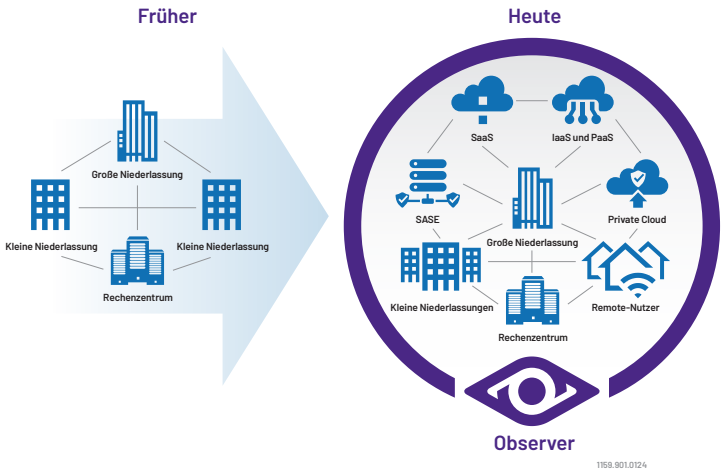
Observer Apex

Entwickelt für NetSecOps: Bessere Sichtbarkeit. Schnellere Untersuchungen.

Vermittlung geteilter Einblicke in Netzwerk und Sicherheit mit erweiterter Analyse und beweisbasierter Untersuchung.

DAS NETZWERK IST ÜBERALL

Komplexe mehrschichtige Anwendungen werden auf lokalen oder cloudbasierten Ressourcen, beispielsweise als SaaS, IaaS, PaaS und SASE, gehostet. Heute ist es selbstverständlich, dass die Nutzer von jedem Standort aus auf diese Anwendungen zugreifen können. Die modernen Netzwerke sind praktisch grenzenlos. Und doch sind alle IT-Dienste von ihnen abhängig.



Fällt eine Komponente des Netzwerkes oder der Dienste-Architektur aus, kann die Bereitstellung von Anwendungen beeinträchtigt werden, sodass die Kundenzufriedenheit und die Rentabilität des Unternehmens sinken. Um dieses Szenario zu verhindern, ist eine lückenlose Beobachtbarkeit der Dienste unverzichtbar.

Observer Apex gewährleistet die Sichtbarkeit dort, wo sie am dringendsten benötigt wird, und ist die erste Leistungsmanagement-Lösung, die für jede Transaktion eine Bewertung des Endnutzer-Erlebnisses (End-User Experience, EUE) ausgibt. Durch die Korrelation von Datenpaketen, Metadaten und Enriched-Flow-Datensätzen vermittelt Apex tiefgehende Einblicke in die Leistung von Anwendungen und Diensten sowie in die Infrastruktur von hybriden Umgebungen. Dabei können Unternehmen die Datenquellen auswählen, die am besten für ihre betrieblichen Anforderungen und ihr Budget geeignet sind, und bei sich weiter entwickelnden Umgebungen gleichzeitig die Sichtbarkeit flexibel erweitern.

Apex stellt einen globalen Überblick über den Status und die Leistung der IT-Systeme zur Verfügung und versetzt die Teams darüber hinaus in die Lage, beim Auftreten von Anomalien umgehend von der Erkennung zur Untersuchung überzugehen. Integrierte Alarme, kontextbasierte Analysen und Untersuchungsabläufe helfen den Teams bei NetOps, DevOps und SecOps, in kürzester Zeit zu ermitteln, ob die Störung durch das Netzwerk, die Anwendung oder den Client verursacht wurde oder ob es sich möglicherweise um eine Sicherheitsverletzung handelt.

Durch die Kombination der Leistungseinblicke mit den forensischen Untersuchungsfunktionen beschleunigt Apex die Fehleranalyse und befähigt die Teams, sowohl betriebliche als auch sicherheitsrelevante Zwischenfälle mit größerer Sicherheit zu beheben.

LEITSTELLE FÜR NETSECOPS

- **Das ML-basierte automatische EUE-Scoring** wandelt mehrere kritische Leistungsindikatoren (KPI) in einen einzigen, auf einen Blick verständlichen Kennwert um. Eine detaillierte Aufschlüsselung sorgt dafür, dass die problematischen Netzbereiche automatisch eingegrenzt werden und alle Informationen vorhanden sind, um eine schnellstmögliche Behebung der Störung nach Dringlichkeit vorzunehmen.
- **Observer Threat Forensics mit Bedrohungsanalyse auf Grundlage von CrowdStrike®** kombiniert die auf Paketebene gewonnenen Einblicke mit Angreifer-Kontext, um die Erkennung und Untersuchungsabläufe zu verbessern. Durch die direkte Einbettung des Bedrohungskontexts in das Untersuchungserlebnis können die Teams die Triage beschleunigen, Bedrohungen mit großer Sicherheit validieren und eine aussagekräftige Sichtbarkeit in hybriden Umgebungen gewinnen.
- **Flexible optionale Datenquellen,** wie Paket-, Meta- und Enriched-Flow-Daten, stellen jedem berechtigten Nutzer, angefangen beim Netzwerktechniker bis zum Manager, stets die benötigten relevanten Daten bereit.

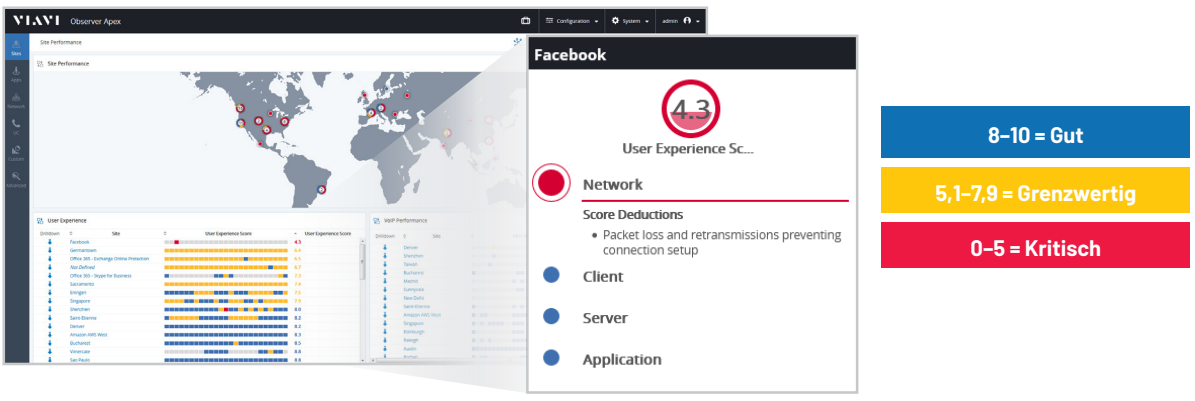
- **Kundenspezifisch anpassbare Dashboard-Ansichten** zur Vermittlung globaler Einblicke in Betriebsabläufe mit effizienten Workflows ermöglichen den NetOp-, SecOp- und DevOp-Teams, auftretende Probleme schnellstmöglich zu identifizieren und zu beheben.
- **Die Darstellung der Abhängigkeiten auf Anforderung (OD-ADM)** sorgt auf mehreren Ebenen und ohne vorherige Konfiguration für eine schnelle und präzise Anwendungstransparenz.
- **Integriertes Leistungsmanagement und Forensik** zum schnellen Reagieren auf Dienststörungen und Cyber-Sicherheitsvorfälle.
- **Tiefgehende Paketprüfungen (DPI)** helfen, den Aufbau des Verkehrsflusses im Netzwerk besser zu verstehen sowie zu ermitteln, ob nicht-kritischer Verkehr wichtige Unternehmensdienste und Endnutzer beeinträchtigt.
- **Die Analyse digitaler Zertifikate** erkennt abgelaufene/demnächst ablaufende Zertifikate und zeigt veraltete Protokolle an. Damit trägt sie dazu bei, sowohl die Konformität als auch eine unterbrechungsfreie Bereitstellung der Dienste an die Nutzer sicherzustellen.
- **UC-Workflows** leiten Unified-Communications-Experten ausgehend von globalen Zusammenfassungen und standortspezifischen Ansichten zu interaktiven Verbindungsdaten. Paket- und Flow-Daten werden nahtlos integriert, um den Pfad einer einzelnen Punkt-zu-Punkt- oder komplexen Mehrpunkt-Verbindung durch die Infrastruktur des Netzes grafisch anzuzeigen.
- **Log-Ingest im Cloud-Flow** sowie Analysen stellen die benötigte Sichtbarkeit in den Cloud-Verkehr zur Verfügung und unterstützen die Bedrohungserkennung, die Identifikation von Anomalien sowie die Konformität in Cloud-Umgebungen, wie Amazon Web Services (AWS) und Microsoft Azure.
- **Flexible Bereitstellungsoptionen,** angefangen bei spezifischen Geräten für Rechenzentren bis zu virtuellen Maschinen für die einfache und effiziente Einbindung in die Cloud.

LEISTUNGSMANAGEMENT

Endnutzer-Scoring

Mit seiner patentierten Analyse auf Grundlage von maschinellem Lernen (ML) zum präzisen Analysieren und Bewerten aller Konversationsparameter erlaubt Apex, die Zufriedenheit des Endnutzers objektiv einzuschätzen. Jede Konversation wird mit 0 bis 10 Punkten bewertet sowie mit einem farbcodierten Ergebnis versehen, um die Leistung aus Sicht des Nutzers darzustellen. Dabei wird das Verhalten der Umgebung und der Anwendungen berücksichtigt, um falsch positive Ergebnisse zu vermeiden.

Die angegebene Punktezahl (Score) gewährleistet die Sichtbarkeit ins Nutzererlebnis, kann aber auch auf den Standort, auf einen Dienst oder auf eine Ansicht für das ganze Unternehmen erweitert werden. Apex geht sogar noch einen Schritt weiter und grenzt die Störung mit aussagekräftigen Problembeschreibungen auf das Netzwerk, den Client, den Server oder die Anwendung ein.



Anpassbare Dashboards auf Geschäftsebene

Geolokalisierte, anwenderdefinierte Dashboard-Ansichten vermitteln unternehmensweite, zusammenfassende und situative Einblicke in den Bereitstellungsstatus von Diensten.

Fehlerdiagnose-Workflows

Standort- und Dienste-basierte Workflows, die mit dem Endnutzer-Scoring kombiniert werden, sorgen dafür, dass die IT-Teams sofortige weltweite und situative Einblicke in alle Ressourcen erhalten. Dadurch können sie umgehend eine detailliertere Analyse bis auf den einzelnen Nutzer hinunter durchführen, um das Problem sofort zu beheben.

Mehrschichtige Anwendungsintelligenz auf Anforderung

Die anforderungsbasierte ADM-Funktion (OD-ADM) berücksichtigt mehrere Dienste-Schichten, erkennt in kürzester Zeit Abhängigkeiten zwischen Anwendungen und erzeugt Diagramme, die diese komplexen Beziehungen übersichtlich darstellen. Mit einem einzigen Mausklick erstellt Apex eine aussagekräftige Komplettübersicht und zeigt automatisch die schlechtesten Nutzer-Verbindungen an, sodass umgehend die Dringlichkeit der Fehlerbehebung eingeschätzt werden kann.

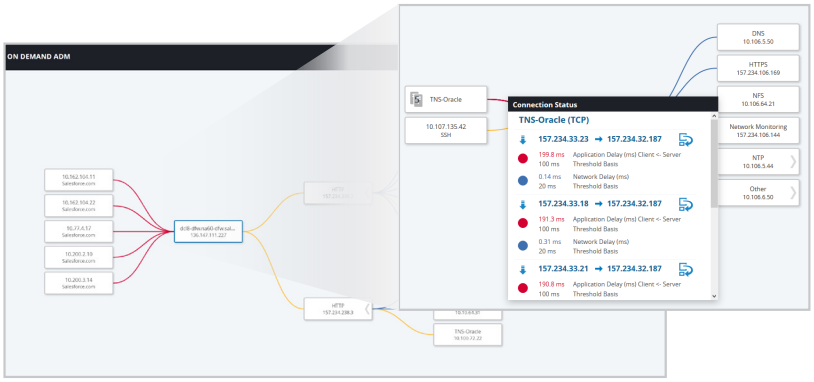
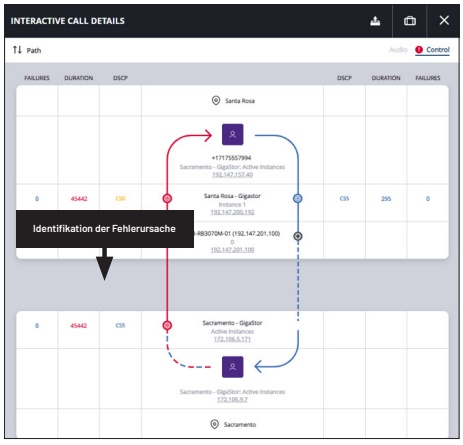


Diagramme mit automatischer Anzeige der Abhängigkeiten zwischen Anwendungen (ADM) und integriertem Endnutzer-Scoring (EUE)

Unified Communications (UC)

Die UC-Dashboards und -Workflows von Apex leiten den VoIP- und UC-Experten von globalen Zusammenfassungen und standortspezifischen Ansichten zu einer beispiellosen und interaktiven Anzeige der Verbindungsdaten. Einzig Observer kombiniert die Paket- und Flow-Daten nahtlos miteinander, um den Pfad eines einzelnen Punkt-zu-Punkt- oder komplexen Mehrpunkt-Anrufs durch die Infrastruktur des Netzwerks anzuzeigen. Damit werden die Ursprünge von Qualitätsmängeln lokalisiert, während der Techniker zudem bei Bedarf auf einen Klick Zugang zu relevanten Paketdaten erhält.



Interaktive Verbindungsdaten erlauben, die Ursache für Qualitätsmängel zu identifizieren.

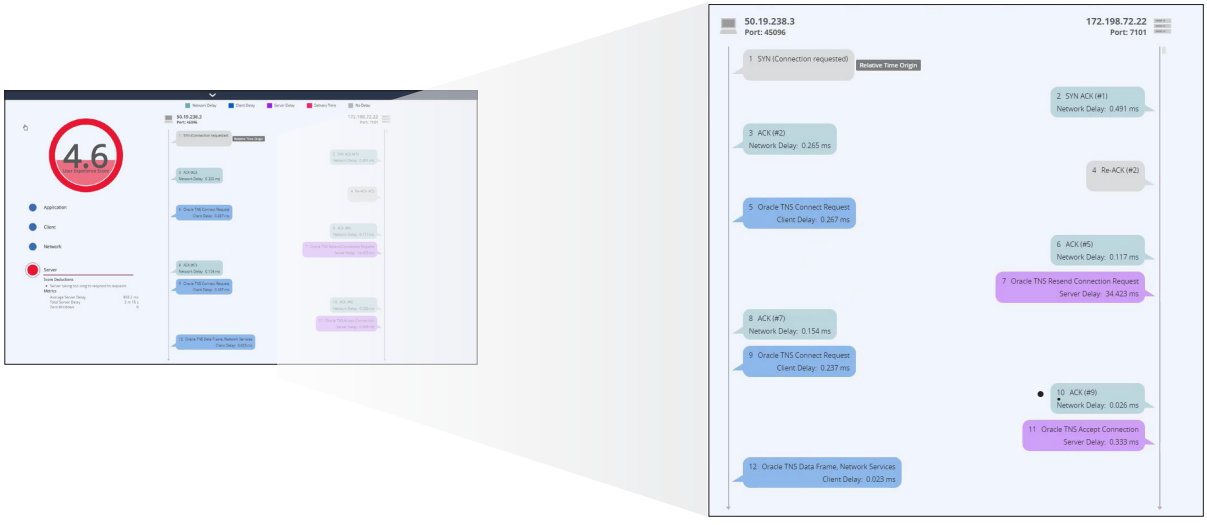
Profitieren auch Sie von diesen Vorteilen:

- **Grafische Darstellung des Verbindungspfads:** Umwandlung von Paket- und Flow-Daten in eine intuitive grafische Darstellung der Call Journey.
- **Umgehende Problemlösung:** Deutlich schnellere Fehlerbehebung/Reparatur mit müheloser Identifikation der tatsächlichen Fehlerursache bei UC-Leistungsstörungen.
- **Bedienerfreundliche Benutzeroberfläche:** Durch die einfach zu bedienende und verständliche Benutzeroberfläche können auch weniger qualifizierte Mitarbeiter anhand der vereinfachten Beschreibungen komplexer Punkt-zu-Punkt- und Mehrpunkt-Verbindungen zuverlässige Analysen ausführen.

NETZWERK- UND SICHERHEITSFORENSIK

Die Netzwerk-Forensik von Observer integriert zwei sich gegenseitig ergänzende Datenquellen, d. h. Pakete und Enriched-Flow-Daten, und ist in der Lage, diese Daten für längere Zeiträume zu archivieren. Mit der als Option angebotenen Image-Bereitstellung virtueller Maschinen (VM) ist es möglich, Enriched-Flow-Daten und Pakete für cloudhosted Apps zu erfassen und zu analysieren. Die Ermittlung der eigentlichen Ursache vieler Leistungsstörungen und von Cybersicherheit-Verletzungen beginnt mit den Metadaten sowie intuitiven Dashboards und endet häufig mit logischen Workflows, die, manchmal erst Tage nach dem eigentlichen Ereignis, die Sichtbarkeit der zugrunde liegenden Daten ermöglichen. Daher archiviert Observer die unterstützenden Daten über längere Zeiträume.

Wie oben beschrieben, werden zahlreiche Leistungsstörungen umgehend mit dem bewerteten Endnutzererlebnis isoliert. Sollten aber noch präzisere, ergänzende Details benötigt werden, stehen diese sofort zur Verfügung.



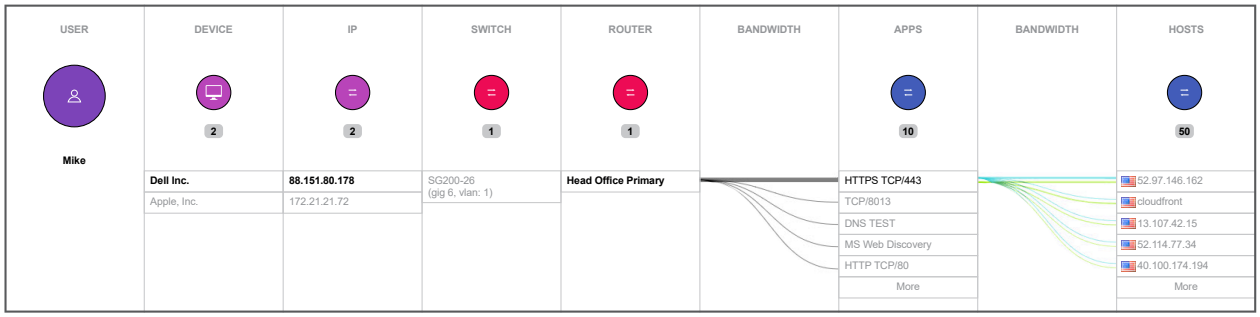
Endnutzer-Scoring mit dazugehöriger Aufschlüsselung der Verbindungsdynamik der Konversation

Konversationsforensik

Da Observer die Paketdaten aufzeichnet, steht die gesamte Konversation jeder Transaktion von Anfang bis Ende zur Überprüfung sowie für die genauere Untersuchung zur Verfügung. Effiziente Workflows leiten den Nutzer bei Bedarf in wenigen Schritten von globalen Dashboard-Ansichten bis hinunter zu den einzelnen Datenpaketen.

Die zusätzliche Sichtbarkeit, die durch die DPI-basierte Anwendungsidentifikation gewährleistet wird, erlaubt Observer, erweiterte Einblicke in den Netzverkehr zur Verfügung zu stellen. Dieses Leistungsmerkmal versetzt die Netzwerktechniker in die Lage, Verkehr, der über Nicht-Standard-Ports läuft, mühelos zu identifizieren, nicht-kritischen Verkehr zu quantifizieren und sich Protokolle, wie HTTP und HTTPS, genauer anzusehen. Die leistungsstarke DPI-Funktion von Observer ermöglicht Ihnen, mehr als 4300 Anwendungen zu identifizieren und zeigt auf einen Blick an, ob es sich bei der Konversation um eine Geschäftstransaktion handelt.

Enriched-Flow-Forensik



Observer GigaFlow IP Viewer zeigt die Aktivität der Nutzer für jede Konversation über die gesamte Netzwerk-Infrastruktur hinweg an

Da Observer die auf den Layern 2 und 3 gesammelten Informationen zu einem einzigen Enriched-Flow-Datensatz zusammenfasst, können beispiellose interaktive Visualisierungen erstellt werden, die die Beziehung zwischen Nutzer, IP-Adresse, MAC-Adresse und Anwendungsnutzung im gesamten Netzwerk verdeutlichen. Die Anwender geben einfach Namen/Nutzer-ID oder IP-Adresse ein und erhalten sofort alle Geräte, Schnittstellen und Anwendungen, die mit dieser Kennung in Verbindung stehen, angezeigt. Nie war es einfacher herauszufinden, welche Geräte angeschlossen sind und wer im Netzwerk kommuniziert.

Management digitaler Zertifikate

Im Rahmen der Analyse des Netzwerkverkehrs überwacht Observer auch SSL/TLS-Handshakes, identifiziert abgelaufene oder demnächst ablaufende digitale Zertifikate und gibt entsprechende Meldungen proaktiv aus. Die Lösung erkennt Server, die unsichere Sitzungen veröffentlichen, zeigt veraltete Protokolle an, prüft die Konformität und hilft, die unterbrechungsfreie Bereitstellung der Dienste an die Nutzer zu gewährleisten.

Der Dashboard-Bildschirm zur Zertifikatsanalyse informiert über die TLS-Version, über den Gültigkeitsstatus des Zertifikats und über Cipher-Suite-Verteilungen.

Bei der Bereitstellung webbasierter Dienste müssen die Netzwerkingenieure und Administratoren unbedingt die Verfügbarkeit und Kundenzufriedenheit sicherstellen. Der Übergang von manuellen Berichtsmethoden, wie mit Arbeitsblättern, zu einer proaktiven Zertifikatanalyse vereinfacht den Prozess und schützt Ihr Unternehmen vor potenziellen zertifikatbedingten Ausfällen.

Profitieren auch Sie von diesen Vorteilen:

- **Proaktive Überwachung:** Die in Echtzeit erfolgte Analyse, Berichterstellung und Benachrichtigung sorgt dafür, dass Sie rechtzeitig über den Ablauf von Zertifikaten informiert sind.
- **Erweiterte Sicherheitseinblicke:** Genauer Überblick über die verwendeten SSL/TLS-Versionen, sodass veraltete oder unsichere Protokolle umgehend ersetzt werden können.
- **Unterbrechungsfreie Dienste:** Die Identifikation und Behebung von Problemen mit digitalen Zertifikaten ermöglicht Ihnen, potenzielle Ausfälle zu vermeiden und ein einwandfreies Nutzererlebnis sicherzustellen.

Wenn es um die Cybersicherheit geht, bietet die dreiteilige Strategie aus Vorbeugen, Erkennen und Reagieren den besten Schutz.

Verbeugen		Erkennen	Reagieren
• Firewall • DDoS-Verhinderung • Datenverlust-Verhinderung • Angriffsverhinderung • Antivirus und Malware	• Verschlüsselung • Anti-Spam/Phishing • Zugangskontrolle • Endpunkt-Sicherheit	• Angriffserkennung • Management sicherheitsrelevanter Vorfälle (SIEM) • Endpunkt-Erkennung	• Netzwerk-Forensik • Management sicherheitsrelevanter Vorfälle (SIEM)

Viele Unternehmen legen häufig den Schwerpunkt nur auf Vorbeugen und Erkennen, bis dann eine Sicherheitsverletzung bestätigt wird und das Notfallszenario beginnt, auf die Bedrohung zu reagieren. Um aber den Schaden begrenzen und zuversichtlich eine umfassende Entwarnung geben zu können, muss man bereits an diesem Punkt Zugriff auf alle vergangenen Netzwerkaktivitäten haben.

Hier zeigt die Netzwerk-Forensik ihren wahren Wert. Observer kombiniert die Leistung der forensischen Untersuchung des Netzwerkverkehrs und der Enriched-Flow-Daten, um den Normalbetrieb im Unternehmen wiederherzustellen. Dazu beantwortet das System für jeden Cybersicherheitsvorfall die Fragen nach dem Wie, Wer, Was und Wo.

Verkehrsforensik

Wie sind oder waren die Geräte verbunden?

Wer (hat) kommuniziert?

Enriched-Flow-Forensik

Was wird oder wurde übertragen?

Wie weit haben sich die verdächtigen Aktivitäten erstreckt?

Die Antworten auf diese Fragen erlauben den IT-Teams, den „Angriffsvektor", also den Weg zu bestimmen, auf dem der Angreifer die Vorbeugungs- und Erkennungsmaßnahmen umgangen hat, sowie zu ermitteln, welche IT-Dienste, Geräte oder sensible Kunden-/Geschäftsdaten kompromittiert wurden. Auf dieser Grundlage ist es dann möglich, eine Eindämmung vorzunehmen und den Schaden endgültig einzuschätzen.

OBSERVER THREAT FORENSICS

Aussagekräftige Sichtbarkeit der Bedrohung für zuverlässige Untersuchungen und Gegenmaßnahmen

Observer Threat Forensics erweitert die Netzwerk-Forensik um eine neue Dimension, da dieses Leistungsmerkmal den Enriched Flow und die auf der Paketschicht ermittelten Beweise durch kontinuierlich aktualisierte Threat Intelligence Daten auf Grundlage von CrowdStrike® ergänzt. Dadurch sind die Sicherheitsteams in der Lage, das Verhalten des Angreifers – in Echtzeit – mit verdächtigen Verkehrsmustern, Sicherheitsalarmen und Leistungsmängeln abzugleichen.

Durch direkte Einbettung von Kompromittierungsindikatoren (Indicators of Compromise, IOC), von Techniken, Taktiken und Vorgehensweisen (TTP) des Angreifers sowie von Angreifer-Kontext in das Untersuchungserlebnis versetzt Observer die Analysten in die Lage, Bedrohungen schnell und ohne manuelle Datenzusammenfassung oder verzögerte Anreicherung zu validieren. Integrierte Alarme und Untersuchungsabläufe erlauben den Sicherheits- und Netzwerk-Teams, noch direkt auf der Plattform mit der Triage und der Analyse zu beginnen und die Zeit vom Verstehen bis zur Maßnahme zu verkürzen.

Unabhängig davon, ob der Alarm von bekannten Bedrohungsindikatoren oder durch ein überraschendes Verhalten des Netzwerks ausgelöst wurde, stellt er in jedem Fall den flexiblen Zugriff auf die Roh-Paketdaten, die Enriched-Flow-Metadaten und die kontextbasierten Bedrohungsdaten zur Verfügung. Damit erhalten die Analysten die Beweise, die sie benötigen, um die Auswirkungen zu bewerten, den Umfang zu untersuchen, die tatsächliche Ursache zu bestimmen und in hybriden Umgebungen entscheidende Maßnahmen zu ergreifen.

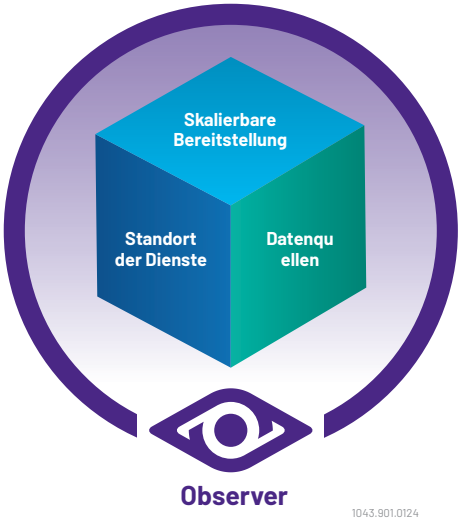
Im Unterschied zu traditionellen Lösungen, die für gewöhnlich erst beim Day One einsetzen, ermöglicht Observer Threat Forensics eine echte retrospektive Analyse, die es den Sicherheitsteams erlaubt, die Bedrohung bis zum Day Zero zurückzuverfolgen. Mit Hilfe der im Zeitverlauf gespeicherten präzisen Netzwerkdaten können die Analysten die gesamte Zeitlinie, sogar noch vor dem ersten Alarm, rekonstruieren, um die eigentliche Ursache, die Einstiegspunkte sowie seitliche Bewegungen auf Grundlage einer einzigen Datenquelle zu ermitteln.

Profitieren auch Sie von diesen Vorteilen:

- **Echtzeit-Korrelation** der Netzwerkaktivität mit Daten zum Angreifer, um die Zeit bis zur Problemlösung (MTTR) bzw. der Ungewissheit zu verkürzen.
- **Retrospektive Analysen** mit Day-Zero-Sichtbarkeit, um die Bedrohungsaktivität mit Hilfe forensischer Beweise vor der Ersterkennung zu untersuchen.
- **Eingebetteter Angreifer-Kontext** und TTPs, die eine zuverlässige Triage und Untersuchung unterstützen.
- **Direkter Übergang von Alarmen zu paketbasierten Beweisen** und zu Enriched-Flow-Daten für die umgehende Bewertung des Umfangs und der Auswirkungen.
- **Geteilte Sichtbarkeit,** die die Zusammenarbeit zwischen den Teams von NetOps und SecOps stärkt.

Observer Threat Forensics hilft, die Abläufe zur Sicherung der Leistung und Sicherheit im Netzwerk in eine präzise geteilte Ansicht zusammenzuführen, die die Leistung, das Verhalten und die Bedrohungsaktivität korreliert. Durch die Kombination der forensischen Beweise im Netzwerk, der Enriched-Metadaten und der Bedrohungsdaten auf einer zentralen Plattform profitieren die Teams von dem aussagekräftigen Überblick, den sie benötigen, um die Reaktionsgeschwindigkeit zu erhöhen und Zwischenfälle zuversichtlich zu beheben.

OBSERVER AUF EINEN BLICK

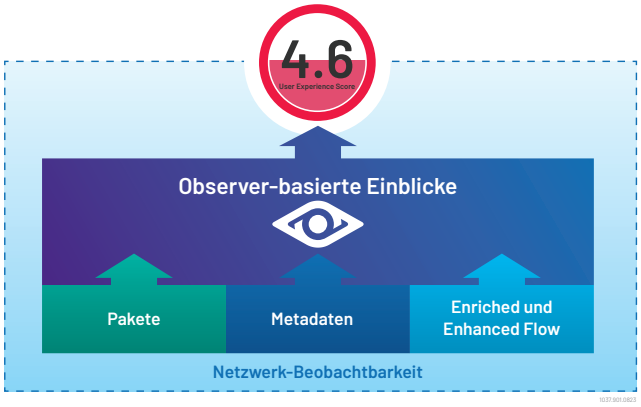


Die Observer-Plattform von VIAVI ist eine umfassende Lösung für das Leistungs- und Sicherheitsmanagement, die den NetOps- und SecOps-Teams aussagekräftige Einblicke in hybride Umgebungen vermittelt. Observer Apex erfasst die Metadaten der Transaktionen von mehreren Datenquellen, um den EUE-Score zu berechnen. Dieses Tool integriert die Erkennung und Untersuchung von Bedrohungen auf forensischer Ebene, um eine geteilte Sichtbarkeit zu ermöglichen und den NetOps- und SecOps-Teams eine zentrale Datenquelle als Single Source of Truth (SSOT) zur Verfügung zu stellen.

Als integrierte Ressource für Dashboard-Ansichten und zur Berichterstellung ist Apex die zentrale globale Anlaufstelle zur Gewährleistung der Sichtbarkeit. Weiterhin dient Apex als Ausgangspunkt für die zügige Fehlerdiagnose mit optimierten Workflows, die mit Paketen und Metadaten sowie mit angereicherten („Enriched") und erweiterten („Enhanced") Datenflüssen helfen, die Ursache von Störungen zu ermitteln. Mit dem eingebettetem Angreifer-Kontext und dem direkten Zugriff auf forensische Daten können die Sicherheitsteams die Vorfälle validieren, deren Auswirkungen bewerten und die tatsächliche Fehlerursache umgehend eingrenzen.

Observer unterstützt die IT-Teams in dreierlei Hinsicht:

- **Standort der Dienste:** Observer gewährleistet die Beobachtbarkeit aller Hosting-Umgebungen, wie von privaten Clouds, Remote-Nutzern, vor Ort in Niederlassungen oder im Rechenzentrum. VIAVI Observer erfasst alle Dienste, unabhängig vom Standort.
- **Datenquellen:** Observer bietet flexible Sichtbarkeitsoptionen mit Paketen, Enriched-Flow-Daten und Metadaten. Dieses mehrschichtige Konzept unterstützt sowohl die Fehlerdiagnose bei Leistungsstörungen als auch die forensische Untersuchung nach dem Sicherheitsvorfall. Mit den rollenbasierten Workflows und den kontextreichen Warnmeldungen können die Teams alle Auffälligkeiten, angefangen bei Dienstanomalien bis zu Sicherheitsbedrohungen, mit den richtigen Daten zur richtigen Zeit zuverlässig untersuchen.



- **Skalierbare Bereitstellungen:** Sie können klein anfangen und dann, wenn die Anforderungen des Netzbetriebs und der Sicherheit dies erfordern, jederzeit skalieren. VIAVI bietet flexible Bereitstellungsmodelle und gestaffelte, an Ihre geplanten Betriebs- und Investitionskosten anpassbare Abo-Preismodelle. Damit sind eine skalierbare Sichtbarkeit und die NetSecOps-Konvergenz möglich, ohne das Budget oder die Ressourcen zu überanspruchen.

Mehr erfahren Sie auf viavisolutions.de/apex

viavisolutions.de

Kontakt +49 7121 86 2222
Sie finden das nächstgelegene VIAVI-Vertriebsbüro auf viavisolutions.de/kontakt

apex-br-ec-de
30186017 915 0326