Beseitigen der größten Schwachstelle mit Precryption™

Die Precryption-Technologie von Gigamon liefert Plaintext-Transparenz des lateralen Datenverkehrs für den gesamten Sicherheits-Stack, einschließlich virtueller, Cloud- und Container-Systeme. Keine Entschlüsselung erforderlich.

Rang 1

auf der Liste der Probleme von IT-Sicherheitsverantwortlichen: ***Schwachstellen, die Ihnen nicht bekannt waren, werden ausgenutzt***[2]

91 %

der Bedrohungen **nutzen verschlüsselte Kanäle**[3]

81 %

der Unternehmen verzeichneten **im letzten Jahr einen Sicherheitsvorfall in der Cloud**[1]

5x

Security-Tools können bei unverschlüsseltem Datenverkehr **fünf- bis siebenmal effektiver** arbeiten[4]

31 %

der **Datenschutzverletzungen im letzten Jahr wurden von Sicherheits- und Überwachungstools nicht bemerkt**[2]

Die Precryption™-Technologie von Gigamon definiert die Sicherheit für virtuelle, cloudbasierte und containerisierte Anwendungen neu: Sie liefert dem gesamten Sicherheits-Stack Plaintext-Einblicke in verschlüsselte Kommunikation, ohne die gewohnten Kosten und die Komplexität von Entschlüsselungsverfahren.

Herausforderungen für die Informationssicherheit

1. Zunehmende Verbreitung der Cloud
2. Produktivität der Entwicklungsteams
3. Verborgene Bedrohungen

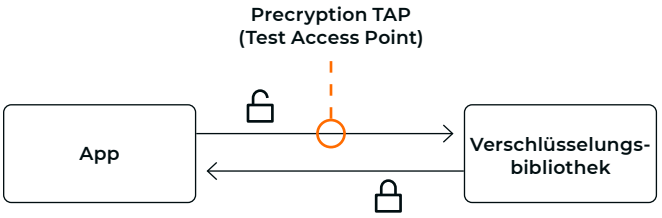
Der Einsatz verschlüsselter Kommunikation ist heutzutage in modernen hybriden Cloud-Infrastrukturen nahezu allgegenwärtig und schützt sensible Daten vor herkömmlichen Angriffsmethoden. Bedrohungsakteure haben darauf mit neuen, ausgefeilteren Ansätzen zur Infiltration reagiert: Sie kompromittieren Schlüsselsysteme, um Zugang zu sensiblen Daten zu erhalten. Die Eindringlinge nutzen nun dieselben verschlüsselten Kommunikationskanäle, um ihre eigenen Aktivitäten, wie Lateral Movement, Zugriff auf sensible Daten und Exfiltration, zu verschleiern. Die Erlangung von Plaintext-Transparenz bei verschlüsseltem Datenverkehr, der sich lateral zwischen virtuellen Workloads bewegt, ist mit den vorhandenen Lösungen auf dem Markt nahezu unmöglich. Dies erschwert die Erkennung von verborgenen Bedrohungsaktivitäten massiv. Aus diesem Grund ist die chiffriert laterale Kommunikation nach wie vor der größte Schwachpunkt im Hinblick auf die Cybersicherheit.

Precryption-Technologie erkennt verborgene Bedrohungen

Die Precryption-Technologie ist eine innovative Lösung, die sich direkt mit dem größten Schwachpunkt der heutigen hybriden Cloud-Infrastruktur befasst: der lateralen Bewegung von Bedrohungsakteuren durch das Netzwerk (Lateral Movement). Diese wird durch moderne Formen der Verschlüsselung , einschließlich TLS 1.3, verschleiert. Precryption bietet Plaintext-Einblicke in die verschlüsselte virtuelle Kommunikation mit einem effizienten, reibungslos integrierbaren Verfahren, ohne teure Entschlüsselungen und aufwändige Schlüsselerfassung und -verwaltung zu erfordern.

Wie funktioniert die Precryption-Technologie?

Die Precryption-Technologie nutzt native Linux-Funktionen, um die Kommunikation zwischen der Anwendung und der Verschlüsselungsbibliothek (z. B. OpenSSL) abzugreifen bzw. zu kopieren.



Auf diese Weise erfasst Precryption den Netzwerkverkehr als „Plaintext“. Dieser Begriff bezieht sich auf Text, der entweder das Ergebnis einer Entschlüsselung ist oder vor der Übertragung oder Speicherung noch verschlüsselt werden soll. Die Precryption-Funktion greift weder in die eigentliche Verschlüsselung der Nachricht noch in deren Übertragung über das Netzwerk ein. Es gibt keinen Proxy, keine erneuten Übertragungen, kein Unterbrechen und Untersuchen. Stattdessen wird die Plaintext-Kopie zur weiteren Optimierung, Umwandlung, Replikation und Bereitstellung an Tools an die Gigamon Deep Observability Pipeline weitergeleitet.

Die Precryption-Technologie basiert auf GigaVUE® Universal Cloud Tap (UCT) und eignet sich für hybride und Multi-Cloud-Umgebungen, einschließlich vor Ort und auf virtuellen Plattformen.

Als zusätzlicher Bonus wird UCT mit Precryption-Technologie unabhängig von der Anwendung ausgeführt und muss nicht in den Lebenszyklus der Anwendungsentwicklung integriert werden.

Wichtige Anwendungsfälle

Vereiteln von Cyberkriminalität: Lateral Movement in der Cloud ist ein Schwachpunkt, der gerne bei Angriffen durch Cyberkriminelle ausgenutzt wird. Sobald diese die Perimeter-Sicherheitsbarriere überwunden haben, werden verschlüsselte Datenpakete nicht mehr überwacht. Daher kann ein Bedrohungsakteur alle möglichen Tricks und Techniken anwenden, um unentdeckt zu bleiben.

TLS 1.3-Compliance: Einige Unternehmen haben die notwendige Einführung des Verschlüsselungsprotokolls TLS 1.3 verzögert, weil sie damit keinen Einblick in den verschlüsselten Datenverkehr haben. Andere haben auf die Verwaltung separater Entschlüsselungslösungen zurückgegriffen.

Zero Trust: Eine wichtige Grundlage für eine effektive Zero-Trust-Architektur ist die Fähigkeit, Datenpakete zu sehen, jede Interaktion zwischen den Ressourcen im Netzwerk zu überprüfen und Richtlinien anzuwenden.

Aus dem Netzwerk abgeleitete Informationen: Sicherheitstools wie SIEMs sind oft darauf angewiesen, Metadaten umzuwandeln und anzureichern, um Bedrohungen besser zu erkennen.

Warum Gigamon Precryption?

GigaVUE Universal Cloud Tap mit Precryption-Technologie ist eine kompakte, reibungslos integrierbare Lösung, die Schwachpunkte in modernen hybriden Cloud-Infrastrukturen beseitigt und Einblicke in lateralen Datenverkehr auf virtuellen, Cloud- und Container-Plattformen bietet. Sie erhalten einen ungetrübten Einblick in alle Verschlüsselungsarten, einschließlich TLS 1.3, ohne Entschlüsselungsschlüssel verwalten und pflegen zu müssen. IT-Organisationen können nun die Einhaltung von Vorschriften sicherstellen, private Kommunikation geheim halten, die notwendige Grundlage für Zero-Trust-Architektur schaffen und die Effektivität von Sicherheitstools um mindestens das 5-fache steigern.

Wesentliche Merkmale

- **Plaintext-Einblicke in Kommunikation mit moderner Verschlüsselung** (TLS 1.3, mTLS und TLS 1.2 mit Perfect Forward Secrecy)
- **Plaintext-Einblicke in Kommunikation mit älterer Verschlüsselung** (TLS 1.2 und früher)
- **Nicht-intrusiver Zugriff** auf den Datenverkehr ohne Agents, die in Container-Workloads ausgeführt werden
- **Eliminierung von kostspieligem Ressourcenverbrauch** im Zusammenhang mit der herkömmlichen Entschlüsselung des Datenverkehrs
- **Keine Schlüsselverwaltung,** die bei der herkömmlichen Entschlüsselung des Datenverkehrs erforderlich ist
- **Keine Auswirkungen auf die Leistung,** auch bei verschiedenen Verschlüsselungstypen, -stärken und -versionen
- **Unterstützung für hybride und Multi-Cloud-Umgebungen,** einschließlich On-Premise-, virtueller und Container-Plattformen
- **Schutz der privaten Kommunikation** im Netzwerk mit Weitergabe von Plaintext-Bedrohungsaktivitäten an Sicherheitstools
- **Integration mit Gigamon Deep Observability Pipeline** zur Nutzung der gesamten Palette an Optimierungs-, Transformations- und Brokering-Funktionen

Wichtigste Vorteile

- **Beseitigung von Schwachstellen** der verschlüsselten lateralen und externen Kommunikation, einschließlich des Datenverkehrs, der keine Firewalls passiert
- **Überwachung von Anwendungskommunikation** mit einem unabhängigen Ansatz, der die Produktivität des Entwicklungsteams erhöht
- **Erweiterung der Transparenz von Sicherheitstools** auf die gesamte Kommunikation, unabhängig vom Verschlüsselungstyp
- **Maximale Effizienz beim Abgreifen des Datenverkehrs** in virtuellen Umgebungen
- **Steigerung der Leistung von Sicherheitstools um das 5- bis 7-fache** durch die Nutzung unverschlüsselter Daten
- **Unterstützung einer Zero-Trust-Architektur,** die auf tiefgreifender Überwachung beruht
- **Einhaltung von Datenschutzrichtlinien** und Compliance in Bezug auf die Verwaltung von entschlüsseltem Datenverkehr

Die Herausforderungen im Detail

IT-Organisationen stehen bei der Sicherung der Systeme und Daten, mit deren Schutz sie betraut sind, vor drei großen Herausforderungen: die zunehmende Verbreitung von virtuellen und cloudbasierten Systemen, die Anforderungen an die Produktivität der Entwicklungsteams und verborgene bedrohliche Aktivitäten.

1. Zunehmende Verbreitung von Virtualität und Cloud

81 Prozent der Unternehmen verzeichneten im letzten Jahr einen Sicherheitsvorfall in der Cloud[1]

Der Trend zu virtualisierten Systemen, wie standortgebundene, private oder öffentliche Cloud, VMs oder Container, nimmt weiter zu und zeigt kaum Anzeichen einer Verlangsamung. Diese modernen Architekturen sind auf betriebliche Effizienz ausgelegt und entwickeln sich größtenteils rascher als Perimeter-basierte Sicherheitsarchitekturen. Lateraler Datenverkehr im Netzwerk (Lateral Movement) ist sehr schwer zu erkennen. Einige Unternehmen gehen ein kalkuliertes Risiko ein, indem sie die verschlüsselte Kommunikation über ihre hybride Cloud-Infrastruktur laufen lassen, während andere versuchen, die virtuelle Architektur durch den Einsatz zusätzlicher Firewalls zu erweitern, und dabei Sicherheit Vorrang vor Effizienz einräumen. Wenn Unternehmen nun mehrere virtuelle Plattformen nutzen, vervielfachen sich diese Herausforderungen und Risiken entsprechend.

2. Produktivität der Entwicklungsteams

83 Prozent der Unternehmen haben eine gemeinsame Verantwortung der IT- und Sicherheitsteams eingeführt[2]

Software-Entwicklungsteams werden generell angeregt, Anwendungen zu entwickeln, die zur Umsatzsteigerung beitragen oder dem Unternehmen Zeit und Geld sparen. Da die DevOps-Teams ständig unter Zeitdruck stehen, konzentrieren sie sich auf ihre Kernaufgabe. Sie kümmern sich zwar bis zu einem gewissen Grad um die Sicherheit, sind aber in der Regel keine Experten, was die Verhinderung von Angriffen angeht, und wissen auch nicht, wo es Schwachstellen geben kann. Darüber hinaus sträuben sie sich möglicherweise gegen den Einsatz von Sicherheitsagents in ihrer Software und ihren Systemen, da Agents das Testen erschweren und den Lebenszyklus der Softwareentwicklung verlängern können.

Sicherheitsorganisationen gehen dieses Problem anders an. Einige führen strenge Verfahren zur Einhaltung der Vorschriften durch und fordern Agents in allen Codes, andere binden Sicherheitsbeauftragte in die Entwicklungsteams ein und wieder andere haben keine andere Wahl, als den Entwicklern zu erlauben, ohne strenge Sicherheitsaufsicht so schnell und produktiv wie möglich zu arbeiten. Die überwiegende Mehrheit überträgt jedoch zumindest ein gewisses Maß an Sicherheitsverantwortung auf die Entwicklerteams.

3. Verborgene Bedrohungen

91 Prozent der Bedrohungen nutzen verschlüsselte Kanäle[3]

Verschlüsselte Kommunikation eignet sich hervorragend, um einigen Bedrohungen vorzubeugen – aber macht andere erst möglich. Es ist gängige Praxis unter den Bedrohungsakteuren, die Zugang zu einem System erlangt haben, als erstes die Protokolle zu löschen, zu deaktivieren und/oder zu verändern. Darauf folgen Aufrufe an einen Command-and-Control-Server, Rechteausweitung, Lateral Movement, heimliches Kopieren von Daten und schließlich die Exfiltration der Daten – und all das unter Verwendung verschlüsselter Kommunikation.

Sicherheitstools sind bei verschlüsseltem Datenverkehr unter Umständen 5- bis 7-mal weniger effektiv[4]

Die gängigen Verschlüsselungsmethoden lassen sich in zwei Kategorien einteilen:

- **Moderne Verschlüsselung,** die Perfect Forward Secrecy (PFS) verwendet, um die Entschlüsselung durch Unterbrechen und Untersuchen (Break-and-Inspect) von abgefangener Kommunikation zu verhindern. Basis hierfür ist, dass alle abgefangenen Verschlüsselungsschlüssel flüchtig und für eine Out-of-Band-Entschlüsselung wertlos sind. Zu den modernen Verschlüsselungsmethoden gehören TLS 1.3, mTLS und einige Implementierungen von TLS 1.2, bei denen PFS optional aktiviert werden kann. Gigamon schätzt, dass derzeit etwa 30–40 Prozent des Netzwerkverkehrs moderne Verschlüsselung nutzen, und dieser Anteil wird weiter wachsen.

- **Veraltete Verschlüsselung,** die kein PFS verwendet und mit einem abgefangenen Schlüssel entschlüsselt werden kann. Dazu gehören einige Bereitstellungen von TLS 1.2 und ältere Versionen von TLS und SSL (Secure Sockets Layer).

Es gibt Sicherheitstools, die Netzwerke mit verschlüsselter Kommunikation überwachen können. Bei der herkömmlichen und mittlerweile veralteten Verschlüsselung versuchen diese Tools in der Regel, den Datenverkehr selbst zu entschlüsseln. Dies ist ein rechenintensives Unterfangen, das erhebliche Auswirkungen auf die Leistung hat, da viel mehr Anforderungen an die Verarbeitung erfüllt werden müssen. Außerdem müssen die zugrunde liegenden Schlüsselbibliotheken ständig aktualisiert werden und die Schlüsselverwaltung gestaltet sich zeitaufwändig und komplex. Dennoch befassen sich diese Tools nur mit veralteter Verschlüsselung, während die moderne Verschlüsselung ignoriert wird.

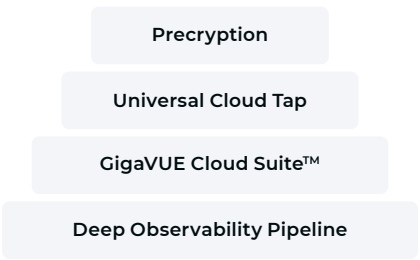
Bei moderner Verschlüsselung muss ein anderen Ansatz verwendet werden, da die Kommunikation nicht „mittendrin" entschlüsselt werden kann. Daher werden Header, Größe, Dichte und andere Signaturen der Datenpakete in Algorithmen für maschinelles Lernen eingegeben, um das Risiko einer bestimmten Kommunikation zu bewerten. Dies ist zwar besser als nichts, aber die Ergebnisse sind bestenfalls gemischt, was einige Unternehmen dazu veranlasst hat, entweder nur die alte Verschlüsselung zu überwachen, sich auf die Perimeter-basierte Sicherheit zu verlassen oder die moderne Verschlüsselung aus ihren Anwendungen zu verbannen. Allerdings stellt nichts davon eine ideale Sicherheitsmaßnahme dar.

In einer kürzlich durchgeführten Umfrage unter mehr als 1.000 IT- und Sicherheitsverantwortlichen wurde zugegeben, dass 31 Prozent der Datenschutzverletzungen nicht von den Sicherheits- und Überwachungstools entdeckt wurden.

Es werden bessere Lösungen benötigt.

Die Precryption-Lösung im Detail

GigaVUE Universal Cloud Tap (UCT) beinhaltet jetzt Precryption-Technologie und beseitigt Schwachstellen in der verschlüsselten virtuellen und Container-Kommunikation, sodass IT- und Sicherheitsverantwortliche die Kontrolle über ihre Daten zurückerlangen.
GigaVUE UCT ist ein moderner virtueller TAP (Test Access Point), der die native Linux eBPF-Technologie nutzt. Diese wurde als die effizienteste Methode zur Spiegelung der Kommunikation in einer virtuellen Umgebung entwickelt. UCT erfasst die unverschlüsselten Daten und liefert sie effizient an die Gigamon Deep Observability Pipeline, wo weitere Optimierungen, Transformationen, Filterungen und Brokering-Vorgänge stattfinden, um letztendlich die richtigen Daten an die richtigen Tools zu liefern, egal ob physisch oder virtuell.



Die Gigamon Precryption-Technologie basiert auf GigaVUE UCT und lässt sich nahtlos in Linux und Verschlüsselungsbibliotheken wie OpenSSL integrieren, um virtuelle und Container-Kommunikation vor der Verschlüsselung über das Netzwerk zu erfassen.
Bei einigen Anwendungen werden Daten erfasst, nachdem sie über das Netzwerk entschlüsselt wurden.

- ✓ Die Netzwerkkommunikation bleibt unberührt, unverändert und im gesamten Netzwerk durchgehend verschlüsselt.
- ✓ Es muss keine rechenintensive Entschlüsselung durchgeführt werden. Daher eignet sich die Precryption-Technologie für moderne und herkömmliche Verschlüsselungen und ist unabhängig von Art, Stärke und Version der Verschlüsselung.
- ✓ Es werden keine Anwendungsschlüssel offengelegt, es gibt keine Probleme mit der Verwaltung dieser Schlüssel und es sind keine ungewöhnlichen virtuellen Routen erforderlich.
- ✓ Die Precryption-Technologie wird unabhängig von der zu überwachenden Anwendung ausgeführt und hat somit keinen Einfluss auf die Ressourcen und das Lebenszyklusmanagement der Anwendung. Es werden also keine Fehler innerhalb der Anwendung verursacht.

So funktioniert die Precryption-Technologie von Gigamon: Einzelner Knoten (Abbildung 1)

1. Wenn eine Anwendung eine Nachricht verschlüsseln muss, verwendet sie eine Verschlüsselungsbibliothek, z. B. OpenSSL, um die eigentliche Verschlüsselung durchzuführen.

2. GigaVUE Universal Cloud Tap (UCT), das mit der Precryption-Technologie ausgestattet ist, erhält eine Kopie dieser Nachricht, bevor sie im Netzwerk verschlüsselt wird.

3. Die verschlüsselte Nachricht wird mit unveränderter Verschlüsselung an die empfangende Anwendung gesendet – ohne Proxy, ohne erneute Verschlüsselung und ohne erneutes Übertragen.

4. GigaVUE UCT erstellt bei Bedarf Datenpaket-Header, fasst sie in einem Tunnel zusammen und leitet sie an die GigaVUE V Series in der Deep Observability Pipeline weiter. Gigamon optimiert die Daten weiter, wandelt sie um und liefert sie an Tools, ohne eine weitere Entschlüsselung zu erfordern.

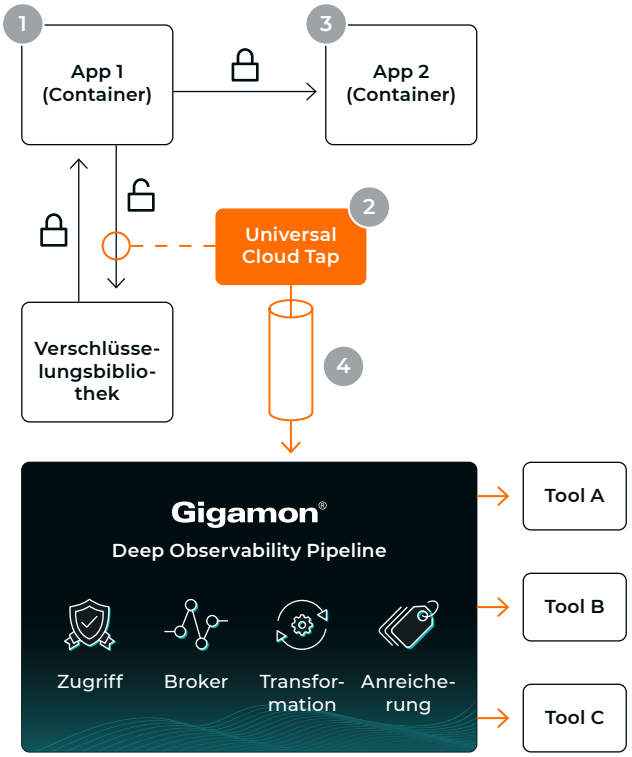


Abbildung 1

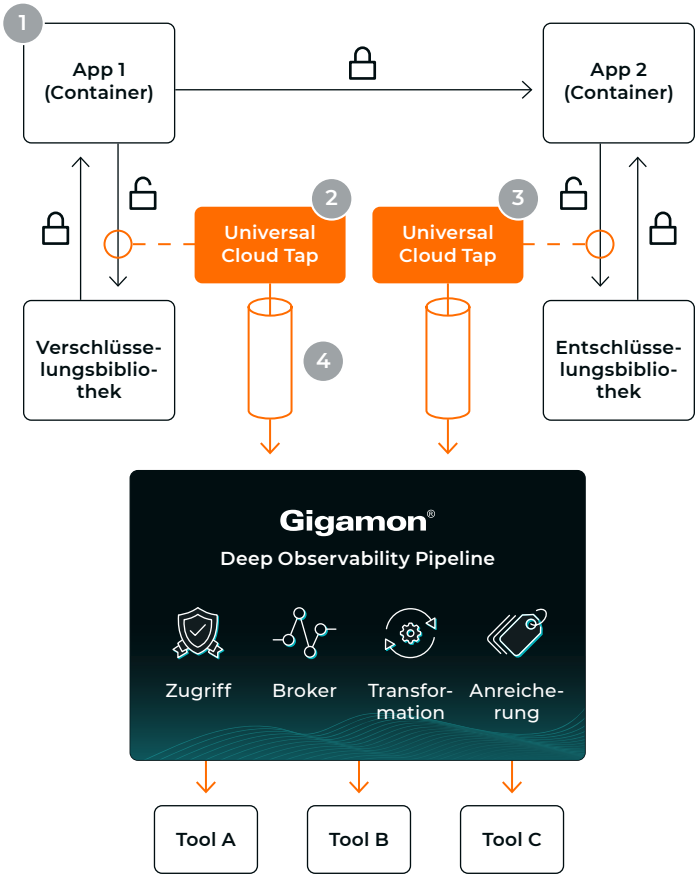


Abbildung 2

So funktioniert die Precryption-Technologie von Gigamon: Mehrere Knoten (Abbildung 2)

1. Wenn eine Anwendung eine Nachricht verschlüsseln muss, verwendet sie eine Verschlüsselungsbibliothek, z. B. OpenSSL, um die eigentliche Verschlüsselung durchzuführen.

2. GigaVUE Universal Cloud Tap (UCT) mit Precryption erhält eine Kopie dieser Nachricht, bevor sie im Netzwerk verschlüsselt wird.

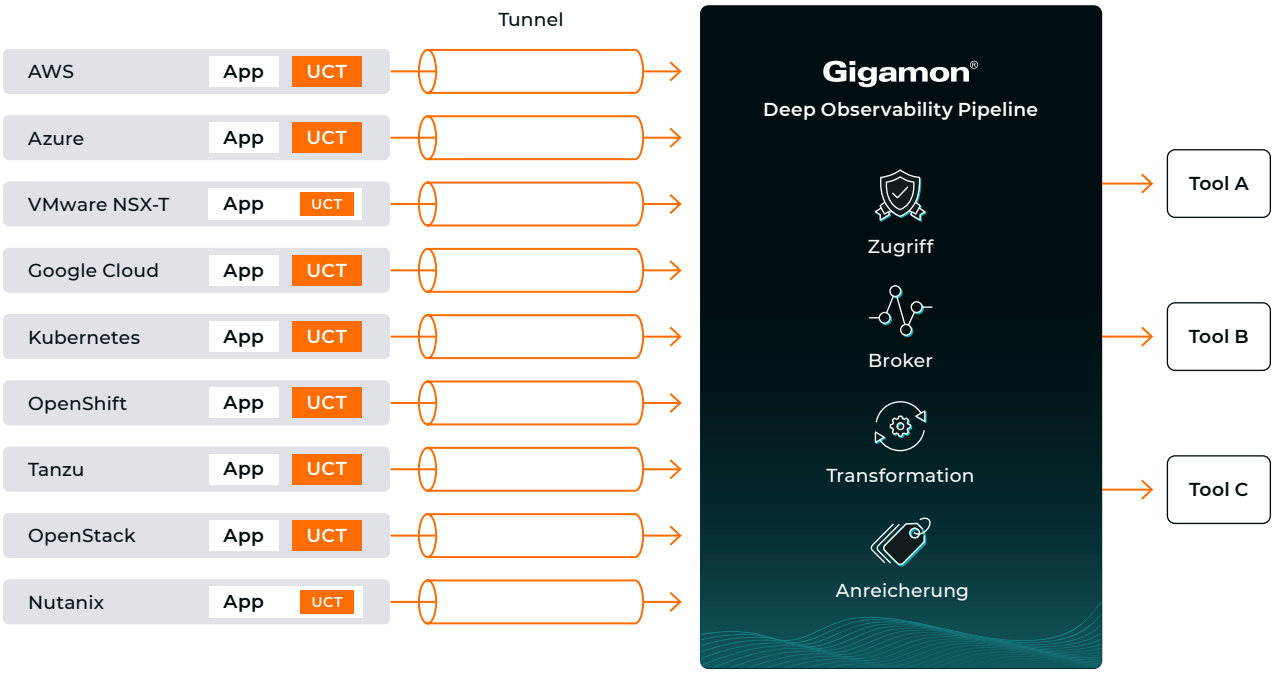
3. Optional kann GigaVUE UCT mit Precryption auch eine Kopie der Nachricht von der Serverseite erhalten, nachdem sie verschlüsselt wurde.

4. GigaVUE UCT erstellt bei Bedarf Datenpaket-Header, fasst sie in einem Tunnel zusammen und leitet sie an die V Series in der Deep Observability Pipeline weiter. Dort werden die Daten weiter optimiert, transformiert und an Tools weitergeleitet, ohne eine weitere Entschlüsselung zu erfordern.

Geeignet für Multi-Cloud- und sehr umfangreiche Umgebungen

GigaVUE UCT mit Precryption-Technologie eignet sich für verschiedene virtuelle und Cloud-Plattformen, einschließlich VMware, AWS, Microsoft Azure, OpenStack, Google Cloud, Nutanix und mehr. Dabei wird eine gemeinsame Daten-Pipeline mit einer einzigen globalen Management-Schnittstelle verwendet.

- ✓ Unterstützung der automatischen Bereitstellung in Kubernetes erleichtert die Skalierung
- ✓ Ein gemeinsamer Lizenzpool für alle Cloud-Umgebungen und unbegrenzte Instanzen



GigaVUE UCT wird unabhängig von der Anwendung ausgeführt

Der Begriff „Agent“ kann je nach Kontext unterschiedliche Bedeutungen haben. Anhand der folgenden Tabelle können Sie die Vorteile von UCT gegenüber herkömmlichen Agents prüfen.

Typische Agents	GigaVUE UCT
X Wird im Anwendungsbereich/Pod ausgeführt	✓ Unabhängige Benutzerfläche in einem unabhängigen Pod
X Auswirkungen auf die Nutzung von Anwendungsressourcen	✓ Unabhängige Knotenressourcen
X Erfordert koordinierte Versions-Upgrades	✓ Unabhängige Upgrades
X Erfordert Tests zusammen mit der Anwendung	✓ Unabhängiges Lebenszyklusmanagement
X Kann Anwendungslatenz verursachen	✓ Unabhängige Erfassung
X Kann Instabilität verursachen oder bei Fehlern den Zugang blockieren	✓ Unabhängiger Fehlerbereich

Mit netzwerkbasierten Informationen die Sicherheit verbessern und die Produktivität der Entwickler steigern

Sobald die unverschlüsselten Daten extrahiert sind, kann die Gigamon Deep Observability Pipeline weiter genutzt werden, um die rohen Kommunikationsdaten in Flow-Level-Metadatensätze umzuwandeln und so Fehlalarme zu reduzieren, bösartige Aktivitäten wie Port-Spoofing zu identifizieren und die Erkennung von Bedrohungen durch proaktive Echtzeit-Überwachung anstatt reaktiver Forensik zu beschleunigen. Diese aus dem Netzwerk abgeleiteten Informationen müssen sich keiner Protokolländerung unterziehen, eignen sich für IoT- und andere Geräte ohne Agents und können an Überwachungstools von SecOps- und DevOps-Teams weitergeleitet werden.

In hochsensiblen Umgebungen kann UCT optional auch gespiegelte Kommunikation, die für die Deep Observability Pipeline bestimmt ist, erneut verschlüsseln und sensible Daten wie Kreditkarten oder persönliche Informationen vor der Weiterleitung an die Tools tarnen.

Anwendungsfall

Aufspüren von Cyberkriminalität mithilfe der Precryption-Technologie

Ein Angriff durch Cyberkriminelle in Form eines Ransomware-Angriffs beginnt in der Regel damit, dass sich ein Bedrohungsakteur durch Phishing oder eine andere Methode zum Abfangen von Anmeldeinformationen Zugang zum Laptop eines Mitarbeiters außerhalb des Netzwerks verschafft. Eigentlich sollte dies durch die Endpunktsicherheit erkannt oder verhindert werden, aber leider ist dies nicht immer der Fall.

Sobald ein Bedrohungsakteur in das Netzwerk eingedrungen ist, stehen ihm zahlreiche Ressourcen zur Verfügung, darunter ausgefeilte Methoden zum Löschen von Protokollen, zur Rechteerweiterung und zur Suche nach anderen, interessanteren Netzwerkressourcen, z. B. Hosts, Anwendungen, Workloads usw., mit sensibleren Daten. Wenn sie genügend Zeit und Angriffsvektoren haben, können sie auch andere Netzwerkressourcen infiltrieren. Diese Vorgehensweise wird als „Lateral Movement“ bezeichnet.

Schließlich dringt der Bedrohungsakteur in interessantere Anwendungen vor, in denen Daten offengelegt und die Kommunikation ausspioniert wird. Der Bedrohungsakteur greift die Daten nach und nach ab und legt sie an einem von ihm kontrollierten Speicherort innerhalb des Netzwerks ab. Dieses Abgreifen erfolgt auf unauffällige Weise, sodass die Leistung nicht beeinträchtigt wird und keine Alarme ausgelöst werden. Wenn der Akteur schließlich über ausreichend Daten verfügt, führt er eine abschließende schnelle und umfangreiche Datenexfiltration durch, um die gestohlenen Daten nach außen zu exportieren und das Unternehmen anschließend zu erpressen.

Bei dieser Geschichte hat der Bedrohungsakteur primär vier Aktivitäten durchgeführt:

1. Anfängliches Phishing bzw. Aneignung von Zugangsdaten zur Umgehung der Endpunktsicherheit
2. Lateraler Datenverkehr innerhalb des Netzwerks (Lateral Movement)
3. Langsames Abgreifen sensibler Daten zur Speicherung an einem sicheren Ort
4. Rasche Exfiltration von Daten

Wir möchten Ihnen zeigen, wie die Plaintext-Transparenz mit der Precryption-Technologie von Gigamon den Tools ermöglicht, diese Aktivitäten zu erkennen:

	Was ein Sicherheitstool ohne Precryption erkennen kann	Was ein Sicherheitstool mit Precryption erkennen kann
Anfängliches Phishing	Normale Mitarbeitertätigkeit	Normale Mitarbeitertätigkeit
Lateraler Datenverkehr	Unbedenkliche Vorgänge	Bekannter Angriff wurde durchgeführt und hat den Server erfolgreich infiltriert
Abgreifen von Daten	Unbedenkliche Vorgänge	VIP-Daten werden über nicht-autorisierte Kanäle abgerufen und übertragen
Exfiltration von Daten	Übertragung großer Datenmengen	Detaillierte Auflistung des Diebesguts

Einen detaillierteren Überblick über dieses Szenario der Cyberkriminalität können Sie mit dieser Infografik herunterladen.

Schlussfolgerung

Der Einblick in verschlüsselten Datenverkehr und verschlüsselte Metadaten verbessert die Sicherheit, Überwachung und Fehlerbehebung in hybriden Cloud-Umgebungen erheblich. Die Gigamon Deep Observability Pipeline adressiert direkt die aktuellen Sicherheitsherausforderungen an die Überwachung von virtuellem und Container-Datenverkehr, sowohl vor Ort als auch in der öffentlichen Cloud. GigaVUE UCT begegnet der zunehmenden Verbreitung der Cloud mit robuster Plattform-Unterstützung und einer einzigen Management-Schnittstelle. Die von Gigamon aus dem Netzwerk abgeleiteten Informationen liefern hochwertige Metadaten für die Sicherheitstools der DevOps-, CloudOps- und SecOps-Teams. Die Gigamon Precryption-Technologie bewältigt zudem das besonders heikle Problem der Überwachung von verborgenen Aktivitäten in einer Cloud mit moderner Verschlüsselung. Dies geschieht auf elegante und unauffällige Art und Weise, verbessert die Sicherheitslage und verwehrt Kriminellen den Zugang.

Über Gigamon

Gigamon bietet eine Deep Observability Pipeline, die verwertbare, aus dem Netzwerk abgeleitete Informationen nutzt, um die Leistung von Überwachungstools zu erhöhen. Diese leistungsstarke Kombination unterstützt IT-Organisationen bei der Gewährleistung von Sicherheits- und Compliance-Governance, bei der schnellen Ursachenanalyse von Leistungsengpässen und bei der Senkung des mit der Verwaltung von hybriden und Multi-Cloud-IT-Infrastrukturen verbundenen betrieblichen Aufwands. Das Ergebnis: Moderne Unternehmen schöpfen das Transformationspotenzial der Cloud voll aus. Gigamon bedient mehr als 4.000 Kunden weltweit, darunter über 80 Prozent der Fortune-100-Unternehmen, neun der zehn größten Mobilfunkanbieter und Hunderte von Behörden und Bildungseinrichtungen weltweit. Weitere Informationen finden Sie auf gigamon.com/de/.

1. Shelley Boose. 81% of Companies Have Had a Cloud Security Incident in the Last Year. Venafi, 28. September 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. Verschlüsselte Angriffe steigen 314%: New ThreatLabz State of Encrypted Attacks Report. Zscaler, 28. Oktober 2021. https://www.zscaler.com/blogs/security-research/encrypted-attacks-rise-314.

Gigamon®

Weltweiter Firmenhauptsitz
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

09.23_01