Observer Apex

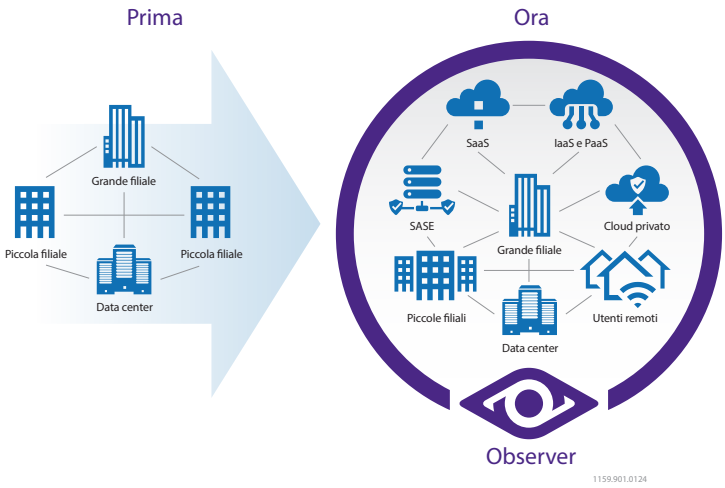
Realizzato per NetSecOps: Ulteriori informazioni. Esamina più velocemente.

Informazioni condivise sulla rete e sulla sicurezza con analisi avanzate e indagini basate sulle prove.

LA RETE È OVUNQUE

Applicazioni complesse e su più livelli, in locale o in hosting su risorse basate sul cloud, tra cui SaaS, IaaS, PaaS e SASE. L'accesso alle app da parte degli utenti, ovunque si trovino, è la nuova norma. La rete di oggi non conosce confini, eppure ogni servizio basato sull'IT dipende ancora da essa.

Se qualsiasi componente della rete o dell'architettura di servizio ha un malfunzionamento, il funzionamento delle app può deteriorarsi rapidamente e questo causa insoddisfazione del cliente e riduzione della redditività aziendale. Per evitare questa situazione, l'osservabilità completa del servizio è fondamentale.



Observer Apex offre visibilità dove ne hai più bisogno; è la prima soluzione di gestione delle prestazioni a generare il punteggio dell'esperienza dell'utente finale EUE (End-User Experience) per ogni transazione. Correlando pacchetti, metadati e flusso arricchito, Apex fornisce informazioni approfondite sulle prestazioni delle applicazioni, dei servizi e delle infrastrutture in ambienti ibridi. Le organizzazioni possono scegliere le origini dei dati più in linea con le loro esigenze operative e i loro budget, con la flessibilità necessaria per espandere la visibilità man mano che gli ambienti si evolvono.

Apex fornisce una visione globale sullo stato di salute e sulle prestazioni dei servizi IT, consentendo ai team di passare rapidamente dal rilevamento all'indagine in caso di anomalie. Avvisi integrati, analisi contestuali e flussi di lavoro delle indagini aiutano i team NetOps, DevOps e SecOps a capire rapidamente se i problemi derivano dalla rete, dall'applicazione, dal client o da un potenziale evento di sicurezza.

Combinando la conoscenza delle prestazioni con le capacità di indagine di livello forense, Apex accelera l'analisi delle cause fondamentali e consente ai team di risolvere gli incidenti operativi e di sicurezza con maggiore consapevolezza.

CENTRO DI COMANDO PER NETSECOPS

- **Il punteggio EUE automatizzato** basato sull'apprendimento automatico converte più KPI in un'unica metrica facile da interpretare, combinata con riduzioni dettagliate del punteggio che isolano automaticamente gli ambiti in cui si manifestano i problemi, fornendo le informazioni necessarie per assegnare la priorità alle soluzioni rapide
- **Observer Threat Forensics con Threat Intelligence powered by CrowdStrike®** combina informazioni a livello di pacchetto con l'intelligence sugli avversari per arricchire i flussi di lavoro di rilevamento e investigazione. Incorporando il contesto delle minacce direttamente nell'esperienza di indagine, i team possono velocizzare il triage, convalidare le minacce con alta sicurezza e ottenere visibilità operativa in ambienti ibridi.
- **Le origini dei dati flessibili,** inclusi pacchetti, metadati e flusso arricchito, offrono la visione ottimale per ogni persona coinvolta, dal tecnico di rete al titolare della linea aziendale

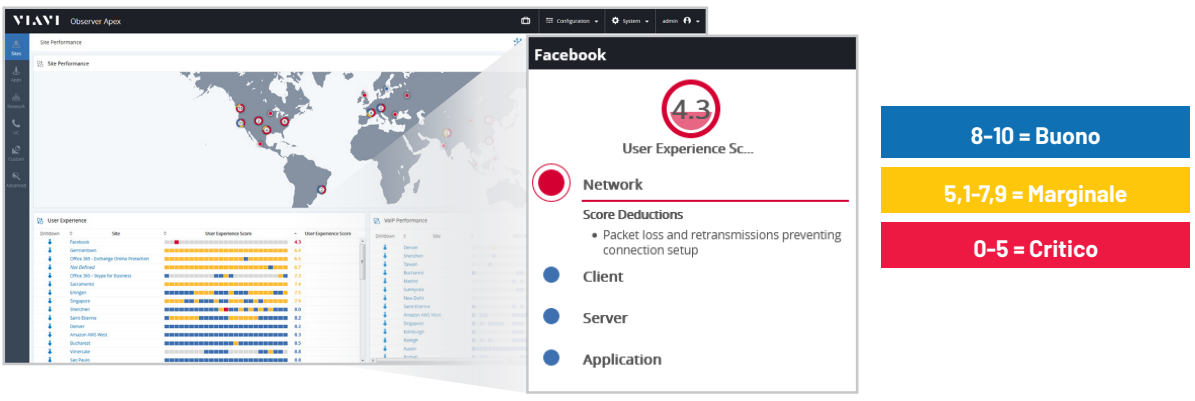
- **Le dashboard personalizzabili** per l'intelligence operativa globale con flussi di lavoro efficienti consentono di individuare e risolvere rapidamente t problemi per NetOps, SecOps e DevOps
- **La funzione On-Demand Application Dependency Mapping (OD-ADM)** consente una visibilità rapida e accurata delle applicazioni multilivello senza necessità di configurazione
- **Gestione integrata delle prestazioni e analisi forensi** per una rapida risposta alle anomalie del servizio e alle violazioni della sicurezza informatica
- **Le funzionalità di Deep Packet Inspection (DPI)** aiutano a comprendere la composizione del traffico di rete e a determinare se il traffico non critico influisce negativamente sui servizi aziendali fondamentali e sugli utenti finali
- **L'analisi dei certificati digitali** individua i certificati scaduti o in scadenza ed evidenzia i protocolli obsoleti, contribuendo a garantire la conformità e un servizio ininterrotto per gli utenti
- **I flussi di lavoro Unified Communications (UC)** aiutano gli esperti UC a passare dai riepiloghi globali e dalle viste specifiche del sito ai dettagli interattivi delle chiamate. I dati relativi ai pacchetti e ai flussi sono perfettamente integrati per visualizzare il percorso di una singola chiamata point-to-point o di una complessa multi-point nell'infrastruttura di rete
- **L'acquisizione e l'analisi dei registri dei flussi del cloud** forniscono la visibilità necessaria sul traffico del cloud, facilitando il rilevamento delle minacce per la sicurezza, l'individuazione delle anomalie e la conformità normativa per ambienti sul cloud come Amazon Web Services (AWS) e Microsoft Azure
- **Opzioni di implementazione flessibili,** dalle appliance dedicate progettate per il data center alle immagini delle macchine virtuali, per implementazioni sul cloud semplici ed efficienti

GESTIONE DELLE PRESTAZIONI

Punteggio dell'esperienza dell'utente finale

Apex elimina le congetture dalla valutazione della soddisfazione degli utenti con analisi brevettate basate sull'apprendimento automatico per analizzare e valutare accuratamente tutte le conversazioni. Ciascuna, valutazione, con un punteggio tra 0 e 10, utilizza la codifica a colori e la classificazione per rappresentare le prestazioni dal punto di vista dell'utente tenendo conto del comportamento ambientale e dell'applicazione specifica per eliminare i falsi positivi.

I punteggi offrono visibilità sull'esperienza di un singolo utente o si possono estendere a un sito, un servizio o a una vista aziendale globale. Apex compie un ulteriore passo avanti isolando il problema nella rete, nel client, nel server o nel dominio dell'applicazione con descrizioni dei problemi di facile comprensione.



Dashboard personalizzate a livello aziendale

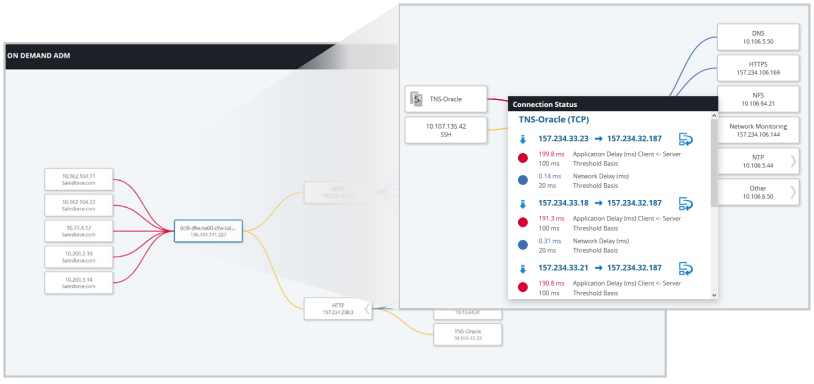
Le dashboard basate sulla geolocalizzazione e definite dall'utente consentono di comprendere la situazione in modo integrato a livello aziendale per quanto riguarda l'integrità dell'erogazione dei servizi.

Risoluzione dei problemi dei flussi di lavoro

I flussi di lavoro basati sui siti e i servizi integrati con il punteggio dell'esperienza dell'utente finale consentono ai team IT di accedere a informazioni contestualizzate istantanee a livello mondiale su tutte le risorse, per poi passare rapidamente ai dettagli del singolo utente e risolvere rapidamente i problemi.

Intelligence multilivello on-demand per le applicazioni

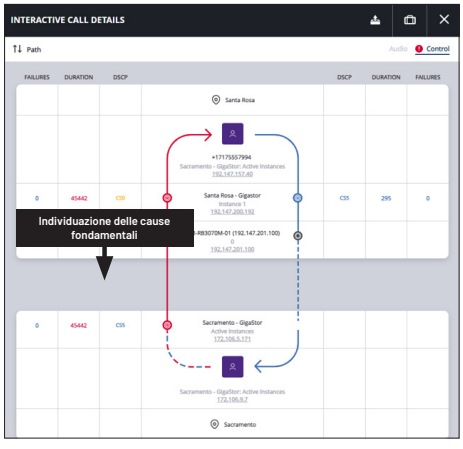
La funzione OD-ADM offre informazioni multilivello sui servizi, una rapida scoperta delle interdipendenze delle app e il rendering ad hoc delle mappe per visualizzare con chiarezza queste relazioni complesse. Con un solo clic del mouse, Apex genera l'intera mappa e individua ed evidenzia automaticamente le connessioni meno performanti affinché gli utenti possano assegnare rapidamente la priorità per la risoluzione dei problemi.



Mappe automatizzate delle dipendenze delle applicazioni con punteggio integrato dell'esperienza dell'utente finale.

Comunicazione unificata (Unified Communications, UC)

Le dashboard e i flussi di lavoro Apex UC orientano con efficienza gli esperti di VoIP e UC da riepiloghi globali e viste specifiche di un sito fino a visualizzazioni univoche e interattive dei dettagli delle chiamate. Observer combina agevolmente i dati dei pacchetti e dei flussi per visualizzare il percorso di una singola chiamata point-to-point o di una complessa chiamata multi-point attraverso l'infrastruttura di rete, individuando le origini della riduzione della qualità e offrendo accesso con un clic ai dati dei pacchetti pertinenti, quando necessario.



I dettagli interattivi delle chiamate consentono di individuare le cause fondamentali della riduzione della qualità.

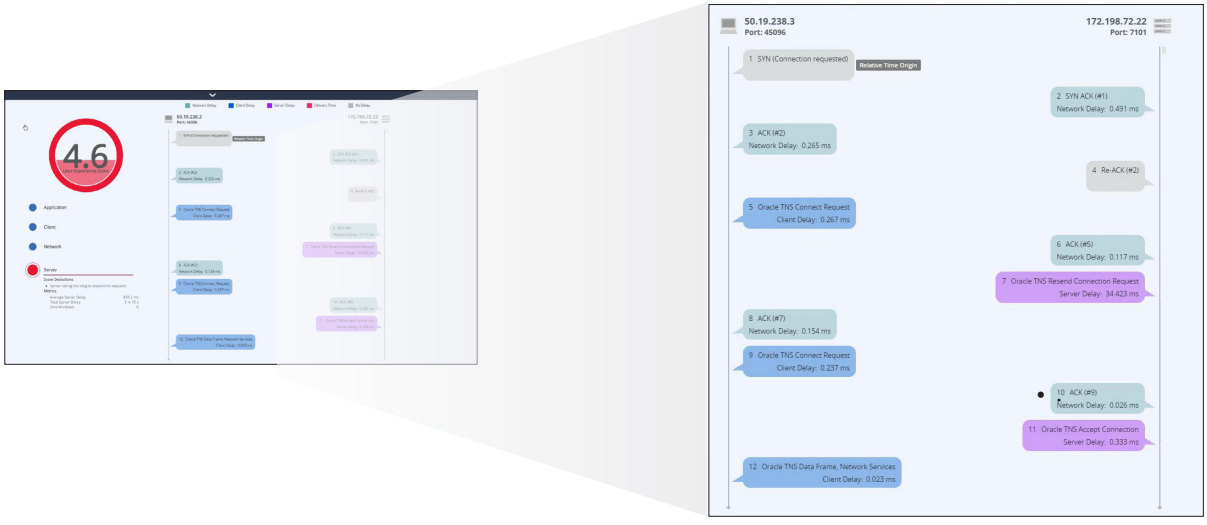
Ecco i principali vantaggi:

- **Mappatura del percorso visivo:** Trasformazione dei pacchetti e dei dati di flusso in visualizzazioni intuitive per i percorsi delle chiamate
- **Risoluzione rapida dei problemi:** Riduzione significativa dell'MTTR con una facile individuazione della cause fondamentale dei problemi relativi alle prestazioni dell'UC
- **Interfaccia intuitiva:** Interfaccia facile da usare e capire che consente anche ai meno esperti di lavorare su rappresentazioni semplificate di complesse chiamate multi-point e point-ti-point UC

ANALISI FORENSE DELLA RETE E DELLA SICUREZZA

L'analisi forense della rete resa possibile da observer integra due fonti di dati complementari: pacchetti e flusso arricchito, oltre alla possibilità di conservare questi dati per lunghi periodi. Le opzioni di implementazione delle immagini delle macchine virtuali consentono l'acquisizione e l'analisi di flussi arricchiti e pacchetti per le app in hosting nel cloud. Per arrivare alla causa fondamentale di molti problemi di prestazioni e violazioni della sicurezza informatica si inizia con metadati e dashboard intuitive, ma spesso ci si ritrova a lavorare su flussi di lavoro logici che a volte portano a vedere i dati sottostanti solo diversi giorni dopo l'evento. Ecco perché Observer continua a supportare i dettagli per periodi più lunghi.

Come accennato, molte anomalie delle prestazioni vengono rapidamente isolate con il punteggio dell'esperienza dell'utente finale. Tuttavia, quando sono necessari dettagli ad alta fedeltà, i dati di supporto sono immediatamente disponibili.



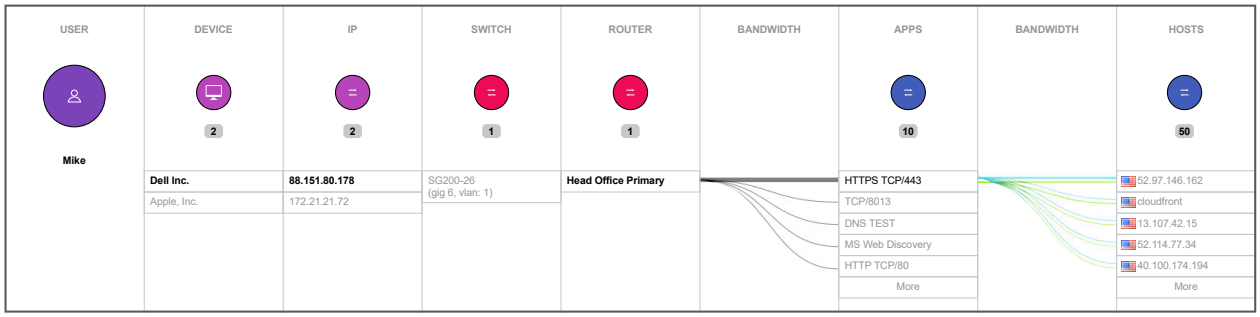
Punteggio dell'esperienza dell'utente finale con analisi dinamica dettagliata delle conversazioni sulle connessioni associate.

Conversazioni forensi

Con i dati dei pacchetti acquisiti da Observer, ogni transazione è interamente disponibile per la revisione e le azioni investigative. Flussi di lavoro efficienti orientano gli utenti dalla dashboard globale ai singoli pacchetti, quando necessario, in pochi passaggi.

Con l'ulteriore visibilità offerta dall'individuazione delle applicazioni basata su DPI, Observer rende disponibili informazioni avanzate sul traffico di rete. Questa funzionalità consente ai tenici di rete di individuare facilmente il traffico su porte non standard, quantificare il traffico non critico e approfondire protocolli come HTTP e HTTPS. Le funzionalità DPI di Observer consentono di individuare oltre 4.300 applicazioni, fornendo chiarezza a colpo d'occhio sul fatto che una conversazione sia una transazione commerciale o altro.

Analisi forense del flusso arricchito



Visualizzazione da parte di Observer GigaFlow IP Viewer dell'attività degli utenti in tutta l'infrastruttura di rete, per ogni conversazione.

Compilando approfondimenti da Layer 2 a Layer 3 in una singola registrazione del flusso arricchito, Observer può produrre visualizzazioni univoche interattive che illustrano le relazioni tra utente, indirizzo IP, indirizzo MAC e utilizzo delle applicazioni in tutta la rete. Gli utenti possono semplicemente inserire un nome/ID utente o un indirizzo IP e trovare immediatamente tutti i dispositivi, le interfacce e le applicazioni associate. Scoprire cosa è connesso e chi sta comunicando nella rete non è mai stato così facile.

Gestione dei certificati digitali

Observer monitora gli handshake SSL/TLS mentre analizza il traffico di rete, individuando i certificati scaduti o vicini alla scadenza e fornendo notifiche proattive. Individua i server che pubblicano sessioni non sicure, evidenzia i protocolli obsoleti, convalida la conformità e contribuisce a un servizio ininterrotto per gli utenti.

La dashboard di analisi dei certificati fornisce la versione TLS, la situazione relativa alla scadenza dei certificati e le implementazioni della suite di cifratura.

Per i tecnici di rete e gli amministratori, garantire il tempo di attività e la soddisfazione del cliente è essenziale, per fornire servizi basati sul Web. Il passaggio dai metodi di segnalazione manuali, come i fogli di calcolo, a un approccio proattivo di analisi dei certificati semplifica il processo, tutelando l'azienda da potenziali interruzioni correlate ai certificati.

Ecco i principali vantaggi:

- **Monitoraggio proattivo:** Le analisi, i report e le notifiche in tempo reale consentono di anticipare la scadenza del certificato
- **Informazioni sulla sicurezza migliorate:** Una visione chiara delle versioni di SSL o TLS in uso, consentendo di ritirare rapidamente i protocolli obsoleti o non sicuri
- **Servizio ininterrotto:** Individuando e risolvendo i problemi relativi ai certificati si evitano potenziali interruzioni, garantendo all'utente un'esperienza fluida

Per la sicurezza informatica, la migliore protezione contro le minacce richiede una strategia su tre fronti: prevenzione, rilevamento e risposta.

Prevenzione		Rilevamento	Risposta
• Firewall • Prevenzione dei DDoS • Prevenzione della perdita di dati • Prevenzione delle intrusioni • Antivirus e malware	• Crittografia • Anti-spam/Anti-phishing • Controlli degli accessi • Sicurezza degli endpoint	• Rilevamento delle intrusioni • Gestione degli eventi di sicurezza (Security Event Management, SIEM) • Scoperta degli endpoint	• Analisi forense della rete • Gestione degli eventi di sicurezza (Security Event Management, SIEM)

Per molte organizzazioni, spesso l'obiettivo consiste nel prevenire e nel rilevare, fino a quando viene confermata una violazione e le risorse di urgenza della sala operativa iniziano a rispondere alla minaccia. È a questo punto che l'accesso immediato a tutte le attività di rete a ritroso nel tempo è fondamentale, per limitare i danni e annunciare con sicurezza il "via libera".

Ed è qui che la rete forense è preziosissima. Observer offre la potenza combinata del traffico e di un'analisi forense del flusso arricchito per far ripartire la tua attività rispondendo al come/chi/cosa/dove di ogni violazione della sicurezza informatica.

Analisi forense del traffico

Come sono stati connessi i dispositivi?

Chi sta (o stava) comunicando?

Analisi forense del flusso arricchito

Che cosa è stato trasmesso?

Fino a che punto sono arrivate le azioni dannose?

Rispondendo a queste domande, i team IT possono determinare rapidamente il "vettore di attacco" (in che modo il malintenzionato ha eluso le misure di prevenzione e rilevamento per accedere) e quali servizi IT, dispositivi o dati sensibili di clienti/aziende sono stati compromessi. Una volta fatto questo è possibile passare al contenimento e alla valutazione del danno.

ANALISI FORENSE DELLE MINACCE (OBSERVER THREAT FORENSICS)

Visibilità operativa sulle minacce per indagini e risposte sicure

Observer Threat Forensics aggiunge una nuova dimensione alla rete forense, introducendo un flusso arricchito e prove a livello di pacchetto con informazioni sulle minacce continuamente aggiornate basate su CrowdStrike®. I team possono così correlare il comportamento degli avversari con schemi di traffico sospetti, avvisi di sicurezza e riduzione delle prestazioni in tempo reale.

Incorporando gli indicatori di compromissione (Indicators of Compromise, IOC), i TTP degli aggressori e il contesto dell'avversario direttamente nell'esperienza di indagine, Observer consente agli analisti di convalidare rapidamente le minacce senza riepiloghi manuali dei dati o arricchimenti ritardati. Gli avvisi integrati e i flussi di lavoro di indagine consentono ai team responsabili della sicurezza e della rete di iniziare il triage e l'analisi direttamente all'interno della piattaforma, riducendo i tempi di analisi e reazione.

Che si tratti si indicatori di minaccia noti o da comportamenti di rete imprevisti, ogni avviso fornisce un accesso pronto per il pivot a dati grezzi sui pacchetti, metadati e flussi arricchiti e informazioni contestuali sulle minacce. Questo consente agli analisti di valutare rapidamente l'impatto, indagare sull'estensione, determinare la cause fondamentale e rispondere in modo decisivo in tutti gli ambienti ibridi.

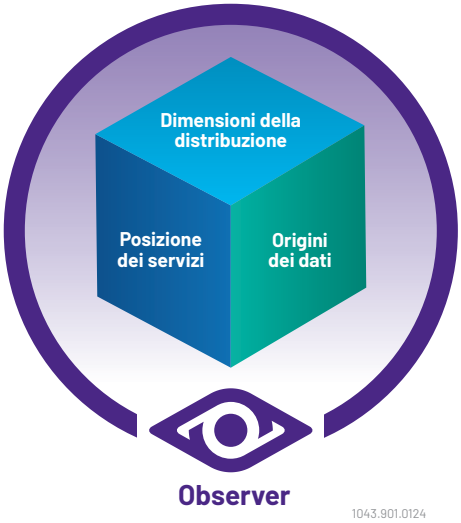
A differenza delle soluzioni tradizionali che in genere iniziano il "giorno uno", Observer Threat Forensics consente una vera analisi retrospettiva, consentendo ai team di sicurezza di tracciare le minacce fino al "giorno zero". Con i dati di rete ad alta fedeltà conservati nel tempo, gli analisti possono ricostruire la cronologia completa degli attacchi, anche prima del primo avviso, per scoprire la cause fondamentale, i punti di ingresso e il movimento laterale partendo da un'unica fonte di riferimento.

Ecco i principali vantaggi:

- **Correlazione in tempo reale** dell'attività di rete con l'intelligence dell'avversario, riducendo il tempo medio di risoluzione (MTTR) o l'incertezza
- **Analisi retrospettiva con visibilità sul giorno zero,** per scoprire l'attività delle minacce utilizzando le prove forensi necessarie prima del rilevamento iniziale
- **Contesto dell'aggressore incorporato** e TTP che supportano triage e indagini sicure
- **Passaggi diretto dagli avvisi alle prove sui pacchetti** e ai dati del flusso arricchito per una rapida valutazione dell'estensione dell'impatto
- **Visibilità condivisa** che rafforza la collaborazione tra i team NetOps e SecOps

Observer Threat Forensics aiuta a unificare le operazioni di rete e di sicurezza con una vista condivisa e ad alta fedeltà che correla prestazioni, comportamento e attività delle minacce. Combinando prove forensi di rete, metadati arricchiti e intelligence sulle minacce all'interno di una piattaforma unificata, i team hanno la chiarezza necessaria per velocizzare la risposta e risolvere gli incidenti con fiducia.

PANORAMICA DI OBSERVER

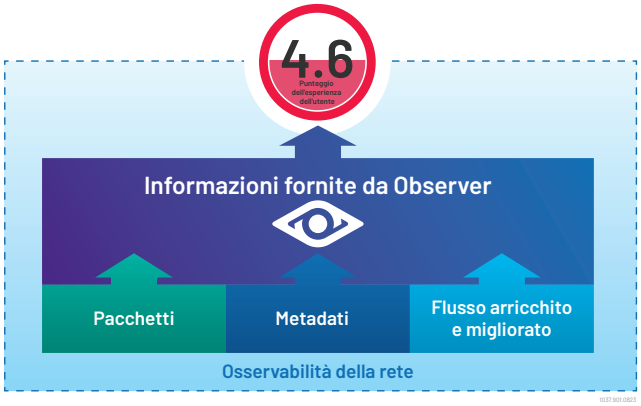


La piattaforma VIAVI Observer è una soluzione completa per la gestione delle prestazioni e della sicurezza che consente ai team di rete, operativi e di sicurezza di ottenere informazioni utili in tutti gli ambienti ibridi. Observer Apex raccoglie i metadati delle transazioni da più origini di dati per il calcolo del punteggio EUE. Integra il rilevamento e le indagini sulle minacce a livello forense per fornire visibilità condivisa e una fonte di riferimento unificata per i team NetOps e SecOps.

Come dashboard integrata e risorsa di reporting, Apex funge da punto di visibilità globale centralizzato e da base di lancio per una rapida risoluzione dei problemi con flussi di lavoro ottimizzati che aiutano a individuare la cause fondamentale utilizzando pacchetti, metadati e flusso arricchito e migliorato. Con il contesto delle minacce incorporato e l'accesso diretto ai dati forensi, i team di sicurezza possono convalidare gli incidenti, valutare l'impatto e isolare rapidamente la cause fondamentale.

Observer aiuta i team IT in tre modi essenziali:

- **Posizione dei servizi**: Observer offre visibilità in ogni ambiente di hosting, che si tratti di cloud privati, utenti remoti, filiali o data center. Indipendentemente dalla posizione, VIAVI Observer a sempre a disposizione.
- **Origini dei dati**: Observer offre opzioni di visibilità flessibili utilizzando pacchetti, flusso arricchito e metadati. Questo approccio multilivello supporta la risoluzione dei problemi relativi alle prestazioni e le analisi forensi post-violazione. Con flussi di lavoro basati sui ruoli e avvisi corredati di contesto, i team possono indagare con sicurezza su più livelli: dalle anomalie del servizio alle minacce alla sicurezza, utilizzando i dati ottimali al momento giusto.
- **Scalabilità delle implementazioni**: inizia in piccolo ed espanditi via via che le esigenze operative e di sicurezza aumentano. VIAVI propone modelli di implementazione flessibili e prezzi degli abbonamenti su più livelli, per allinearsi alle esigenze di OpEx o CapEx, consentendo una visibilità scalabile e la convergenza delle NetSecOps senza sovraccarichi a livello di budget o risorse.



Ulteriori informazioni all'indirizzo
viavisolutions.com/apex

viavisolutions.com

Contattateci +1 844 GO VIAVI | (+1 844 468 4284)
Per contattare l'ufficio VIAVI più vicino, visitare viavisolutions.com/contacts

apex-br-ec-it
30176200 915 0326