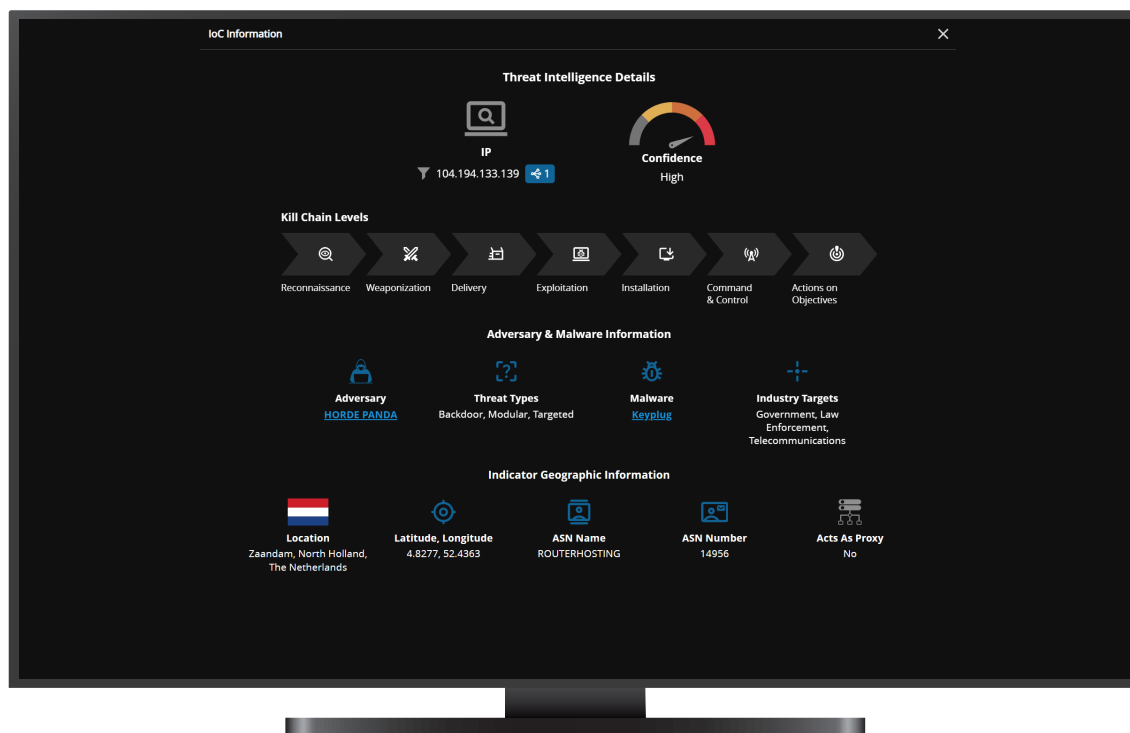
OBSERVER THREAT FORENSICS

Visibilidade de ameaças acionáveis para resposta confiável

O Observer Threat Forensics adiciona uma nova dimensão à análise forense de rede, infundindo fluxo enriquecido e evidências de camada de pacotes com inteligência de ameaças continuamente atualizada alimentada pela CrowdStrike®. Isso capacita as equipes de segurança a correlacionar o comportamento do adversário com padrões de tráfego suspeitos e degradações de desempenho, tudo em tempo real.

Ao incorporar indicadores de comprometimento (IOCs), TTPs do invasor e outros detalhes do adversário no momento da detecção, o Observer permite a validação imediata e de alta confiança de ameaças, sem emendas manuais ou enriquecimento tardio.

Seja acionado por uma ameaça conhecida ou comportamento inesperado em padrões de tráfego de rede, cada alerta inclui acesso pronto a dados de pacotes brutos e metadados de fluxo enriquecido, fornecendo aos analistas as evidências necessárias para avaliar o impacto, investigar o escopo, determinar a causa raiz e tomar medidas decisivas em ambientes híbridos.



Ao contrário das soluções tradicionais que normalmente começam no “dia um”, o Observer Threat Forensics permite uma análise retrospectiva verdadeira, tornando possível que as equipes de segurança rastreiem as ameaças até o “dia zero”. Com dados de fidelidade total retidos ao longo do tempo, os analistas podem reconstruir a linha do tempo completa do ataque, mesmo antes da detecção inicial, para descobrir a causa raiz, os pontos de entrada e o movimento lateral dentro de uma fonte de verdade.

Os principais benefícios incluem:

- **Correlação em tempo real** entre tráfego de rede e inteligência de ameaças, reduzindo o tempo médio de resolução (MTTR) ou adivinhação
- A **análise retrospectiva** fornece visibilidade do “dia zero”, fornecendo aos analistas de segurança as evidências forenses necessárias para investigar a atividade de ameaças antes da detecção inicial
- O **contexto incorporado do invasor** e os TTPs apoiam triagem e investigação confiantes
- **Links diretos para evidências de pacotes** permitem análise rápida para avaliação de escopo e impacto
- A **visibilidade compartilhada** impulsiona a colaboração entre os fluxos de trabalho NetOps e SecOps

O Observer Threat Forensics ajuda a unificar as operações de rede e segurança com uma visão compartilhada e de alta fidelidade que correlaciona o desempenho e a atividade de ameaças, aprimorando as investigações e melhorando a confiança nos fluxos de trabalho. O fluxo enriquecido integrado e os metadados fornecem a granularidade e a retenção necessárias para triagem em tempo real e análise forense pós-violação, eliminando a adivinhação e acelerando a resolução.



VISÃO GERAL DO OBSERVER

A plataforma Observer da VIAVI é uma solução abrangente de gerenciamento de desempenho e segurança que capacita as equipes de rede, operações e segurança com informações acionáveis em ambientes híbridos. O Observer Apex coleta metadados de transações de várias fontes de dados para cálculo da pontuação EUE. Ele integra detecção e investigação de ameaças em nível forense para fornecer visibilidade compartilhada e uma única fonte de verdade para equipes de NetOps e SecOps.

Como painel integrado e recurso de geração de relatórios, o Apex serve como ponto de visibilidade global central e ponto de partida para rápido troubleshooting com fluxos de trabalho otimizados que ajudam a identificar a causa raiz usando pacotes, metadados e fluxo enriquecido e aprimorado. Com contexto de ameaça incorporado e acesso direto a dados forenses, as equipes de segurança podem validar incidentes, avaliar o impacto e isolar rapidamente a causa raiz.

O Observer ajuda as equipes de TI de três maneiras essenciais:

- **Localização dos serviços** – O Observer fornece capacidade de observação em todos os ambientes de hospedagem, seja em nuvem privada, usuários remotos, nas instalações das filiais ou no data center. Não importa a localização, o VIAVI Observer tem tudo o que você precisa.
- **Fontes de dados** – O Observer oferece opções de visibilidade flexíveis usando pacotes, fluxo enriquecido e metadados. Essa abordagem multicamadas suporta o troubleshooting de desempenho e a análise forense pós-violação. Com fluxos de trabalho baseados em funções e alertas ricos em contexto, as equipes podem investigar com confiança, desde anomalias de serviço até ameaças à segurança, usando os dados certos no momento certo.
- **Escala de implantações** – Comece pequeno e dimensione conforme as demandas operacionais e de segurança evoluem. A VIAVI oferece modelos de implantação flexíveis e preços de assinatura em níveis para alinhar com suas necessidades de OpEx ou CapEx, permitindo visibilidade escalável e convergência NetSecOps sem exceder o orçamento ou os recursos.



1043.901.0124



Saiba mais em viavisolutions.com.br/apex



viavisolutions.com.br

Contato +55 11 5503 3800

Para encontrar o escritório mais perto de você, visite viavisolutions.com.br/contato

© 2025 VIAVI Solutions Inc.

As especificações e descrições do produto
neste documento estão sujeitas a mudanças
sem aviso prévio.

apex-br-ec-pt-br
30194043 914 1025