

Gigamon launcht Precryption-Technologie: Deep Observability für verschlüsselten Datenverkehr

Paketerfassung innerhalb des Linux-Kernels und Klartext-Sichtbarkeit für verschlüsselten Traffic beseitigen blinde Flecken bei virtuellen, Cloud- und Container-Anwendungen

München, 12. September 2023 – [Gigamon](#), Marktführer im Bereich Deep Observability, erweitert die Gigamon Deep Observability Pipeline im Rahmen des GigaVUE 6.4 Releases um eine Reihe von Cybersecurity-Innovationen. Die wegweisende Precryption-Technologie ermöglicht es IT- und Sicherheitsunternehmen erstmals, mit einer automatisierten Lösung Einblick in verschlüsselten Datenverkehr über virtuelle Maschinen (VM) oder Container-Workloads zu erhalten. Somit können sie fortschrittliche Bedrohungserkennung, -untersuchung und -reaktion über die gesamte Hybrid-Cloud-Infrastruktur hinweg durchführen. Das ist notwendig, da Verschlüsselung, die eigentlich der Sicherheit und dem Schutz der Privatsphäre dienen sollte, sich inzwischen zu einem Angriffsvektor für Cyber-Kriminelle entwickelt hat: Mehr als [93 Prozent der Malware](#) wird mittlerweile hinter einer Verschlüsselung versteckt.

Versteckte Gefahren in verschlüsseltem Datenverkehr

In einer aktuellen [Gigamon-Umfrage](#) geben über 70 Prozent der 1.000 befragten IT- und Sicherheitsverantwortlichen zu, dass sie die verschlüsselten Daten, die über ihre Hybrid-Cloud-Infrastruktur fließen, derzeit nicht überprüfen. Dies stellt ein ernsthaftes Geschäftsrisiko dar, da verschlüsselte Daten nicht ausreichend analysiert werden und Malware-Bedrohungen nicht allein durch Sicherheits- und Überwachungstools erkannt werden können, wenn verschlüsselte Daten durch die Infrastrukturen eines Unternehmens fließen.

Gigamons Precryption-Technologie deckt bisher verborgene Bedrohungen auf, einschließlich Lateral Movement, Malware-Verteilung und Datenexfiltration in virtuellen, Cloud- und Container-Anwendungen. Der innovative Ansatz nutzt die eBPF-Technologie innerhalb des Linux-Kernels, um Klartext-Sichtbarkeit zu liefern und den Datenverkehr vor der Verschlüsselung oder nach der Entschlüsselung zu erfassen. Es müssen keine Schlüssel abgefangen oder ausgespäht werden und es ist keine teure Entschlüsselung erforderlich. Darüber hinaus läuft die Precryption-Technologie anwendungsunabhängig und vermeidet die operativen Herausforderungen klassischer agentenbasierter Ansätze.

„Globale Unternehmen sind zunehmend erfolgreich mit der Vereinheitlichung von Sicherheitsprotokollen in Security Data Lakes, aber verschlüsselter Datenverkehr stellt eine echte Herausforderung dar“, sagt Omer Singer, Head of Cybersecurity Strategy bei Snowflake. „Fortschritte in der Branche wie Gigamons Precryption-Technologie stellen einen überzeugenden Weg für Unternehmen dar, um verschlüsselten Cloud-Verkehr sichtbar zu machen, was wiederum zu verbesserter Sicherheit und Compliance führt.“

Vorteile der Gigamon Precryption-Technologie:

- Vollständige Sichtbarkeit von verschlüsseltem Traffic über VM- oder Container-Workloads hinweg
- Nahtlose Einbettung moderner Verschlüsselungsmethoden, einschließlich TLS 1.3 oder TLS 1.2 mit aktivierter Perfect-Forward-Secrecy (PFS), und älterer Verschlüsselungsmethoden wie TLS 1.2 ohne PFS
- Möglichkeit, Traffic mit personenbezogenen Daten zu maskieren
- Keine weitere Notwendigkeit des Austausches privater Schlüssel

- Effiziente Entlastung für Cloud-, Sicherheits- und Observability-Tools durch TLS-Entschlüsselungsaufwand

„In einer kürzlich durchgeführten Studie unter IT- und Sicherheitsverantwortlichen großer Unternehmen haben wir herausgefunden, dass 50 Prozent der Unternehmen das Risiko in Kauf nehmen und Datenverkehr aufgrund von technischen und finanziellen Herausforderungen nicht entschlüsseln“, so Christopher Steffen, Vice President of Research bei EMA. „Das bedeutet, dass die Hälfte der Unternehmen Zero Trust nicht erreichen kann. Es ist an der Zeit, Einblicke in verschlüsselten Datenverkehr möglich zu machen anstatt sie als unmöglich abzustempeln. Mit Innovationen wie der Gigamon Precryption-Technologie können Unternehmen die Sichtbarkeit erhalten, die sie benötigen, um die sich entwickelnden Standards und die Einhaltung von Vorschriften zu erfüllen und ihre hybride Cloud-Infrastruktur zuverlässig abzusichern.“

„Da die Cloud-Akzeptanz über eine wachsende Anzahl von privaten und öffentlichen Plattformen beschleunigt wird, müssen Unternehmen auch die eskalierenden Risiken von Bedrohungsaktivitäten angehen, die sich im verschlüsselten Datenverkehr verbergen“, sagt Michael Dickman, Chief Product Officer bei Gigamon. „Bisher war das Entschlüsseln von Cloud-Datenverkehr mühsam und teuer. Mit der Gigamon Precryption-Technologie ändert sich das grundlegend. Wir schaffen Deep Observability für verschlüsselten Traffic, was es Kunden ermöglicht, ihre Sicherheitslage über eine beliebige Anzahl von Clouds und Workloads hinweg zu verbessern, ohne ihre Entwickler zu belasten.“

GigaVUE 6.4: nahtlose Sicherheitsintegration in Infrastruktur und Anwendungen

Das aktuelle Software Release beinhaltet auch mehrere erweiterte Sicherheitsfunktionen, darunter:

- **Cloud-SSL-Entschlüsselung** – Erweiterung der klassischen On-Premise-Entschlüsselungsfunktionen für eine breite Palette von virtuellen und Cloud-Plattformen
- **Universal Cloud Tap (UCT)** – ein einziger, ausführbarer Tap für führende Plattformen, der sich über VMs und Container erstreckt, mit Vorfilterung an der Quelle für maximale Effizienz
- **Application Metadata Intelligence (AMI) Integration** – Erkennung von Schwachstellen und verdächtigen Aktivitäten auf managed und unmanaged Hosts (zum Beispiel. IoT-Geräten)

Um mehr über die neuesten Innovationen zu erfahren, können Sie auch an virtuellen Deep Dive Sessions im Rahmen des [Gigamon Visualize Bootcamp](#) teilnehmen.

Über Gigamon

Gigamon® bietet eine Pipeline für Deep Observability, die sofort verwertbare Informationen auf Netzwerkebene nutzt, um die Leistungsfähigkeit von Observability-Werkzeugen zu maximieren. Diese effektive Kombination ermöglicht es IT-Organisationen, Sicherheit und Compliance umfassend zu gewährleisten, die Ursachen von Leistungsengpässen schneller zu identifizieren und den Verwaltungsaufwand zu senken, der ansonsten durch das Management hybrider und Multi-Cloud-Infrastrukturen entsteht. Das Ergebnis: Moderne Unternehmen realisieren das volle Transformationspotenzial der Cloud. Gigamon unterstützt mehr als 4.000 Kunden weltweit, darunter über 80 Prozent der Fortune-100-Unternehmen, 9 der 10 größten Mobilfunkanbieter und Hunderte von Behörden und Bildungseinrichtungen weltweit.

Weitere Informationen finden Sie unter www.gigamon.com.

© 2023 Gigamon. Alle Rechte vorbehalten. Gigamon und das Gigamon-Logo sind Warenzeichen von Gigamon in den Vereinigten Staaten und/oder anderen Nationen. Gigamon Marken finden Sie unter www.gigamon.com/legal-trademarks. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.