Éliminer les angles morts les plus importants avec Precryption™

La technologie Precryption de Gigamon permet d'obtenir une visibilité claire du trafic latéral sur l'ensemble de la couche de sécurité, y compris à l'intérieur des applications virtuelles, en cloud et en conteneur. Aucun déchiffrement n'est nécessaire.

1ère

préoccupation des responsables de la sécurité informatique : ***Utilisation d'angles morts dont vous ne soupçonniez pas l'existence***[2]

91 %

des menaces **utilisent des canaux chiffrés**[3]

81 %

des entreprises ont connu un **incident de sécurité lié au cloud au cours des douze derniers mois**[1]

5x

Les outils de sécurité peuvent être **cinq à sept fois plus efficaces** avec le trafic non chiffré[4].

31 %

des **violations de données survenues l'année dernière n'ont pas été détectées** par les outils de sécurité et d'observabilité[2]

La technologie Precryption™ de Gigamon redéfinit la sécurité des applications virtuelles, en cloud et en conteneur, en offrant une visibilité claire des communications chiffrées sur l'ensemble de la couche de sécurité, sans les coûts et la complexité inhérents au déchiffrement traditionnel.

Enjeux en matière de protection de l'information

1. Adoption croissante du cloud
2. Des équipes de développement rapidement opérationnelles
3. Des menaces cachées

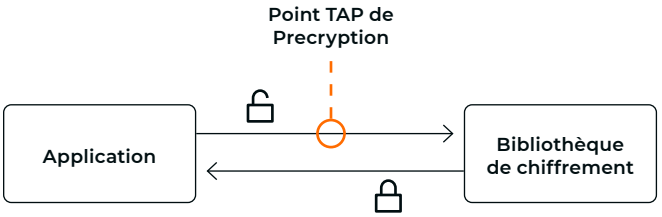
Le recours aux communications chiffrées est presque omniprésent de nos jours dans l'infrastructure cloud hybride moderne, protégeant les données sensibles contre les techniques d'interception classiques. Les cybercriminels ont répondu par de nouvelles approches plus sophistiquées d'infiltration, en compromettant des systèmes clés pour accéder aux données sensibles. Désormais, ces attaquants utilisent les mêmes canaux de communication chiffrés pour camoufler leurs propres activités, en particulier les mouvements latéraux, l'accès aux données sensibles et l'exfiltration. Avec les solutions actuellement proposées sur le marché, il est presque impossible d'obtenir une visibilité claire du trafic chiffré qui circule latéralement entre les workloads virtuels, à tel point où l'on a du mal à détecter les menaces cachées. C'est pourquoi les communications latérales chiffrées constituent le plus grand angle mort en matière de sécurité.

La technologie Precryption révèle les menaces cachées

La technologie Precryption est une solution innovante qui s'attaque à l'angle mort le plus important des infrastructures de cloud hybride d'aujourd'hui, le mouvement latéral utilisé par les cybercriminels, qui est caché par les formes modernes de chiffrement, dont TLS 1.3. Precryption offre une visibilité en claire sur les communications virtuelles chiffrées dans un format efficace et sans perturbation, qui ne nécessite ni déchiffrements dispendieux ni collecte et gestion des clés.

Comment fonctionne la technologie Precryption ?

La technologie Precryption exploite la fonctionnalité native de Linux pour enregistrer ou copier les communications entre l'application et la bibliothèque de chiffrement, telle qu'OpenSSL.



Ainsi, Precryption capture le trafic en clair avant qu'il ne soit chiffré sur le réseau ou après qu'il ait été déchiffré. La fonction Precryption n'entrave pas le chiffrement proprement dit du message ni sa transmission sur le réseau. Par conséquent, il n'y a ni proxy, ni retransmission, ni interception et ni inspection. Au lieu de cela, cette copie en clair est transmise à la solution d'observabilité avancée pour les flux de données de Gigamon qui va l'optimiser, la transformer, la répliquer et la transmettre aux outils.

La technologie Precryption repose sur GigaVUE® Universal Cloud Tap (UCT) et fonctionne dans des environnements hybrides et multi-cloud, y compris sur site et sur des plateformes virtuelles.

En prime, UCT équipé de la technologie Precryption fonctionne indépendamment de l'application et n'a pas besoin d'être inclus dans le cycle de développement de l'application.

Cas d'usage principaux

Déjouer les manœuvres des cybercriminels : Les mouvements latéraux dans le cloud constituent un angle mort qui s'observe surtout dans les cyberattaques. Une fois le périmètre de sécurité franchi, les paquets chiffrés échappent à la surveillance, ce qui permet à un cybercriminel de recourir à toutes sortes d'astuces et de techniques pour ne pas se faire détecter.

Conformité au TLS 1.3 : De nos jours, certaines entreprises tardent à adopter TLS 1.3 en raison du manque de visibilité sur le trafic chiffré. D'autres ont recours à la gestion de solutions de déchiffrement distinctes.

Zero Trust : La capacité de voir les paquets, d'inspecter chaque interaction entre les ressources sur le réseau et d'appliquer une stratégie est indispensable pour l'efficacité d'une architecture de Zero Trust.

Renseignements émanant du réseau : Les outils de sécurité, comme les SIEM, reposent souvent sur la transformation et l'enrichissement des métadonnées pour améliorer la détection des menaces.

Pourquoi utiliser Precryption de Gigamon ?

GigaVUE Universal Cloud Tap équipé de la technologie Precryption est une solution légère et sans perturbation qui élimine les angles morts présents dans l'infrastructure moderne de cloud hybride. Elle offre une visibilité du trafic est-ouest dans les plateformes virtuelles, de cloud et de conteneur. Elle garantit une visibilité totale sur tous les types de chiffrement, dont TLS 1.3, sans se préoccuper de la gestion ou de la conservation des clés de déchiffrement. Les services informatiques peuvent désormais gérer la conformité, préserver la confidentialité des communications privées, mettre en place les bases nécessaires à la Zero Trust, et améliorer l'efficacité des outils de sécurité par un gain d'efficacité de 5 ou plus.

Caractéristiques principales

- **Visibilité en clair des communications avec le chiffrement moderne** (TLS 1.3, mTLS et TLS 1.2 avec Confidentialité de transmission parfaite)
- **Visibilité en clair des communications avec le chiffrement traditionnel** (TLS 1.2 et versions antérieures)
- **Accès au trafic sécurisé** sans l'exécution d'agents à l'intérieur des workloads des conteneurs
- **Élimination de la consommation de ressources dispendieuses** associée au déchiffrement traditionnel du trafic
- **Élimination de la gestion des clés** requises pour le déchiffrement traditionnel du trafic
- **Aucun impact sur les performances** en fonction du type, de la puissance ou de la version du chiffrement.
- **Prise en charge des environnements hybrides et multi-cloud,** y compris les plateformes sur site, virtuelles et de conteneurs.
- **Préservation de la confidentialité des communications privées** sur le réseau grâce à la transmission des menaces en texte en clair aux outils de sécurité.
- **Intégration avec l'observabilité avancée Gigamon pour les flux de données** pour bénéficier de la suite complète de fonctions d'optimisation, de transformation et d'intermédiation.

Principaux avantages

- **Éliminer les angles morts** des communications chiffrées du trafic est-ouest (latéral) et nord-sud, y compris le trafic ne pouvant pas traverser les pare-feu.
- **Surveiller les communications des applications** avec une approche indépendante qui améliore la réactivité de l'équipe de développement.
- **Étendre la visibilité des outils de sécurité** à toutes les communications, quel que soit le type de chiffrement
- **Optimiser l'interception du trafic** dans les environnements virtuels
- Faire croître de 5 à 7 fois les performances des outils de sécurité grâce à la consommation des données non chiffrées
- **Prendre en charge une architecture Zero Trust** basée sur l'observabilité avancée
- **Protéger la vie privée** et assurer la conformité en matière de gestion du trafic non chiffré

Enjeux : Regard détaillé

Les services informatiques se heurtent à trois grands enjeux pour sécuriser les systèmes et les données qu'ils sont chargés de protéger : l'adoption croissante du virtuel et du cloud, l'obligation pour les équipes de développement d'agir rapidement et les menaces cachées.

1. Adoption croissante du virtuel et du cloud

81 % des entreprises ont connu un incident de sécurité lié au cloud au cours des douze derniers mois[1]

Cette évolution vers des systèmes virtualisés (sur site, cloud privé ou cloud public, MV ou conteneur) ne cesse de s'accélérer et ne présente aucun signe de ralentissement. Ces architectures modernes sont conçues pour être efficaces sur le plan opérationnel et se sont développées beaucoup plus vite que les architectures de sécurité fondées sur le périmètre. La détection des mouvements latéraux est très complexe. Certaines entreprises sortent du cadre en autorisant la circulation des communications chiffrées dans leur infrastructure de Cloud hybride ; d'autres essaient d'accroître leur architecture virtuelle en déployant des pare-feu supplémentaires, au point de renoncer à l'efficacité souhaitée au profit de la sécurité. Et lorsque la majorité des entreprises se dotent de plusieurs plateformes virtuelles, les difficultés et les risques se multiplient.

2. Des équipes de développement rapidement opérationnelles

83 % des entreprises ont adopté le principe de la responsabilité collective entre les équipes de l'informatique et de la sécurité[2]

Les équipes de développement logiciel sont particulièrement encouragées à développer des applications qui contribuent à la croissance du chiffre d'affaires ou qui aident l'entreprise à gagner du temps et économiser de l'argent. Alors qu'elles sont sans cesse tenues de respecter les délais, les équipes DevOps se concentrent davantage sur leurs missions propres. Dans une certaine mesure, elles peuvent accorder une grande importance à la sécurité, mais elles ne sont généralement pas spécialisées dans la prévention des intrusions et ne connaissent pas nécessairement les vulnérabilités qui pourraient être introduites. En outre, elles pourraient préférer ne pas déployer des agents de sécurité dans leurs logiciels et leurs systèmes, car les agents peuvent gêner les tests et augmenter les efforts et le temps requis pour le développement logiciel. Les entreprises de sécurité ont diverses façons de résoudre ce problème. Certains se soumettent à des exercices rigoureux de conformité et appliquent des agents dans chaque code, d'autres intègrent des responsables de la sécurité dans les équipes de développement, et d'autres encore n'ont d'autre choix que de laisser les développeurs accélérer l'opérationnalisation sans une surveillance rigoureuse de la sécurité. Toutefois, la grande majorité confie au moins une partie de la responsabilité de la sécurité aux équipes de développement.

3. Des menaces cachées

91 % des menaces utilisent des canaux chiffrés[3]

Les communications chiffrées sont d'un grand intérêt pour prévenir certaines menaces, mais elles en favorisent d'autres. Il est en effet habituel que les cybercriminels suppriment, désactivent et/ou modifient les journaux en premier lieu lorsqu'ils accèdent à un système. Viennent ensuite les appels vers un serveur de commande et de contrôle, les réaffectations de privilèges, les mouvements latéraux, la copie secrète de données et, enfin, l'exfiltration de données, le tout au moyen de communications chiffrées.

Les outils de sécurité peuvent être 5 à 7 fois moins efficaces lorsque le trafic est chiffré[4]

On pourrait diviser les méthodes de chiffrement courantes en deux catégories :

- **Le chiffrement moderne,** qui utilise la confidentialité de transmission parfaite (PFS) pour empêcher le déchiffrement par interception et inspection des communications interceptées, car chaque clé de chiffrement interceptée est éphémère et inutile en cas de déchiffrement hors bande. Le chiffrement moderne inclut TLS 1.3, mTLS et certains déploiements de TLS 1.2 pour lesquels la fonction PFS peut être éventuellement activée. Gigamon estime qu'environ 30 à 40 % du trafic réseau utilise aujourd'hui un chiffrement moderne et que cela va continuer à s'accentuer.

- **Le chiffrement traditionnel,** qui n'utilise pas la fonction PFS et peut être déchiffré au moyen d'une clé interceptée. Cela inclut certains déploiements de TLS 1.2 et d'anciennes versions de TLS et de SSL (Secure Sockets Layer).

Il existe des outils de sécurité capables de surveiller les réseaux dont les communications sont chiffrées. Dans le cas d'un chiffrement traditionnel, ces outils essaient généralement de déchiffrer eux-mêmes le trafic. Il s'agit d'une proposition qui nécessite d'énormes calculs et qui a un impact significatif sur les performances, avec beaucoup plus de « champs » pour répondre aux besoins de traitement. En outre, les bibliothèques de clés sous-jacentes doivent être constamment mises à jour, et la gestion des clés est une tache complexe qui nécessite beaucoup de temps. Mais même avec cela, elle ne se limite qu'au chiffrement traditionnel et ne tient pas compte du chiffrement moderne.

Pour le chiffrement moderne, ces outils doivent adopter une approche différente, car les communications ne peuvent pas être déchiffrées quand elles « sont en cours ». Ils ajoutent donc des en-têtes de paquets, leur taille et leur fréquence, ainsi que d'autres signatures dans des algorithmes d'apprentissage automatique afin d'évaluer le risque d'une communication donnée. Même si ces résultats valent mieux que rien, le bilan est, au mieux, mitigé. Cela pousse ainsi certaines entreprises à ne surveiller que le chiffrement traditionnel, à ne faire confiance qu'à la sécurité basée sur le périmètre ou à exclure le chiffrement moderne de leurs applications, or aucune de ces stratégies n'est idéale en matière de sécurité.

Une enquête récente menée auprès de plus de 1 000 responsables informatiques et de la sécurité a révélé que 31 % des violations de données n'ont pas été détectées par les outils de sécurité et d'observabilité.

Des solutions plus efficaces s'imposent.

Solution Precryption : Un peu plus de détails

Désormais équipé de la technologie Precryption, GigaVUE Universal Cloud Tap (UCT) élimine les angles morts des communications chiffrées au sein des environnements virtuels et de conteneurs, permettant ainsi aux responsables informatiques et de la sécurité de reprendre le contrôle.

GigaVUE UCT est un TAP virtuel moderne qui exploite la technologie eBPF au sein du noyau Linux. Il est considéré comme la technique la plus efficace pour reproduire les communications dans un environnement virtuel. UCT capture les données non chiffrées et les transmet efficacement au flux d'observabilité avancée Gigamon, en vue de leur optimisation, transformation, filtrage et intermédiation, avant de finalement transmettre les bonnes données aux bons outils, qu'ils soient physiques ou virtuels.

La technologie Precryption de Gigamon repose sur GigaVUE UCT et s'intègre en toute transparence à Linux et aux bibliothèques de chiffrement telles que OpenSSL. Elle capture ainsi les communications au sein d'environnements virtuels et de conteneurs avant qu'elles ne soient chiffrées sur le réseau ou après qu'elles aient été déchiffrées pour certaines applications.

- ✓ Les communications réseau sont intactes, préservées et restent chiffrées à travers le réseau.
- ✓ Le déchiffrement ne nécessite pas d'énormes calculs. Ainsi, la technologie Precryption exploite les chiffrements moderne et traditionnel et n'est pas affecté par le type, la force ou la version du chiffrement.
- ✓ En effet, cette technologie ne présente pas de clés d'application exposées, de problèmes de gestion des clés d'application et d'itinéraires virtuels artificiels.
- ✓ La technologie Precryption fonctionne indépendamment de l'application surveillée, éliminant ainsi tout impact sur les ressources et la gestion du cycle de vie de l'application et n'entraînant aucune défaillance au sein de l'application.

Fonctionnement de la technologie Precryption de Gigamon : Nœud unique (figure 1)

1. Lorsqu'une application doit chiffrer un message, elle utilise une bibliothèque de chiffrement, telle qu'OpenSSL, pour effectuer le chiffrement proprement dit.

2. GigaVUE Universal Cloud Tap (UCT), équipé de la technologie Precryption, reçoit une copie de ce message avant qu'il ne soit chiffré sur le réseau.

3. Le message chiffré est envoyé à l'application destinataire, avec un chiffrement non modifiable. Aucun proxy, aucun rechiffrement et aucune retransmission ne sont nécessaires.

4. GigaVUE UCT crée des en-têtes de paquets si nécessaire, les encapsule dans un tunnel et les transmet à GigaVUE V Series dans le flux d'observabilité avancée. Gigamon optimise, transforme et transmet les données aux outils, sans devoir recourir à un nouveau déchiffrement.

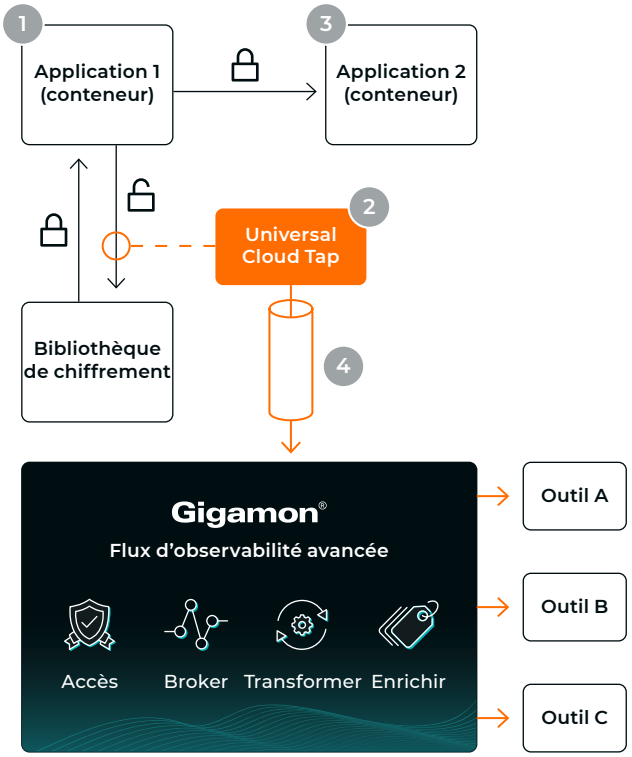


Figure 1

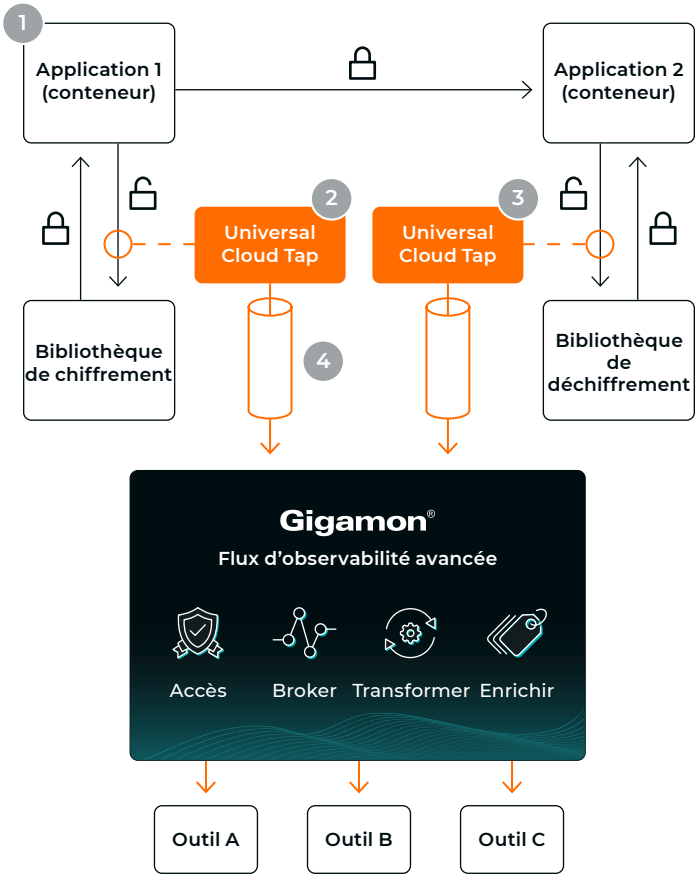


Figure 2

Fonctionnement de la technologie Precryption de Gigamon : Multi-nœuds (figure 2)

1. Lorsqu'une application doit chiffrer un message, elle utilise une bibliothèque de chiffrement, telle qu'OpenSSL, pour effectuer le chiffrement proprement dit.

2. GigaVUE Universal Cloud Tap (UCT), équipé de Precryption, reçoit une copie de ce message avant qu'il ne soit chiffré sur le réseau.

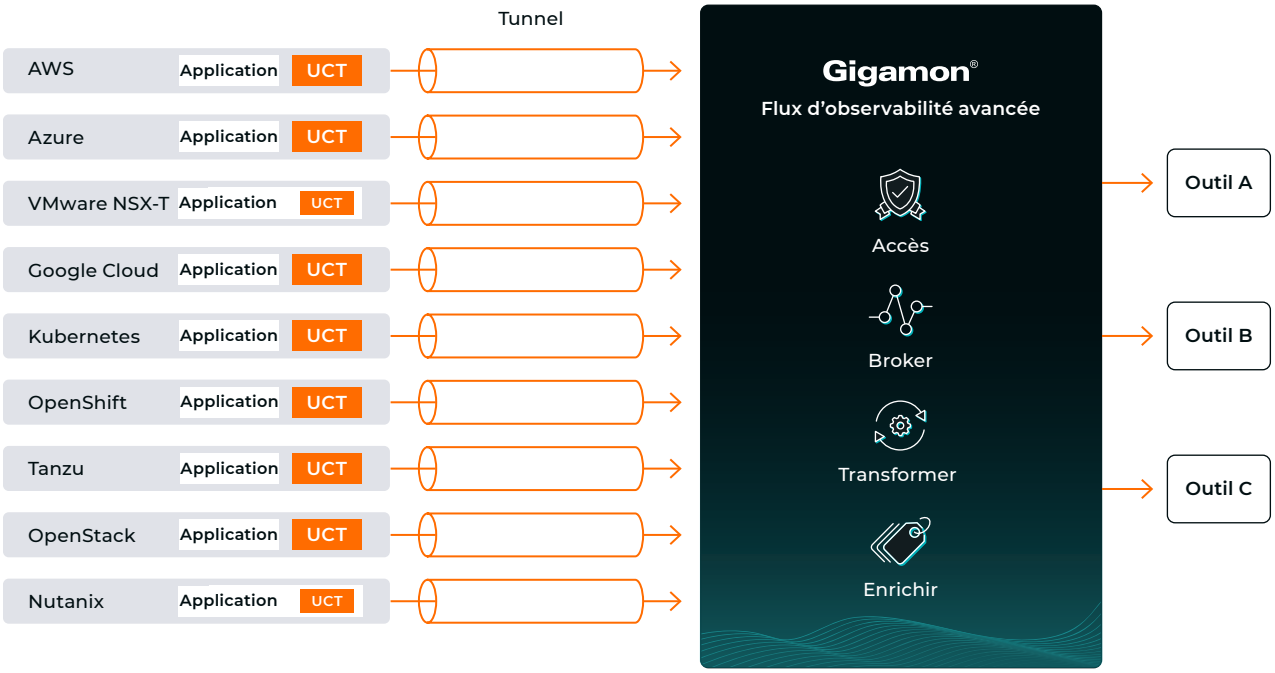
3. Il est éventuellement possible que GigaVUE UCT équipé de Precryption capture également une copie du message à partir du serveur à l'issue du déchiffrement.

4. GigaVUE UCT crée des en-têtes de paquets si nécessaire, les encapsule dans un tunnel et les transmet à V Series dans le flux d'observabilité avancée, où ils sont enrichis, transformés et transmis aux outils, sans devoir recourir à un nouveau déchiffrement.

Fonctionne pour les environnements multi-cloud et à grande échelle

GigaVUE UCT équipé de la technologie Precryption fonctionne sur plusieurs plateformes virtuelles et cloud, notamment VMware, AWS, Microsoft Azure, OpenStack, Google Cloud, Nutanix, etc. Il alimente un pipeline de données commun à l'aide d'une seule interface de gestion globale.

- ✓ Prise en charge du déploiement automatique dans Kubernetes pour simplifier l'évolutivité.
- ✓ Un pool de licences partagées pour tous les environnements cloud ; un nombre illimité d'instances



GigaVUE UCT fonctionne indépendamment de l'application

Le terme « agent » peut avoir des significations différentes selon le contexte. Examinez le tableau suivant pour comprendre les avantages d'UCT par rapport aux agents classiques.

Agents classiques	GigaVUE UCT
X S'exécute dans l'espace ou le bloc d'applications	✓ Espace utilisateur indépendant dans un bloc indépendant
X Affecte l'utilisation des ressources de l'application	✓ Ressources de nœuds indépendants
X Nécessite des mises à niveau de version coordonnées	✓ Mises à niveau indépendantes
X Nécessite des tests en même temps que l'application	✓ Gestion indépendante du cycle de vie
X Peut introduire une latence dans l'application	✓ Capture indépendante
X Peut introduire une instabilité ou une panne à l'arrêt	✓ Domaine de défaillance indépendant

Ajouter des renseignements provenant du réseau pour améliorer la stratégie de sécurité pendant que les développeurs opèrent rapidement

Après l'extraction des données non chiffrées, le flux d'observabilité avancée Gigamon peut être mis à profit pour transformer les données de communication brutes en enregistrements de métadonnées au niveau du flux. Cela permet de réduire les faux positifs, de faciliter l'identification des activités malveillantes telles que l'usurpation de port, et d'accélérer la détection des menaces en ayant recours à une surveillance proactive en temps réel plutôt qu'à une analyse médico-légale réactive. Ces renseignements provenant du réseau ne font pas l'objet d'une modification des journaux. Ils s'utilisent pour l'IdO et d'autres appareils sans agent, et alimentent les outils d'observabilité utilisés par les équipes SecOps et DevOps.

Pour les environnements ultrasensibles, UCT peut éventuellement rechiffrer les communications reproduites destinées au flux d'observabilité avancée, et masquer les données sensibles, notamment celles des cartes de crédit, ou les informations personnelles

identifiables (PII) avant de les transmettre aux outils.

Cas d'usage

Détecter les cybercrimes à l'aide de la technologie Precryption

Une attaque cybercriminelle, également appelée attaque par ransomware, commence généralement lorsqu'un cybercriminel accède hors réseau à l'ordinateur portable d'un employé, par hameçonnage ou par toute autre technique de collecte d'informations d'identification. Il faut espérer que la sécurité des points d'accès permette de détecter ou d'éviter ce genre de situation. Malheureusement, ce n'est pas toujours le cas.
Une fois infiltré dans le réseau, un cybercriminel a plusieurs ressources à sa disposition, notamment des techniques sophistiquées pour supprimer les journaux, réaffecter ses privilèges et rechercher d'autres ressources réseau plus intéressantes, telles que des hôtes, des applications, des charges de travail, etc. contenant des données plus sensibles. Avec suffisamment de temps et de vecteurs d'attaque, il pourra infiltrer ces autres ressources réseau. Cette technique est appelée mouvement latéral.

Les cybercriminels finiront par se frayer un chemin vers des applications plus intéressantes, où les données sont exposées et les communications espionnées. Le cybercriminel détournera lentement les données vers un emplacement de destination dans le réseau, qu'il contrôle. Ce détournement se fait avec beaucoup de soin pour éviter d'affecter les performances ou de déclencher des alarmes. Lorsqu'il a récupéré suffisamment de données et qu'il est prêt, le cybercriminel déclenche un dernier événement d'exfiltration de données rapide et à grande échelle, afin d'exporter les données volées vers des systèmes externes et d'extorquer ensuite de l'argent à l'entreprise affectée.

Il ressort de ce récit que le cybercriminel a effectué quatre grands types d'activités :

1. Hameçonnage initial ou récupération d'informations d'identification pour contourner la sécurité du point d'accès
2. Mouvement latéral au sein du réseau
3. Détournement lent des données sensibles vers un emplacement de destination
4. Exfiltration rapide des données

Voici un aperçu de la façon dont la visibilité en clair via la technologie Precryption de Gigamon aide les outils à détecter cette activité :

	Ce qu'un outil de sécurité peut déceler s'il n'est pas équipé de Precryption	**Ce qu'un outil de sécurité peut déceler s'il est équipé de Precryption**
Hameçonnage initial	Activités régulières des employés	Activités régulières des employés
Mouvement latéral	Bruit anodin	Une attaque connue a été déployée et l'attaquant a réussi à s'infiltrer dans le serveur
Siphonnage de données	Bruit anodin	Les données VIP sont consultées et transmises sur des canaux non autorisés
Exfiltration de données	Gros transfert de données	Comptabilité détaillée des pertes subies

Pour une présentation détaillée du contexte de cybercriminalité, téléchargez l'infographie.

Conclusion

L'amélioration de la visibilité sur le trafic chiffré et les métadonnées renforce considérablement la sécurité, la surveillance et le traitement des incidents des environnements cloud hybrides. L'observabilité avancée pour les flux de données de Gigamon s'attaque directement aux enjeux d'aujourd'hui en matière de sécurité pour la surveillance du trafic entre les plateformes virtuelles et les conteneurs, tant sur site que sur le cloud public. GigaVUE UCT répond à l'adoption croissante du cloud en renforçant la prise en charge des plateformes et en utilisant une interface de gestion unique. Les renseignements provenant du réseau Gigamon alimentent en métadonnées de qualité les outils de sécurité des équipes DevOps, CloudOps et SecOps. La technologie Precryption de Gigamon s'attaque désormais au problème particulièrement épineux de la surveillance des activités cachées dans le cloud. Pour ce faire, elle utilise un chiffrement moderne, harmonieux et léger, afin d'améliorer la stratégie de sécurité et d'empêcher les malfaiteurs de s'infiltrer dans l'entreprise.

À propos de Gigamon

Gigamon propose une observabilité avancée pour les flux de données qui repose sur les renseignements provenant du réseau pour étendre les fonctionnalités des outils d'observabilité. Cette puissante combinaison permet aux services informatiques de garantir le respect des normes de sécurité et de gouvernance de la conformité, d'accélérer l'analyse des causes profondes des engorgements de performance, et de réduire les coûts opérationnels associés à la gestion des infrastructures informatiques hybrides et multi-cloud. Résultat : les entreprises d'aujourd'hui réalisent pleinement les promesses de transformation du cloud. Gigamon compte plus de 4 000 clients dans le monde, dont plus de 80 % des entreprises du classement Fortune 100, neuf des dix plus grands fournisseurs de réseaux mobiles et des centaines de gouvernements et d'organismes d'enseignement. Pour plus d'informations, veuillez consulter le site gigamon.com.

1. Shelley Boose. 81 % des entreprises ont connu un incident de sécurité lié au cloud au cours des douze derniers mois. Venafi, 28 septembre 2022. https://venafi.com/blog/81-companies-have-had-had-cloud-security-incident-last-year-venafi-research.
2. 2023 Hybrid Cloud Security Survey: Perception vs. Reality. Gigamon, 2023. https://www.gigamon.com/content/dam/gated/wp-gigamon-survey-hybrid-cloud-security-2023.pdf.
3. Internet Security Report – Q2 2021. Watchguard, 2021. https://www.watchguard.com/wgrd-resource-center/security-report-q2-2021.
4. Deepen Desai. Encrypted Attacks Rise 314%: New ThreatLabz State of Encrypted Attacks Report. Zscaler, 28 octobre 2021. https://www.zscaler.com/blogs/security-research/encrypted-attacks-rise-314.

Gigamon®

Siège mondial
3300 Olcott Street, Santa Clara, CA 95054 États-Unis
+1 (408) 83 - 4000 | gigamon.com

09.23_01