Observer Apex

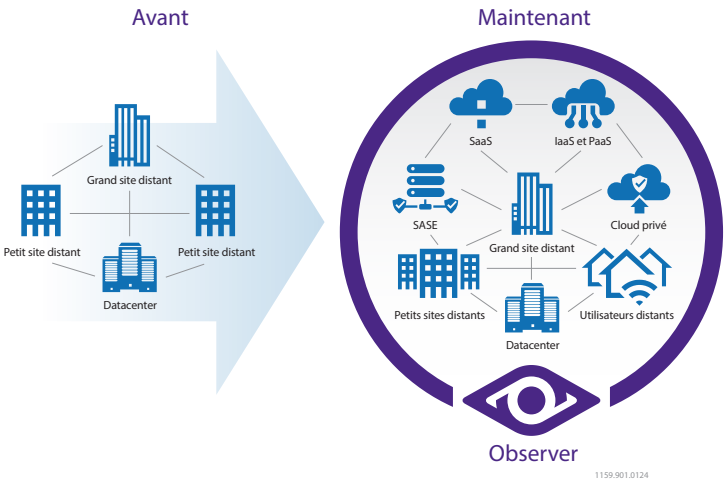
Conçu pour NetSecOps : En savoir plus. Accélérez l'investigation.

Obtenez des informations partagées relatives au réseau et à la sécurité grâce à des analyses avancées et une investigation fondée sur des preuves.

LE RÉSEAU EST PARTOUT

Applications complexes et à plusieurs niveaux, hébergées sur site ou dans le cloud, de type SaaS, IaaS, PaaS et SASE. Pour les utilisateurs, la capacité à accéder à leurs applications partout, à tout moment, constitue la nouvelle norme. Aujourd'hui, le réseau n'a aucune frontière et tous les services informatiques en dépendent.

En cas de défaillance d'un élément du réseau ou de l'architecture de service, le débit d'application peut se dégrader rapidement et conduire à l'insatisfaction du client et à une réduction des profits commerciaux. Pour éviter cela, une observabilité de service complète est indispensable.



Observer Apex offre de la visibilité là où elle est la plus nécessaire. C'est la première solution de gestion des performances capable de générer un score d'expérience de l'utilisateur final (EUE) pour chaque transaction. En corrélant les paquets, les métadonnées et les flux enrichis, Apex fournit des informations approfondies sur les performances des applications, des services et de l'infrastructure dans les environnements hybrides. Les organisations peuvent choisir les sources de données qui s'alignent le mieux avec leurs budgets et leurs besoins opérationnels tout en conservant la flexibilité nécessaire pour développer la visibilité à mesure que les environnements évoluent.

Apex offre une visibilité globale sur l'état de santé et les performances des services informatiques et permet également aux équipes de passer rapidement de l'investigation à la détection en cas d'anomalies. À l'aide des alertes intégrées, des analyses contextuelles et des processus d'investigation, les équipes NetOps, DevOps et SecOps déterminent promptement si les problèmes proviennent du réseau, d'une application, d'un client ou d'un événement de sécurité potentiel.

En combinant les données de performances et des capacités d'investigation technico-légale, Apex accélère l'analyse des causes profondes et permet aux équipes de résoudre les incidents d'exploitation et de sécurité en toute confiance.

CENTRE DE COMMANDE POUR NETSECOPS

- **Les scores d'EUE automatisés, pilotés par l'apprentissage machine** convertissent de multiples KPI (Key Performance indicator) en une mesure unique. À cela s'ajoutent des réductions de score détaillées qui permettent d'identifier automatiquement les problèmes et de les résoudre rapidement.
- **Observer Threat Forensics avec informations sur les menaces, optimisé par CrowdStrike®** associe des données exploitables au niveau des paquets à des informations sur les menaces afin d'enrichir les processus de détection et d'investigation. En intégrant directement le contexte des menaces dans l'expérience d'investigation, les équipes peuvent accélérer le triage, assurer une validation extrêmement fiable des menaces, bénéficier d'une visibilité dans les environnements hybrides et réagir en conséquence.
- **Des options de sources de données flexibles**, incluant des paquets, des métadonnées et un flux enrichi, offrent une visibilité appropriée à chaque partie prenante, de l'ingénieur réseau jusqu'au propriétaire de l'unité d'exploitation.

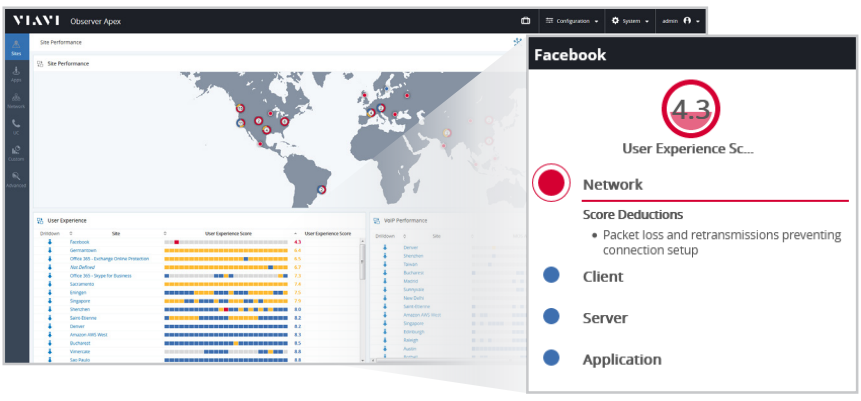
- **Des tableaux de bord personnalisables** fournissant des informations opérationnelles globales et des workflows efficaces permettent aux équipes NetOps, SecOps et DevOps d'identifier et de résoudre rapidement les problèmes.
- **Le mappage des dépendances applicatives à la demande (OD-AM)** offre une visibilité immédiate et précise sur les applications à plusieurs niveaux sans nécessiter aucune configuration.
- **Gestion des performances et analyses technico-légales intégrées** pour une réponse rapide aux anomalies de service et aux violations de cybersécurité
- Les capacités d'**inspection des paquets en profondeur (DPI)** aident à comprendre la composition du trafic réseau et à déterminer si le trafic non critique a une incidence négative sur les principaux services aux entreprises et sur les utilisateurs finaux.
- L'**analyse de certificats numériques** identifie ceux qui ont expiré ou approchent de la date d'expiration, ainsi que les protocoles obsolètes afin d'assurer la conformité et un service ininterrompu aux utilisateurs.
- Les processus de **communications unifiées (UC)** guident les experts en UC depuis les résumés généraux et vues spécifiques à un site jusqu'aux détails d'appels interactifs. Les données des paquets et des flux sont directement intégrées de manière à visualiser un parcours d'appel unique point à point ou d'appels complexes multipoints sur l'infrastructure réseau.
- L'**ingestion et l'analyse des journaux des flux cloud** offrent la visibilité nécessaire sur le trafic cloud, contribuant à la détection des menaces pesant sur la sécurité, à l'identification des anomalies et au respect de la conformité pour les environnements cloud tels qu'Amazon Web Services (AWS) et Microsoft Azure.
- **Options de déploiement flexibles** depuis des dispositifs conçus sur mesure pour les datacenters vers des images de machines virtuelles, pour des déploiements dans le cloud simples et efficaces

GESTION DES PERFORMANCES

Score de l'expérience utilisateur

Grâce à des analyses brevetées, soutenues par l'apprentissage machine, Apex supprime les doutes relatifs à l'évaluation de la satisfaction de l'utilisateur et mesure toutes les conversations de façon précise. Chaque conversation est notée sur une échelle de 0 à 10 et à l'aide d'un code/classement de couleurs indiquant le niveau de performance du point de vue de l'utilisateur, tout en prenant en compte son comportement environnemental et applicatif unique, permettant ainsi l'élimination des faux positifs.

Les scores offrent de la visibilité sur l'expérience d'un utilisateur spécifique, ou ils peuvent être élargis à un site, un service ou une vue globale de l'entreprise. Apex va encore plus loin en isolant les problèmes au niveau du réseau, du client, du serveur ou du domaine d'application concerné, et en fournissant une description claire du problème.



Tableaux de bord commerciaux personnalisés

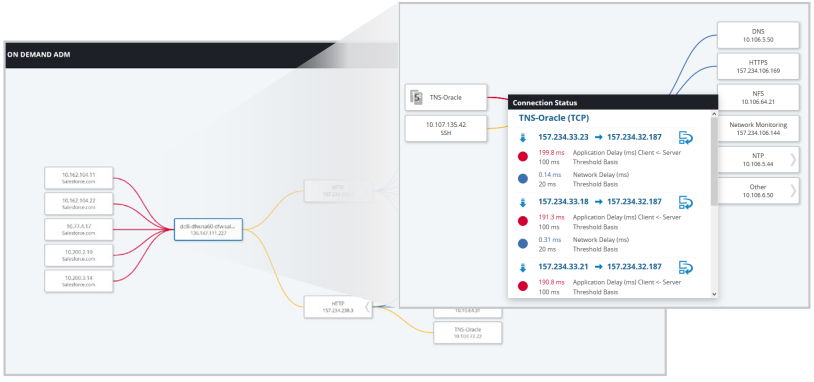
Des tableaux de bord basés sur la géolocalisation et définis par l'utilisateur assurent une connaissance intégrée, à l'échelle de l'entreprise, de la situation en ce qui concerne l'état du service.

Processus de dépannage

Avec des processus axés sur les sites et les services, et intégrés au score de l'expérience de l'utilisateur final, les équipes informatiques obtiennent une visibilité instantanée, au niveau mondial, sur la situation de toutes les ressources. Ils obtiennent ainsi plus vite des informations relatives à un utilisateur individuel pour une résolution rapide du problème.

Données d'application à plusieurs niveaux et à la demande

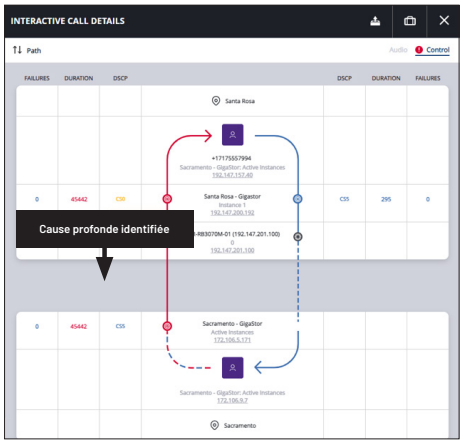
L'OD-AM assure a prise en charge de services à plusieurs niveaux, la détection rapide des interdépendances applicatives et la représentation ad hoc de cartes permettant de visualiser ces relations complexes de façon claire. D'un simple clic, Apex génère une cartographie complète, puis identifie automatiquement et met en évidence les pires connexions afin que les utilisateurs puissent rapidement déterminer leurs priorités en matière de dépannage.



Les dépendances applicatives automatisées sont mappées avec les scores de l'expérience utilisateur intégrés.

Communications unifiées (UC)

Les tableaux de bord et processus d'UC d'Apex guident efficacement les experts en VoIP et UC depuis des résumés globaux et des vues spécifiques à un site jusqu'à des visualisations interactives des détails d'appels. Observer est le seul outil à combiner les données des paquets et des flux de manière à visualiser un parcours d'appel unique point à point ou d'appels complexes multipoints sur l'infrastructure réseau. Il identifie les sources de la dégradation de qualité tout en offrant, si nécessaire, un accès en un clic aux données de paquets pertinentes.



Les détails des appels interactifs identifient les causes profondes des dégradations de la qualité.

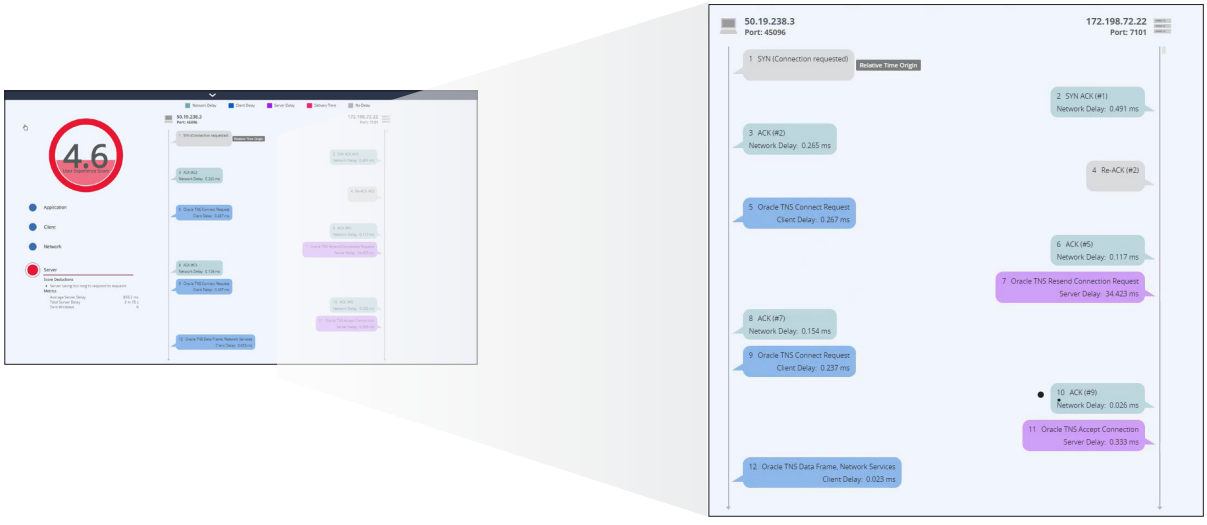
Principaux avantages :

- **Mappage visuel du parcours :** Transformation des données de paquets et de flux en des visualisations intuitives des parcours d'appels
- **Résolution rapide des problèmes :** Réduisez considérablement le temps moyen de réparation en identifiant facilement la cause profonde des problèmes de performances des UC.
- **Interface conviviale :** L'interface facile à utiliser et à comprendre fournit aux non-experts des représentations simples des appels d'UC complexes multipoints et point à point.

ANALYSE TECHNICO-LÉGALE DE SÉCURITÉ ET DES RÉSEAUX

Les analyses technico-légales du réseau réalisées avec Observer intègrent deux sources de données complémentaires, à savoir les paquets et le flux enrichi, tout en étant capables de conserver ces données pendant des périodes de temps prolongées. Les options de déploiement d'images de machines virtuelles permettent de collecter et d'analyser des paquets des flux enrichis pour les applications cloud hébergées. L'identification de la cause profonde de nombreux problèmes de performance et violations de sécurité commence avec des métadonnées et des tableaux de bord intuitifs, mais se termine souvent avec des workflows logiques menant à la visibilité sur les données sous-jacentes, parfois même plusieurs jours après l'événement. C'est pourquoi Observer conserve ces détails sur de plus longues périodes.

Comme indiqué ci-dessus, de nombreuses anomalies de performance sont rapidement isolées grâce au score de l'expérience de l'utilisateur final. Cependant, lorsque des détails de plus haute fidélité sont requis, les données de soutien sont instantanément disponibles.



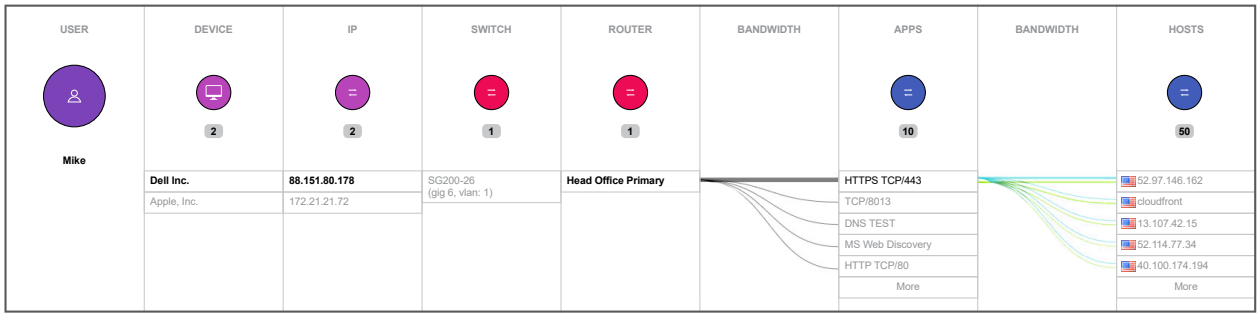
Score de l'expérience de l'utilisateur final avec segmentation des conversations dynamiques des connexions associées

Analyses technico-légales de conversations

Grâce aux données de paquets capturées par Observer, l'intégralité de chaque transaction, du début à la fin, est disponible pour l'analyse et l'investigation. Quelles que soient vos attentes, du tableau de bord global aux paquets individuels, tout est disponible en quelques étapes.

Grâce à la visibilité supplémentaire fournie par l'identification des applications gérée par l'inspection des paquets en profondeur (DPI), Observer fournit des informations exploitables avancées sur le trafic réseau. Cette capacité permet aux ingénieurs réseau d'identifier facilement le trafic sur les ports non standard, de quantifier le trafic non critique et d'examiner en profondeur les protocoles tels que le HTTP et le HTTPS. Les capacités DPI d'Observer vous aident à identifier plus de 4 300 applications et à découvrir en un coup d'œil si une conversation est une transaction commerciale ou une autre opération.

Analyse technico-légale de flux enrichis



Observer GigaFlow IP Viewer permet de visualiser l'activité de l'utilisateur sur l'ensemble de l'infrastructure réseau pour chaque conversation.

En compilant des données de couches 2 et 3 au sein d'un enregistrement unique de flux enrichis, Observer est capable de produire des visualisations uniques et interactives qui illustrent les relations entre utilisateur, adresse IP, adresse MAC et utilisation de l'application au sein du réseau. Il suffit alors aux utilisateurs de saisir un nom/nom d'utilisateur ou une adresse IP pour accéder immédiatement à une liste de tous les appareils, interfaces et applications qui lui sont associés. Découvrir les éléments connectés et les personnes communiquant sur votre réseau n'a jamais été aussi facile.

Gestion des certificats numériques

Observer surveille les poignées de main SSL/TLS à mesure qu'il analyse votre trafic réseau, identifiant les certificats numériques expirés ou proches d'expirer et envoyant des notifications proactives. Il identifie les sessions non sécurisées de publication sur les serveurs, signale les protocoles obsolètes, valide la conformité et aide à assurer un trafic ininterrompu pour les utilisateurs.

Le tableau de bord d'analyse des certificats fait apparaître la version de TLS, la date d'expiration des certificats et les versions de Cipher Suite.

Pour les ingénieurs et administrateurs réseau, assurer la disponibilité et la satisfaction des clients est essentiel dans la prestation de services Web. L'adoption d'une approche proactive d'analyse des certificats au lieu d'une méthode de rapports manuels (tels que des tableurs) simplifie le processus et protège votre entreprise contre les dégradations potentielles liées aux certificats.

Principaux avantages :

- **Surveillance proactive :** Des analyses, rapports et notifications en temps réel qui vous aident à anticiper l'expiration des certificats
- **Informations exploitables améliorées sur la sécurité :** Obtenez une vue claire des versions SSL ou TLS utilisées et désactivez rapidement les protocoles obsolètes ou non sécurisés
- **Continuité de service :** L'identification et la correction des problèmes liés aux certificats permettent d'éviter les pannes potentielles et d'assurer une expérience utilisateur transparente

En matière de cybersécurité, la meilleure protection contre les menaces exige une stratégie en trois parties : prévention, détection et réponse.

Prévention		Détection	Réponse
• Pare-feu • Prévention des attaques par déni de service (DDoS) • Prévention des pertes de données • Prévention des intrusions • Anti-virus et logiciels malveillants	• Chiffrement • Anti-spam/ Hameçonnage • Contrôles d'accès • Sécurité des terminaux	• Détection des intrusions • Gestion des événements liés à la sécurité (SIEM) • Détection de terminaux	• Analyses technico-légales du réseau • Gestion des événements liés à la sécurité (SIEM)

De nombreuses entreprises se focalisent sur la prévention et la détection, jusqu'à ce qu'une violation soit confirmée et qu'une cellule de crise créée dans l'urgence commence à répondre à la menace. À ce moment, le fait d'avoir accès à toutes les activités passées du réseau, à partir d'un point donné, est crucial pour pouvoir limiter les dommages et régler le problème en toute confiance.

Et c'est là que les analyses technico-légales du réseau présentent un intérêt inestimable. Observer, grâce à la puissance combinée des analyses technico-légales au niveau du trafic et du flux enrichi, vous permet de reprendre vos activités en répondant aux questions comment/qui/quoi/où pour chaque violation de cybersécurité.

Analyses technico-légales du trafic

Comment sont ou étaient connectés les appareils ?

Qui communique ou communiquait ?

Analyse technico-légale de flux enrichis

Qu'est-ce qui est ou a été transmis ?

Quelle a été la portée des actions douteuses ?

En répondant à ces questions, les équipes informatiques peuvent rapidement déterminer le « vecteur d'attaque » (comment le malfaiteur est parvenu à contourner les mesures de prévention et de détection pour obtenir l'accès) et identifier les services informatiques, les appareils ou les données client/commerciales sensibles ayant été compromis. Il est ensuite possible d'endiguer le problème et de finaliser l'évaluation des dommages.

OBSERVER THREAT FORENSICS

Visibilité exploitable sur les menaces pour une investigation et des réponses sûres

Observer Threat Forensics ajoute une nouvelle dimension à l'analyse technico-légale des réseaux en intégrant des informations constamment mises à jour sur les menaces et optimisées par CrowdStrike® aux preuves de flux enrichis et de couche de paquets. Les équipes peuvent ainsi relier des comportements hostiles à des schémas de trafic suspects, à des alertes de sécurité et à la dégradation des performances, le tout en temps réel.

En intégrant les indicateurs d'intrusion (IOC), les TTP des attaquants et autres détails sur les agents hostiles directement dans l'expérience d'investigation, Observer permet aux analystes de valider rapidement les menaces sans associations manuelles et sans retard dans l'enrichissement. À l'aide des alertes intégrées et des processus d'investigation, les équipes de sécurité et de réseau lancent directement le triage au sein de la plate-forme pour cerner plus rapidement le problème et réagir promptement.

Qu'elle soit déclenchée par des indicateurs de menace connus ou par un comportement inattendu du réseau, chaque alerte inclut un accès stratégique aux données de paquet brutes, aux métadonnées des flux enrichis et à des informations contextuelles sur les menaces. Elle fournit aux analystes les preuves grâce auxquelles ils pourront évaluer l'impact et la portée, déterminer la cause profonde et prendre les mesures critiques nécessaires dans les environnements hybrides.

À la différence des solutions traditionnelles qui commencent généralement au « Jour 1 », Observer Threat Forensics permet une analyse véritablement rétrospective dans le cadre de laquelle les équipes de sécurité peuvent retracer les menaces jusqu'au Jour 0. Grâce à la conservation à long terme des données réseau haute fidélité, les analystes sont en mesure de reconstituer la chronologie complète de l'attaque, même avant la première alerte, et de révéler la cause profonde, les points d'entrée et le mouvement latéral à partir d'une source de vérité unique.

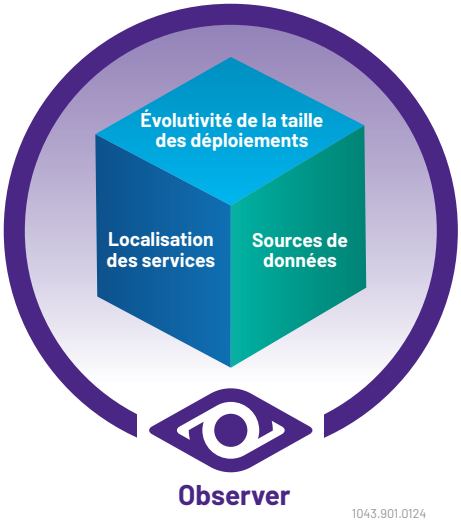
Principaux avantages :

- La **corrélation en temps réel** entre l'activité du réseau et les informations sur les menaces entraîne une réduction des approximations et du temps moyen de réparation (MTTR)
- L'**analyse rétrospective** offre une visibilité sur le Jour 0 en fournissant les preuves technico-légales nécessaires pour examiner l'activité des menaces précédant la détection initiale
- L'**intégration du contexte de l'attaquant** et la prise en charge des TTP assurent un triage et une analyse en toute fiabilité
- Des **liens directs vers les preuves de paquets** permettent de les explorer rapidement en cascade pour évaluer la portée et l'impact de l'attaque
- La **visibilité partagée** renforce la collaboration entre les équipes NetOps et SecOps

Observer Threat Forensics aide à unifier les opérations de réseau et de sécurité grâce à une vue partagée haute fidélité qui établit la corrélation entre les performances, le comportement et l'activité des menaces. En associant les preuves technico-légales relatives au réseau, les métadonnées enrichies et les informations sur les menaces au sein d'une plate-forme unifiée, les équipes bénéficient de la clarté nécessaire pour réagir plus rapidement et résoudre les incidents en toute confiance.

PRÉSENTATION D'OBSERVER

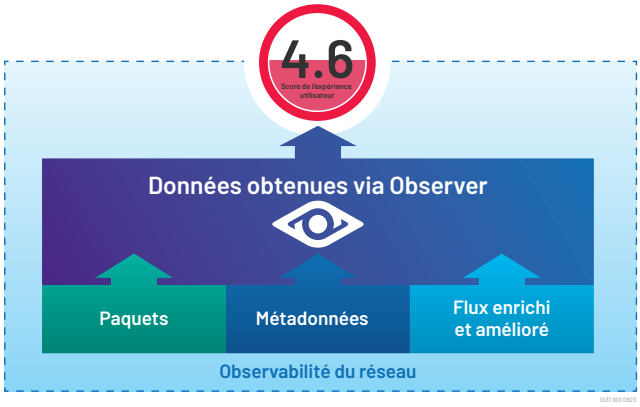
La plateforme Observer de VIAVI est une solution complète de gestion des performances et de la sécurité qui fournit aux équipes chargées des réseaux, des opérations et de la sécurité des informations exploitables issues de tous les environnements hybrides. Observer Apex collecte les métadonnées de transaction depuis de multiples sources de données lors du calcul du score de l'EUE. Elle intègre la détection des menaces et l'analyse au niveau technico-légal afin d'offrir une visibilité partagée, sous forme de source de vérité unique, aux équipes NetOps et SecOps.



En tant que tableau de bord intégré et ressource de création de rapport, Apex fait office de point de visibilité global et central, mais il sert aussi de point de départ pour un dépannage rapide à l'aide de workflows optimisés qui contribuent à identifier les causes profondes en utilisant des paquets, des métadonnées, ainsi que des flux enrichis et améliorés. Grâce à l'intégration du contexte des menaces et à un accès direct aux données technico-légales, les équipes de sécurité peuvent valider les incidents, en évaluer l'impact et isoler rapidement la cause profonde.

Observer assiste les équipes informatiques de trois façons principales :

- **Localisation de services :** Observer permet l'observation de tous les environnements d'hébergement, qu'il s'agisse de cloud privé, d'utilisateurs distants, de sites de bureaux ou de datacenters. Quel que soit l'emplacement, vous pouvez compter sur VIAVI Observer.
- **Sources de données :** Observer offre des options flexibles de visibilité à l'aide de paquets, de flux enrichis et de métadonnées. Cette approche multicouche prend en charge le dépannage des problèmes de performances aussi bien que l'analyse technico-légale après incident. Avec des workflows basés sur des rôles et des alertes riches en contexte, les équipes peuvent tout analyser avec fiabilité, depuis les anomalies de service jusqu'aux menaces de sécurité, en s'appuyant sur des données pertinentes mises à disposition au moment opportun.



- **Évolutivité de la taille des déploiements :** commencez à petite échelle et développez votre déploiement à mesure que les besoins opérationnels et de sécurité évoluent. VIAVI propose des modèles de déploiement flexibles et une hiérarchie de tarifs d'abonnement qui s'alignent sur vos besoins OpEx ou CapEx.
  Vous bénéficiez ainsi d'une visibilité évolutive et d'une convergence NetSecOps sans grever votre budget ou vos ressources.

Pour en savoir plus : viavisolutions.fr/apex

viavisolutions.fr

Contactez-nous+1 844 GO VIAVI | (+1 844 468 4284) | +33 1 30 81 50 50
Pour contacter le bureau VIAVI le plus proche, rendez-vous sur viavisolutions.fr/contact

apex-br-ec-fr
30186016 915 0326