VIAVI Solutions

Broschüre

VIAVI Observer

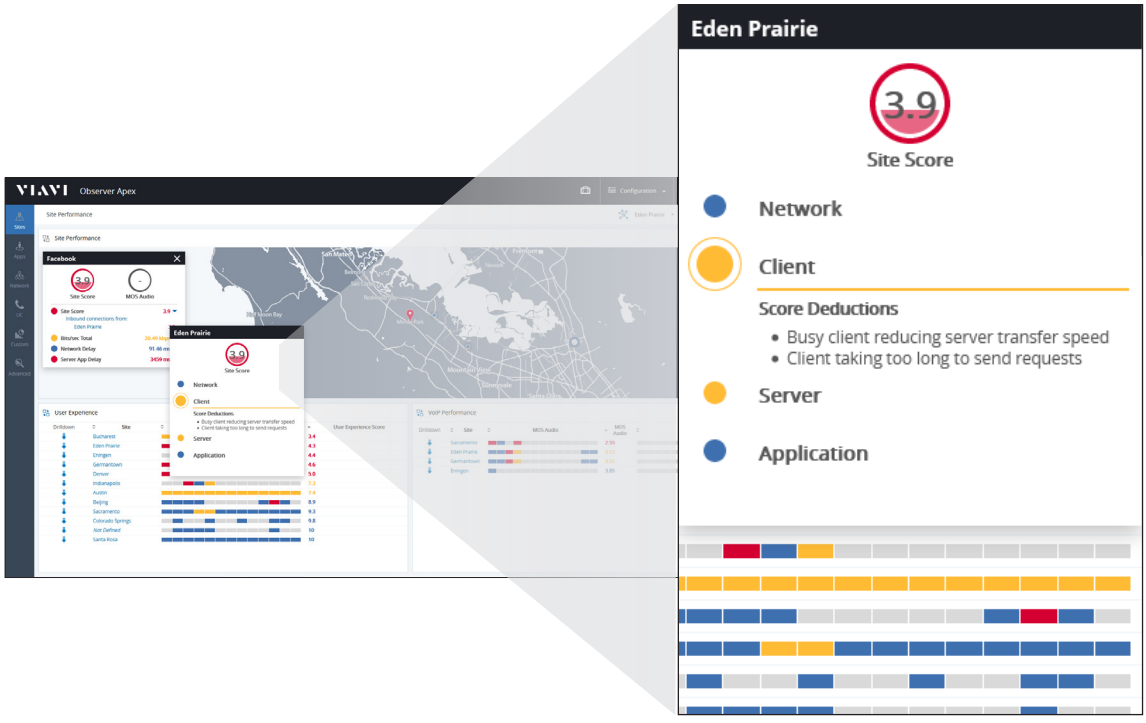
Leistungsüberwachung und Fehlerdiagnose in Netzwerken

Leistungsprobleme lösen und IT-Sicherheitsstrategien stärken

Die Vorteile von Observer

VIAVI Observer® ist eine umfassende Lösung zur Leistungsüberwachung und Fehlerdiagnose in Netzwerken (NPMD), die mit dem Ziel entwickelt wurde, sowohl vor Ort als auch in der Cloud und in hybriden IT-Umgebungen eine optimale Bereitstellung der IT-Dienste sicherzustellen. Mit ihrer erweiterten Datenerhebung und mit aktiven Abwehrfunktionen, wie dem Verfolgen von Bedrohungen (Threat Hunting), stärkt sie zudem die IT-Sicherheit.

Observer nutzt mehrere Datenquellen, darunter Paketdaten und Enriched-Flow-Daten, um mithilfe übersichtlicher und aussagekräftiger Dashboard-Ansichten sowie der branchenweit ersten Bewertung (Scoring) des Endnutzer-Erlebnisses über den aktuellen Status des Netzwerks zu informieren. Enriched-Flow-Datensätze vermitteln umfangreiche Einblicke in den Verkehr und in die zugrunde liegende Infrastruktur im Hinblick auf nutzerspezifische Informationen. Observer ist die erste NPMD-Lösung, die diese beiden leistungsstarken Datenquellen kombiniert, um den Netzwerk- und Sicherheitsteams zu helfen.



Mehr Leistung mit Observer Version 18

Mit der Veröffentlichung von Observer v18 bestehen Paketdaten und Enriched-Flow-Daten in Observer Apex nun nebeneinander. Das bedeutet, dass alle Kompetenzniveaus jetzt Zugriff auf die verschiedenen Ebenen der IT-Transparenz erhalten. Hierfür können sie zudem ihre jeweils bevorzugten Datenquellen nutzen, um beispielsweise QoS-Messungen und Kapazitätsplanungen durchzuführen sowie Referenzwerte zu prüfen. Diese gemeinsame, integrierte Benutzeroberfläche verbessert für alle IT-Nutzerebenen die Effizienz betrieblicher Abläufe durch eine höhere Qualität der Daten, intuitive Visualisierungen und vereinfachte Arbeitsabläufe.

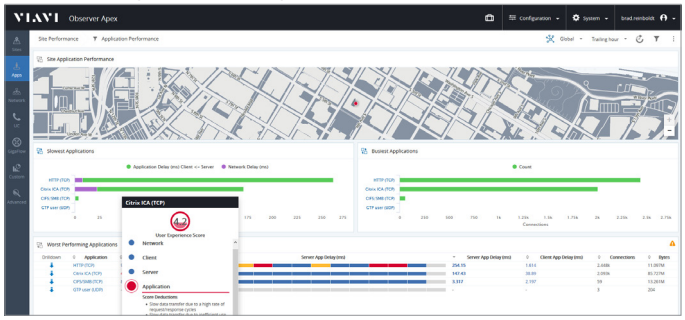
Apex

Zentrales Management des Endnutzer-Erlebnisses, der Leistung und Sicherheit

Observer Apex bietet im Kern des Rechenzentrums, am Netzrand sowie in der Cloud umfassende Echtzeit-Einblicke in kritische IT-Ressourcen. Apex ist der zentrale Ausgangspunkt zum Beheben von Leistungsstörungen mit einem anspruchsvollen Endnutzer-Scoring und sofort einsatzbereiten Workflows. Zur Gewährleistung der Netzwerksicherheit unterstützt Apex nicht nur die Untersuchung von besorgniserregenden Ereignissen (Indicators of Compromise, IOC) oder bestätigten Sicherheitsverletzungen, sondern stellt gleichzeitig tiefgehende retrospektive Forensikdaten zur Verfügung. Die Lösung ermöglicht ebenfalls, Profile der einzelnen Geräte und Hosts zu erstellen. Damit können die IT-Teams nicht nur auf einen Blick erkennen, wer im Netzwerk kommuniziert und was gesagt wird, sondern gleichzeitig Bedrohungen aktiv verfolgen.

Leistungsmerkmale und Vorteile

- Anwenderdefinierte Dashboard-Anzeigen vermitteln unternehmensweite, zusammenfassende und situative Einblicke in den Bereitstellungsstatus von Diensten sowie in die Sicherheitslage.
- Eine auf integrierten Workflows basierende Bedrohungskarte gibt einen aussagekräftigen Echtzeitüberblick über aktuelle Angriffsvektoren.
- Die Bewertung des Endnutzererlebnisses (Scoring) mit Anzeige des die Störung verursachenden Bereiches beschleunigt die Fehlerdiagnose auf Ebene der Transaktion und des Standortes.
- Die anforderungsbasierte ADM-Funktion (Application Dependency Mapping) informiert auf einen Blick über Abhängigkeiten zwischen komplexen mehrschichtigen Anwendungen.
- Die intelligente Analyse und Langzeitarchivierung hochpräziser Daten ermöglichen zuverlässige forensische Untersuchungen.
- Die branchenweit erste Kombination der Daten zu Nutzern, Geräten, Hosts und Infrastrukturelementen in einem einzigen Datensatz, der mit Paketdaten verknüpft ist, erlaubt, erweiterte Profile zu erstellen und erkannte Bedrohungen zu verfolgen.



Mit seinen standortbasierten Dashboard-Anzeigen und der Bewertung des Endnutzererlebnisses vermittelt Apex tiefgehende Einblicke in die Netzwerkleistung

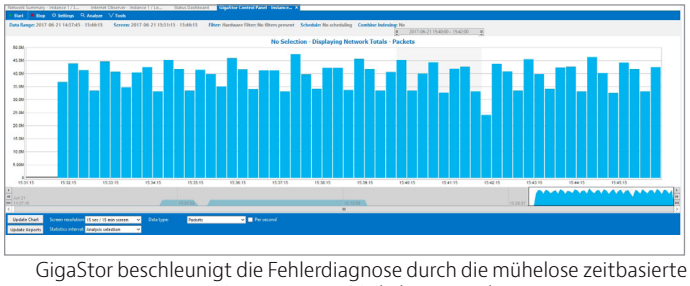
GigaStor

Aufzeichnung kritischer IT-Dienstereignisse

Mit Observer GigaStor™ als dem anerkanntermaßen führenden Produkt zur retrospektiven Analyse gehört das zeitaufwändige Simulieren von Störungen zur Fehlerbehebung endgültig der Vergangenheit an. Stattdessen können Sie die Zeit mühelos „zurückspulen" und vergangene Aktivitäten im Netzwerk nachprüfen. So ist es Ihnen möglich, genau zu dem Zeitpunkt zu navigieren, an dem die Dienststörung aufgetreten ist, um detaillierte Ansichten auf Paketebene zu laden, die den Status vor, während und nach dem Ereignis beschreiben. Die paketbasierten Analysen von GigaStor ermöglichen eine robuste Datenerhebung zur Einhaltung der regulatorischen Anforderungen, für die Sicherheitsforensik und die Fehlerdiagnose im Netzwerk. GigaStor wird in Ausführungen für den Rack-Einbau, als portables Gerät sowie als Softwareversion für cloudbasierte und hybride IT-Anwendungen angeboten.

Leistungsmerkmale und Vorteile

- Unabhängige Validierung der Aufzeichnungsleistung bis 60 Gbit/s mit Unterstützung von 100-Gbit/s-Netzwerken zum schnellen Beheben von Dienststörungen und Durchführen von Sicherheitsuntersuchungen.
- Durch die retrospektive Analyse entfällt das Warten auf erneute, sporadisch auftretende Anomalien, um deren Ursachen klären zu können.
- Die Skalierbarkeit auf mehr als ein Petabyte Speichervolumen ermöglicht umfassendere Einblicke in den früheren Bereitstellungsstatus von Diensten. Die Verschlüsselung der gespeicherten Daten (Data-at-Rest) nach AES-256 gewährleistet die Einhaltung der regulatorischen Vorgaben zum Datenschutz.
- Expertenanalysen stellen detaillierte Einblicke in das Netzwerk und in die Anwendungen, darunter mit tiefgehender Paketprüfung (DPI), zur Verfügung. Damit sind sie ideal geeignet, um bei Dienststörungen und potenziellen Sicherheitsproblemen genaue Einblicke in Transaktionen zu vermitteln.
- Das anwendungsspezifische und fehlertolerante Design unterstützt einen fünfjährigen Dauerbetrieb mit Aufzeichnung bei 100 % Last, ohne dass ein einziges Paket verloren geht.



GigaStor beschleunigt die Fehlerdiagnose durch die mühelose zeitbasierte Navigation zur Verkehrsanomalie

GigaFlow

Enriched-Flow-Daten für Netzwerk- und Sicherheitsteams

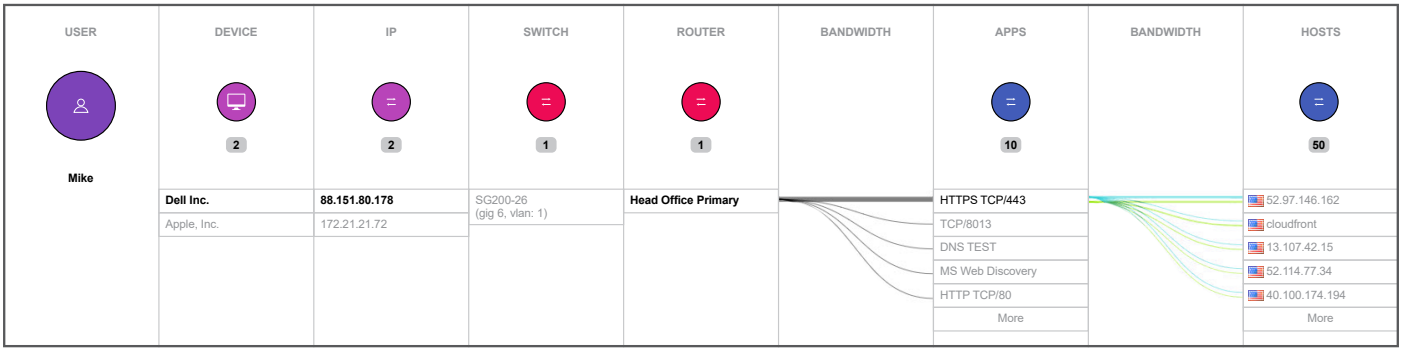
Durch Zusammenführung zuvor isolierter Daten in einen einzigen angereicherten Datensatz stellt Observer GigaFlow nutzerorientierte Informationen zur Verfügung, die es erlauben, Leistungs- und Sicherheitsprobleme zu beheben. Die so gewonnenen Einblicke fördern das Verständnis für das Verhalten und die Leistung von Endnutzern, Anwendungen und Infrastrukturelementen in virtuellen, cloudbasierten und traditionellen Netzwerken und erweitern die Transparenz am Netzwerkrand auf Niederlassungen und abgesetzte Ressourcen.

Auf dieser Grundlage ist eine tiefgehende Untersuchung von Sicherheits- und Leistungsstörungen an Netzwerkgeräten, Verbindungen, Verkehrssteuerungen, Nutzungsmustern und Verhalten bis hinunter auf die Ebene des einzelnen Nutzers und der einzelnen Sitzung möglich.

Leistungsmerkmale und Vorteile

- Die IT-Teams erhalten Einblicke in das Endnutzererlebnis und in die aktuelle Infrastruktur. Auf dieser Grundlage ist es ihnen möglich, informierte Entscheidungen zu treffen, um die Bereitstellung der Dienste zu optimieren und Sicherheitsprobleme zuverlässig einzuschätzen.
- Präzise forensische Einblicke in alle Netzwerk-Konversationen im Zeitverlauf beschleunigen die Problemlösung.
- Die neue, assistentenbasierte Konfiguration von Bedrohungsprofilen erlaubt, die Hosts und Dienste, deren Verkehrsmuster auf Auffälligkeiten überwacht werden sollen, schnell und zuverlässig festzulegen.
- Einblicke in cloudbasierte und virtuelle Geräte erhöhen das Echtzeit-Verständnis für die Leistung in virtuellen, cloudbasierten und abgesetzten Umgebungen.

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, MAC und Anwendungsnutzung im Netzwerk verdeutlichen. Die Mitglieder der Netzwerk- und Sicherheitsteams (NetOps/SecOps) geben dann einfach einen Nutzernamen ein und erhalten sofort alle Geräte, Schnittstellen und Anwendungen, die mit diesem Namen in Verbindung stehen, angezeigt. Nie war es einfacher herauszufinden, welche Geräte angeschlossen sind und wer im Netzwerk kommuniziert.



Ein IP Viewer erleichtert die Navigation zwischen Nutzer, IP, MAC-Adresse und Anwendungsnutzung im Netzwerk

VIAVI Observer auf einen Blick

Observer ist eine Lösung zur Leistungsüberwachung und Fehlerdiagnose in Netzwerken (NPMD), die aktive Funktionen zur Abwehr von Sicherheitsbedrohungen zur Verfügung stellt. Dazu zählen die Verfolgung von Bedrohungen (Threat Hunting) und das Erstellen von Profilen, sodass die NetOps-/SecOps-Teams aussagekräftige operative Informationen zum Status der IT-Systeme erhalten.

Auf Grundlage der hochgenauen Daten, die mit GigaFlow und GigaStor gewonnen wurden, ist Apex der Ausgangspunkt für die sofortige Fehlerdiagnose oder für Sicherheitsuntersuchungen.

Workflowbasierte Kombination von Fluss- und Paketdaten mit Apex

Observer v18 führt Paketdaten und Enriched-Flow-Daten mit optimierten Workflows und leistungsstarken Analysen zusammen. Diese Kombination verdeutlicht den komplementären Charakter der beiden Datentypen:

1. **Paketdaten von GigaStor:** Die Paketdaten bleiben die kritische Quelle für die Ende-zu-Ende-Transparenz und die beste Grundlage für die präzise Messung des Endnutzererlebnisses und der exakten forensischen Analyse.
2. **Enriched-Flow-Daten von GigaFlow:** GigaFlow erfasst die Daten von den Geräten, die von diesen Daten beim Passieren des Netzwerks durchlaufen werden. Damit stehen zusätzliche Informationen zum Nutzer, zum physischen Anschluss, zur Verkehrsklasse, zur Priorisierung (oder Sperre) und zu Verhaltensmustern sowie weitere kritische Details zur Verfügung.

Apex fasst diese Daten von GigaStor und GigaFlow in Form von aussagekräftigen Visualisierungen und effizienten Workflows zusammen. Damit stellt das System lückenlose Ansichten zur Leistung und Bedrohungslage in der gesamten Umgebung des Netzwerks bereit. Der Anwender hat die Möglichkeit, Probleme mit dem zum Patent angemeldeten Endnutzer-Scoring und den Echtzeit-Bedrohungskarten zu lokalisieren. Die so gewonnenen verwertbaren Einblicke beschleunigen den Wissenszuwachs und verkürzen die Zeit bis zur Behebung der Störung.

Durch die Kombination von Paketdaten mit datenflussbasierten Analysen vermittelt Observer Apex den SecOps-/NetOps-Teams lückenlose Einblicke in ihr Netzwerk. Diese Transparenz versetzt sie in die Lage, die täglichen Betriebsabläufe unter Kontrolle zu halten, Sicherheitsrisiken zu mindern und Probleme schneller als je zuvor zu beheben.

VIAVI Solutions

Kontakt +49 7121 86 2222

Sie finden das nächstgelegene VIAVI-Vertriebsbüro auf viavisolutions.de/kontakt

observerplatform-ov-ni-de
30186020 914 0820