Gigamon®

En l’absence d’observabilité avancée, vous risquez un début d’incendie sans vous en rendre compte

L’intelligence provenant du réseau détecte les menaces que les outils de sécurité existants ne peuvent pas voir.

Le casse-tête du CISO

Selon *Forbes*, le nombre de grandes entreprises ayant une stratégie multi-cloud devrait atteindre 85 % en 2024[1], car les entreprises cherchent à équilibrer la souplesse de l'entreprise et la cybersécurité dans les transformations du cloud.

Dans le même temps, le coût et l'ampleur des cyberattaques n'ont jamais été aussi élevés, les coûts mondiaux de la cybercriminalité devant atteindre 10 500 milliards de dollars d'ici à 2025.[2] Les CISO sont donc confrontés au défi de sécuriser et de surveiller leur infrastructure complexe face à un ensemble de menaces de plus en plus complexes, tout en maîtrisant les coûts et la complexité. Malgré des dépenses record consacrées aux stratégies et outils de sécurité les plus récents, tels que SASE, EDR, micro-segmentation du réseau et SIEM, les CISO ont toujours du mal à faire face à la vague croissante de menaces émergentes, en particulier les rançongiciels et les atteintes à l'intégrité des personnes.

1. Marr, B. (2024, February 20). The 10 biggest cloud computing trends in 2024 Everyone must be ready for now. Forbes.
2. Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.

Comment les failles de sécurité affectent les résultats

Le coût d'une faille de sécurité va bien au-delà des dollars et des centimes, et a des répercussions considérables sur les entreprises :

- Perturber les activités de l'entreprise en provoquant des temps d'arrêt et des pertes de revenus.
- Nuire à la réputation d'une entreprise et à la fidélité de ses clients par le vol de propriété intellectuelle et de données sur les clients.
- Rendre plus coûteuse (voire impossible) la souscription d'une cyber-assurance.
- Exposer l'entreprise et ses dirigeants au risque d'amendes liées à la réglementation et à la conformité, voire à une peine de prison.

Vos outils de sécurité font un excellent travail. Pour autant que vous le sachiez.

En l’absence d’observabilité avancée, vous risquez de vous retrouver avec les cheveux en feu.

Les plus grands angles morts de votre réseau : le trafic latéral et crypté

L’adoption croissante de clouds s’accompagne également d’une augmentation des coûts, ainsi que de la complexité de la sécurisation et de la gestion de votre infrastructure de cloud hybride. Les différents composants de l’infrastructure ont leurs propres outils et processus de surveillance, ce qui conduit à une structure fragmentée d’outils compartimentés qui n’offre pas une image complète de ce qui se passe réellement dans votre infrastructure de cloud hybride.

Vos outils de sécurité sont résistants face à certaines menaces et étonnamment passifs face à d’autres.

La plupart des outils de sécurité inspectent le trafic nord-sud, mais négligent souvent les mouvements latéraux, qui peuvent conduire à des conséquences dévastatrices pour votre entreprise. Si des individus mal intentionnés pénètrent votre réseau, ils peuvent se déplacer librement dans votre infrastructure de cloud hybride sans être détectés, et finalement accéder aux données les plus sensibles de votre entreprise.

L’observabilité avancée Gigamon pour les flux de données est la seule solution qui se concentre exclusivement sur l’élimination de cet angle mort en fournissant la visibilité latérale Est-Ouest nécessaire pour détecter des menaces jusqu’alors invisibles, y compris celles qui peuvent déjà se trouver à l’intérieur de votre réseau.

Les dangers du trafic crypté

Étant donné que 95 % de l'ensemble du trafic web est crypté,[4] les entreprises qui n'ont pas de visibilité sur le trafic crypté sont exposées à des menaces cachées que leurs outils de sécurité existants ne peuvent pas détecter. Et à mesure que le chiffrement progresse, les menaces d'exploitation des canaux chiffrés se multiplient.

Chaque réseau a quelque chose à cacher. Jusqu'à présent.

Le décryptage de l'ensemble du trafic peut s'avérer coûteux et complexe, exigeant une puissance de calcul élevée tout en augsmentant la latence et en réduisant les performances, jusqu'à aujourd'hui. Gigamon offre une combinaison puissante de solutions brevetées qui rendent la visibilité du trafic crypté abordable et évolutive, y compris notre technologie Precryption™ primée et le déchiffrement des connexions TLS/SSL GigaSMART©.

Parmi les entreprises qui ont subi une attaque sur des données chiffrées au cours de l'année écoulée, 85 % ont été témoins d'attaques sur des données « fiables », tels que les sites web légitimes des entreprises de confiance ou des vendeurs tiers. C'est un rappel brutal qu'aucun trafic crypté par TLS/SSL ne peut être considéré comme sûr.[5]

4. Google Transparency Report
5. Zscaler ThreatLabz 2023 State of Encrypted Attacks Report
6. 2024 Gigamon Hybrid Cloud Survey

Le manque de préparation

L'excès de confiance dans la sécurité du trafic crypté crée d'énormes zones d'ombre propices à l'exploitation.

76 %
DES CISO
estiment que le trafic crypté est sécurisé.

63 %
DES CISOS
estiment que le trafic crypté a moins de chances d'être inspecté.

86 %
DES CYBERMENACES
sont dissimulées dans le trafic crypté.

62 %
DES ENTREPRISES
ont constaté une augmentation des attaques sur les canaux cryptés au cours de l'année écoulée.[6]

Même les meilleurs outils de sécurité et d'observabilité ont des points faibles

Voir l'ensemble de l'iceberg grâce à l'observabilité avancée.

Les outils traditionnels et natifs du cloud qui obtiennent une visibilité exclusivement par le biais de données métriques, d'événements, de journaux et de traces (MELT) sont limités dans ce qu'ils peuvent détecter et dans la profondeur ou l'étendue de leur surveillance de l'infrastructure complexe actuelle.

L'observabilité avancée Gigamon pour les flux de données va plus loin que les approches d'observabilité classiques en extrayant des informations directement du trafic réseau, en les transmettant efficacement à vos outils en temps réel. Grâce à cette intelligence dérivée du réseau, vos outils peuvent détecter des menaces jusque-là cachées, ce qui aide à réduire le coût et la gravité d'une attaque.

> L'observabilité avancée permet d'éliminer les angles morts en donnant à vos outils l'intelligence et les informations dérivées du réseau nécessaires pour détecter les menaces qui seraient passées inaperçues auparavant.

L'importance croissante de la détection des menaces en temps réel

Les cyberattaques sont de plus en plus rapides et agressives, car les auteurs raccourcissent le délai entre l'entrée initiale, le mouvement latéral et l'intrusion.

62 minutes

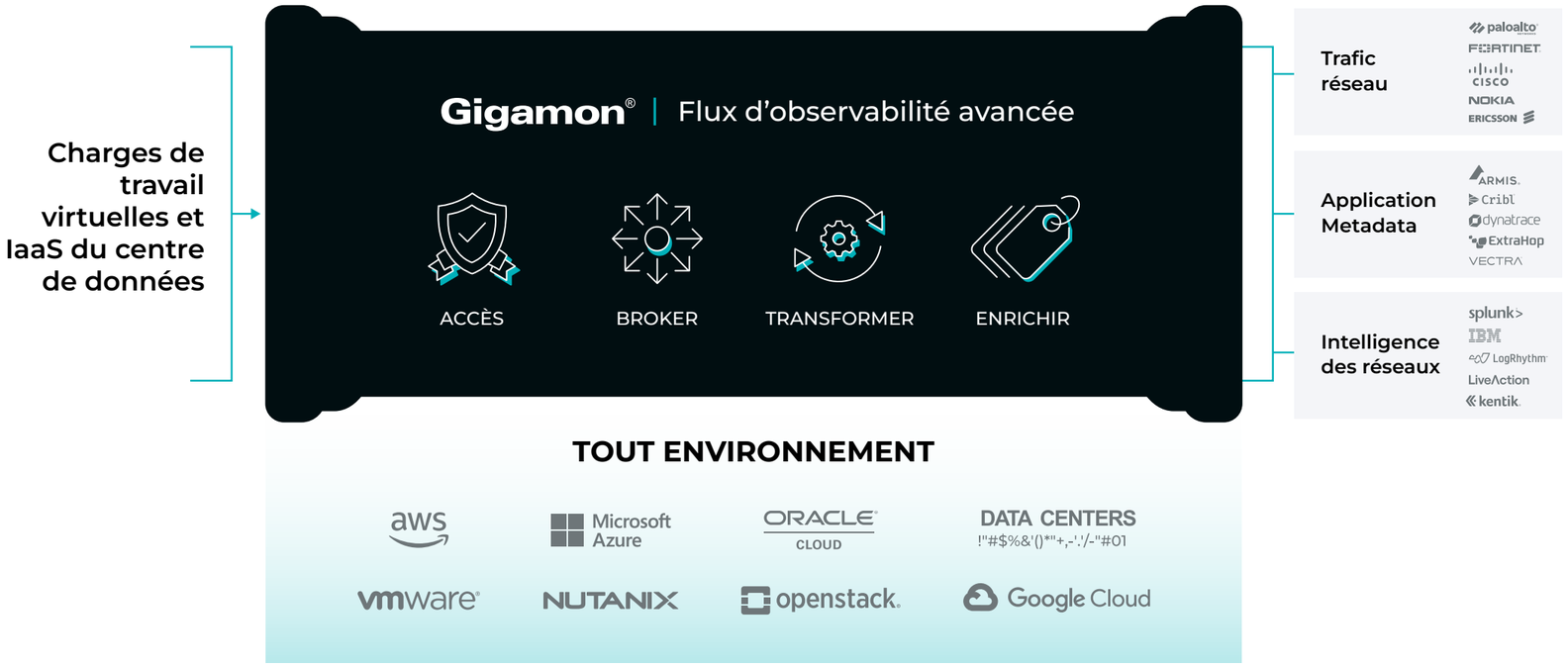
Le temps moyen nécessaire à un individu pour passer d'un hôte initialement compromis à un autre au sein de l'entreprise s'est accéléré de 23 % depuis l'année dernière, certains ne mettant que quelques minutes pour y parvenir.

204 jours

Il faut en moyenne 204 jours aux entreprises pour identifier une violation de données et 73 jours pour y remédier.[7]

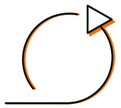
7. CrowdStrike 2024 Global Threat Report

Un flux d’observabilité avancée spécialement conçu



L’observabilité avancée Gigamon pour les flux de données, basée sur GigaVUE Cloud Suite™, fournit efficacement des informations dérivées du réseau à vos outils de cloud, de sécurité et d’observabilité. Cela permet d’éliminer les angles morts en matière de sécurité et de réduire le coût des outils, afin de mieux sécuriser et gérer l’infrastructure du cloud hybride.

Optimisez vos outils de sécurité pour obtenir des résultats tangibles



Augmenter la souplesse, réduire les coûts

La solution pour renforcer votre niveau de sécurité n'est pas nécessairement d'investir dans davantage d'outils. En fait, un trop grand nombre d'outils s'est avéré moins efficace pour détecter et atténuer les menaces en surchargeant les équipes de sécurité et en créant des compartiments de données qui entraînent des manques de visibilité et des angles morts.[3]

Gigamon optimise la performance et l'efficacité des outils pour aider les entreprises à gérer la prolifération des outils, à réduire les coûts, et surtout à obtenir l'observabilité avancée dont vous avez besoin pour éliminer les angles morts.

Réduire les coûts opérationnels

En optimisant et en améliorant le rapport signal/bruit de l'ingestion du trafic réseau, les clients de Gigamon réalisent souvent des économies de 50 à 60 % sur les dépenses d'outils et reportent les achats de nouvelles capacités en cours d'année. Gigamon élimine également le besoin de passerelles et de services d'équilibrage de charge coûteux, réduisant le coût d'acquisition du trafic sur le cloud de 0,75 centimes à 0,04 centimes par gigaoctet.

L'observabilité avancée rend vos outils de sécurité et d'observabilité existants jusqu'à **90 % plus efficaces** et peut réduire les coûts des outils et de la bande passante jusqu'à 50 %, ce qui permet à un client de taille moyenne d'obtenir un retour sur investissement de 4 à 6 mois.

3. 2020 Cyber Resilient Organization Report

Éteindre le feu avant qu’il ne démarre.

Sans possibilité d’observabilité avancée, vous êtes vulnérable à des menaces invisibles.

Le leader du marché de l’observabilité avancée

650 GROUP
Market Intelligence Research
N° 1 EN TERMES DE PARTS DE MARCHÉ
Observabilité avancée
2023

Selon le cabinet d’études de marché 650 Group, Gigamon est un leader du marché de l’observabilité avancée avec une part de marché de 63 % en 2023.

Les agences gouvernementales et les entreprises les plus soucieuses de la sécurité dans le monde s’appuient sur Gigamon pour réduire concrètement les risques.

+ de 4 000
CLIENTS DANS LE MONDE ENTIER

10/10
AGENCES FÉDÉRALES AMÉRICAINES

8/10
PLUS GRANDS PRESTATAIRES DE SOINS DE SANTÉ

83/100
ENTREPRISES DU CLASSEMENT FORTUNE 100

7/10
PLUS GRANDES BANQUES MONDIALES

9/10
PLUS GRANDS OPÉRATEURS DE RÉSEAUX MOBILES

« Pour quelques incidents survenus au cours des six derniers mois, nous avons pu intervenir assez rapidement, environ une heure après que le pirate a pris possession d'un serveur. Nous avons pu les détecter juste à temps, avant qu'ils fassent de réels dégâts. La raison en est que nous avons mis en place des outils de sécurité et que Gigamon fournit toutes les données dans ces outils de sécurité. »

Kajeevan Rajanayagam,
Directeur de la cybersécurité à la University Health Network

« Les entreprises continuent de déplacer de plus en plus de charges de travail vers le cloud, mais ces environnements hybrides et multi-cloud posent des problèmes de sécurité importants en raison du manque de visibilité. La création d'une solution globale avec Gigamon et Vectra AI change la donne en matière de sécurité dans les clouds. Nous serons désormais en mesure d'offrir à nos clients internationaux une solution complète de cyberdéfense pour tous les réseaux cloud, en combinant l'observabilité avancée de Gigamon dont ils ont besoin avec une plateforme de détection, d'investigation et de réponse aux menaces basée sur l'IA de Vectra AI, la meilleure de sa catégorie, le tout en une seule offre. »

Paul Eccleston,
SVP EMEA pour Exclusive Networks

« L'année dernière, nous avons constaté l'impact des nouvelles menaces de cybersécurité, avec la couverture publique des violations, des rançongiciels et des fuites de données. Ces vulnérabilités font de l'observabilité avancée, et de la visibilité Est-Ouest qu'elle offre sur le trafic crypté, une base essentielle pour toutes les opérations organisationnelles, ce qui stimule la demande dans les budgets de sécurité et d'informatique d'aujourd'hui. Gigamon a maintenu une position de leader avec son flux d'observabilité avancée, en adoptant une approche innovante de la sécurisation et de la gestion des infrastructures hybrides modernes. »

Alan Weckel, Fondateur et analyste technologique au 650 Group

Conclusion

Chez Gigamon, notre objectif est de protéger les réseaux hybrides et les données des entreprises les plus grandes et les plus complexes de la planète. Nous sommes obsédés par l'apprentissage, la collaboration et l'innovation afin de fournir des solutions qui protègent les entreprises contre les cybermenaces. Avec l'aide de nos employés, de nos partenaires et de nos clients, nous avons développé un système d'observabilité avancée qui offre le plus haut niveau de sécurité pour les clouds hybrides disponible aujourd'hui.

Laissez Gigamon surcharger vos outils de cloud, de sécurité et d'observabilité en leur donnant quelque chose qu'ils n'ont pas : **une intelligence et des informations exploitables dérivées du réseau.**

En savoir plus sur l'observabilité avancée

Gigamon®

Siège mondial
3300 Olcott Street, Santa Clara, CA 95054 États-Unis
+1 (408) 831-4000 | gigamon.com