Gigamon®

Ohne tiefgreifende Überwachung droht ein böses Erwachen.

Die aus dem Netzwerk abgeleitete Intelligenz erkennt Bedrohungen, die Ihre vorhandenen Sicherheitstools nicht erkennen können.

Das CISO-Rätsel

Laut *Forbes* wird die Zahl der großen Unternehmen, die eine Multi-Cloud-Strategie verfolgen, bis zum Jahr 2024 auf 85 Prozent ansteigen[1], denn die Unternehmen versuchen, bei der Cloud-Transformation ein Gleichgewicht zwischen geschäftlicher Flexibilität und Cybersicherheit herzustellen.

Gleichzeitig sind die Kosten und das Ausmaß von Cyberangriffen so hoch wie nie zuvor: Die weltweiten Kosten für Cyberkriminalität werden bis 2025 voraussichtlich 10,5 Billionen US-Dollar erreichen.[2] Daher stehen CISOs vor der Herausforderung, ihre komplexe Infrastruktur vor einer immer ausgefeilteren Bedrohungslandschaft zu schützen und zu überwachen und gleichzeitig Kosten und Komplexität einzudämmen. Trotz rekordverdächtiger Ausgaben für die neuesten Sicherheitsstrategien und -tools wie SASE, EDR, Netzwerk-Mikrosegmentierung und SIEMs haben CISOs nach wie vor Schwierigkeiten, mit der wachsenden Flut neuer Bedrohungen Schritt zu halten, insbesondere mit Ransomware und Insider-Verletzungen.

1. Marr, B. (20. Februar 2024). The 10 biggest cloud computing trends in 2024 Everyone must be ready for now. Forbes.
2. Gartner prognostiziert, dass die weltweiten Ausgaben für Sicherheits- und Risikomanagement bis 2024 um 14 % steigen werden.

Wie sich Sicherheitsverletzungen auf das Geschäftsergebnis auswirken

Die Kosten eines Sicherheitsverstoßes gehen weit über Geldbeträge hinaus. Sie haben tiefgreifende Auswirkungen auf das Geschäft:

- Unterbrechung des Geschäftsbetriebs durch Ausfallzeiten und Umsatzeinbußen.
- Rufschädigung und Beeinträchtigung der Kundentreue durch Diebstahl von IP- und Kundendaten.
- Dadurch wird es teurer (oder gar unmöglich), eine Cyberversicherung abzuschließen.
- Das Unternehmen und seine Mitarbeiter werden dem Risiko von Bußgeldern und Gefängnisstrafen für die Missachtung von Vorschriften ausgesetzt.

Ihre Sicherheitstools leisten hervorragende Arbeit.
Soweit Sie wissen.

Ohne tiefgreifende Überwachung droht ein böses Erwachen.

Die größten Schwachstellen in Ihrem Netzwerk: Lateraler und verschlüsselter Datenverkehr

Mit der zunehmenden Verbreitung der Cloud gehen auch steigende Kosten und Komplexität bei der Sicherung und Verwaltung von Hybrid-Cloud-Infrastrukturen einher. Die verschiedenen Infrastrukturkomponenten haben ihre eigenen Überwachungstools und -prozesse, was zu einem fragmentierten Bestand an Silo-Tools führt, die kein vollständiges Bild davon vermitteln, was in Ihrer Hybrid-Cloud-Infrastruktur wirklich passiert.

Ihre Sicherheitstools sind hart im Umgang mit Nord-Süd-Bedrohungen und erstaunlich gelassen gegenüber Ost-West-Bedrohungen.

Die meisten Sicherheitstools untersuchen zwar den Nord-Süd-Verkehr, vernachlässigen aber oft den lateralen Datenverkehr, was verheerende Folgen für Ihr Unternehmen nach sich ziehen kann. Wenn Bedrohungsakteure in Ihr Netzwerk eindringen, können sie sich unbemerkt in Ihrer Hybrid-Cloud-Infrastruktur bewegen und schließlich auf die höchst vertraulichen Daten Ihres Unternehmens zugreifen.

Die Gigamon Deep Observability Pipeline ist die einzige Lösung, die sich ausschließlich darauf konzentriert, diese Schwachpunkte zu beseitigen, indem sie die notwendige laterale Transparenz bietet, um bisher ungesehene Bedrohungen zu erkennen, einschließlich solcher, die sich bereits in Ihrem Netzwerk befinden.

Die Gefahren, die im verschlüsselten Verkehr lauern

In Anbetracht der Tatsache, dass 95 Prozent des gesamten Internetverkehrs verschlüsselt sind[4], sind Unternehmen mit fehlendem Einblick in den verschlüsselten Datenverkehr versteckten Bedrohungen ausgesetzt, die ihre vorhandenen Sicherheitstools nicht erkennen können. Und je mehr die Verschlüsselung zunimmt, desto größer sind die Möglichkeiten für Bedrohungsakteure, verschlüsselte Kanäle auszunutzen.

Jedes Netzwerk hat etwas zu verbergen. Bis jetzt.

Die Entschlüsselung des gesamten Datenverkehrs kann kostspielig und komplex sein, erfordert eine hohe Rechenleistung, erhöht die Latenzzeit und verringert die Leistung – bis jetzt. Gigamon bietet eine leistungsstarke Kombination aus patentierten Lösungen, die den Einblick in verschlüsselten Datenverkehr erschwinglich und skalierbar machen, einschließlich unserer preisgekrönten Precryption™-Technologie und GigaSMART© TLS/SSL Decryption.

Von den Unternehmen, die im vergangenen Jahr einen Angriff über verschlüsselte Kanäle erlebten, wurden 85 Prozent über „vertrauenswürdige“ Kanäle angegriffen, wie z. B. die legitimen Websites vertrauenswürdiger Unternehmen oder Drittanbieter – eine deutliche Erinnerung daran, dass kein TLS/SSL-verschlüsselter Datenverkehr als sicher gelten kann.[5]

4. Google-Transparenzbericht
5. Zscaler ThreatLabz 2023 State of Encrypted Attacks Report
6. 2024 Gigamon Hybrid Cloud-Umfrage

Die Lücke bei der Vorsorge

Übermäßiges Vertrauen in die Sicherheit des verschlüsselten Datenverkehrs sorgt für große Schwachstellen, die sich leicht ausnutzen lassen.

76 %
DER CISOS
vertrauen darauf, dass der verschlüsselte Datenverkehr sicher ist

63 %
DER CISOS
glauben, dass verschlüsselter Datenverkehr seltener überwacht wird

86 %
DER CYBERBEDROHUNGEN
sind im verschlüsselten Datenverkehr verborgen

62 %
DER UNTERNEHMEN
verzeichneten im vergangenen Jahr eine Zunahme der Angriffe über verschlüsselte Kanäle[6]

Auch die besten Sicherheits- und Beobachtungstools haben Schwachstellen

Sehen Sie den ganzen Eisberg mit tiefgreifender Überwachung.

Herkömmliche und native Cloud-Tools, die ausschließlich über MELT-Daten (Metrics, Events, Logs und Traces) Einblicke gewinnen, sind eingeschränkt, wenn es darum geht, Angriffe zu erkennen und die komplexe Infrastruktur von heute tiefgehend oder umfassend zu überwachen.

Die Gigamon Deep Observability Pipeline geht über herkömmliche Überwachungsansätze hinaus, indem sie Informationen direkt aus dem Netzwerkverkehr extrahiert und diese effizient und in Echtzeit an Ihre Tools weitergibt. Mit dieser aus dem Netzwerk abgeleiteten Intelligenz können Ihre Tools bislang verborgene Bedrohungen erkennen und dabei helfen, die Kosten und den Schweregrad eines Angriffs zu mindern.

> Deep Observability hilft, Schwachstellen zu beseitigen, indem sie Ihren Tools die vom Netzwerk abgeleitete Intelligenz und die Einblicke gibt, die erforderlich sind, um Bedrohungen zu erkennen, die zuvor unbemerkt geblieben wären.

Die wachsende Bedeutung der Echtzeit-Erkennung von Bedrohungen

Cyberangriffe werden immer schneller und aggressiver: Angreifer verkürzen die Zeit zwischen dem ersten Eindringen, der lateralen Bewegung und dem eigentlichen Angriff.

62 Minuten

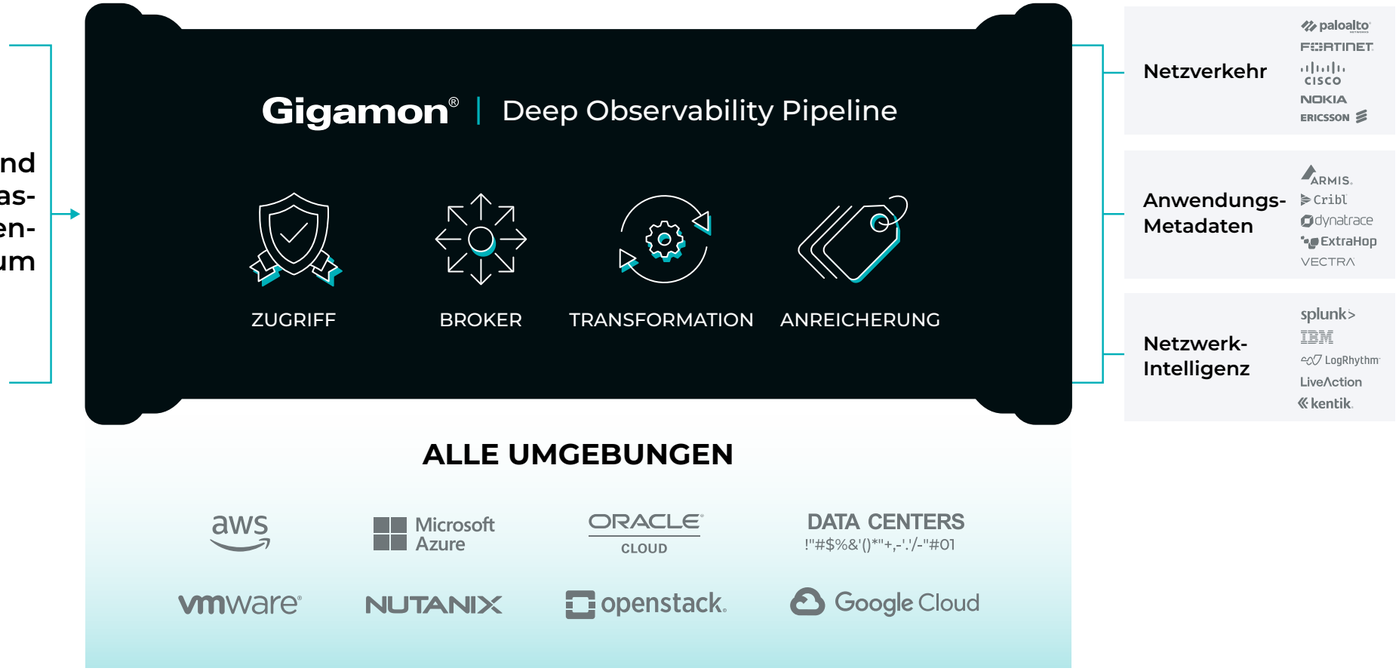
Die durchschnittliche Zeit, die ein Bedrohungsakteur benötigt, um von einem ursprünglich kompromittierten Host zu einem anderen innerhalb des Unternehmens zu wechseln, hat sich seit dem letzten Jahr um 23 Prozent beschleunigt. Manche benötigen nur wenige Minuten.

204 Tage

Es dauert durchschnittlich 204 Tage, bis Unternehmen eine Datenschutzverletzung erkennen, und 73 Tage, um sie unter Kontrolle zu bekommen.[7]

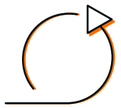
7. CrowdStrike 2024 Global Threat Report

Eine speziell entwickelte Deep Observability Pipeline



Die Gigamon Deep Observability Pipeline, basierend auf der GigaVUE Cloud Suite™, liefert effizient netzwerkbasierte Informationen an Ihre Cloud-, Sicherheits- und Observability-Tools. Auf diese Weise lassen sich Schwachstellen im Bereich Sicherheit beseitigen und die Kosten für Tools reduzieren, sodass Sie die hybride Cloud-Infrastruktur besser sichern und verwalten können.

Überladen Sie Ihre Sicherheitstools, um greifbare Ergebnisse zu erzielen



Agilität erhöhen, Kosten senken

Die Lösung für die Stärkung Ihrer Sicherheitslage ist nicht unbedingt die Investition in mehr Tools. Es hat sich vielmehr gezeigt, dass zu viele Tools bei der Erkennung und Eindämmung von Bedrohungen weniger effektiv sind, da sie die Sicherheitsteams überfordern und Datensilos schaffen, die zu Sichtbarkeitslücken und Schwachstellen führen.[3]

Gigamon optimiert die Leistung und Effektivität von Tools, um Unternehmen dabei zu helfen, den Tool-Wildwuchs in den Griff zu bekommen, Kosten zu senken und vor allem die tiefgreifende Überwachung zu ermöglichen, die Sie benötigen, um Schwachstellen zu beseitigen.

Sparen Sie Betriebskosten

Durch die Optimierung und Verbesserung des Signal-Rausch-Verhältnisses bei der Netzwerkverkehrerfassung erzielen Gigamon-Kunden oftmals Einsparungen in Höhe von 50 bis 60 Prozent bei den Ausgaben für Tools und können den Kauf neuer Kapazitäten verschieben. Außerdem macht Gigamon kostspielige Cloud-Gateway- und Lastausgleichsdienste überflüssig und senkt die Kosten für den Erwerb von Cloud-Traffic von 0,75 Cent auf 0,04 Cent pro Gigabyte.

3. 2020 Cyber Resilient Organization Report

Deep Observability macht Ihre vorhandenen Sicherheits- und Observability-Tools um bis zu **90 Prozent effizienter** und kann die Tool- und Bandbreitenkosten um bis zu 50 Prozent senken – so kann ein typischer mittelständischer Kunde einen ROI von 4 bis 6 Monaten erzielen.

Löschen Sie den Brand, bevor er ausbricht.

Ohne tiefgreifende Überwachung sind Sie anfällig für unsichtbare Bedrohungen.

Ein Marktführer im Bereich Deep Observability

650 GROUP Market Intelligence Research
#MARKTANTEILSFÜHRER
Deep Observability
2023

Laut dem Marktforschungsunternehmen 650 Group ist Gigamon mit einem Marktanteil von 63 Prozent im Jahr 2023 Marktführer im Bereich Deep Observability.

Die sicherheitsbewusstesten Behörden und Unternehmen auf der ganzen Welt setzen auf Gigamon, wenn es um spürbare Risikominderung geht.

+4.000
KUNDEN WELTWEIT

10/10
DER WICHTIGSTEN US-BUNDESBEHÖRDEN

8/10
DER TOP-ANBIETER IM GESUNDHEITSWESEN

83/100
DER FORTUNE-100-UNTERNEHMEN

7/10
DER WELTWEIT FÜHRENDEN BANKEN

9/10
DER GRÖSSTEN MOBILFUNKNETZBETREIBER

„Einige Vorfälle, die wir in den letzten sechs Monaten hatten, konnten wir recht schnell aufklären – innerhalb von etwa einer Stunde, nachdem der Angreifer einen Server übernommen hatte. Wir haben ihn gerade noch rechtzeitig erwischt, bevor ein echter Schaden entstanden ist. Der Grund dafür ist, dass wir über Sicherheitstools verfügen und Gigamon alle Daten in diese Sicherheitstools einpflegt.“

Kajeevan Rajanayagam, Leiter für Cybersicherheit beim University Health Network

„Unternehmen verlagern immer mehr Workloads in die Cloud, doch diese hybriden und Multi-Cloud-Umgebungen stellen aufgrund der mangelnden Transparenz eine große Herausforderung für die Sicherheit dar. Die Schaffung einer schlüsselfertigen Lösung mit Gigamon und Vectra AI ist ein entscheidender Schritt in Richtung Cloud-Sicherheit. Wir sind nun in der Lage, unseren Kunden auf der ganzen Welt eine komplette Cyber-Abwehrlösung für alle Cloud-Netzwerke anzubieten, indem wir die tiefgreifende Beobachtbarkeit, die sie von Gigamon benötigen, mit einer erstklassigen, KI-basierten Plattform zur Erkennung, Untersuchung und Reaktion auf Bedrohungen von Vectra AI kombinieren – und zwar in Form eines Gesamtangebots.“

Paul Eccleston, SVP im EMEA-Raum für Exclusive Networks

„Letztes Jahr haben wir die Auswirkungen neuer Cybersecurity-Bedrohungen erlebt, mit öffentlicher Berichterstattung über Sicherheitsverletzungen, Ransomware und Datenlecks“, „Diese Schwachstellen machen Deep Observability und die damit verbundene Ost-West-Transparenz des verschlüsselten Datenverkehrs zu einer unverzichtbaren Grundlage für alle Unternehmensabläufe, was die Nachfrage in den heutigen Sicherheits- und IT-Budgets erhöht. Gigamon konnte mit seiner Deep Observability Pipeline, die einen innovativen Ansatz zur Sicherung und Verwaltung moderner Hybrid-Cloud-Infrastrukturen bietet, seine marktführende Position beibehalten.

Alan Weckel, Gründer und Technologieanalyst bei der 650 Group

Abschließende Hinweise

Gigamon hat es sich zur Aufgabe gemacht, die hybriden Netzwerke und Daten der größten und komplexesten Unternehmen der Welt zu schützen. Wir verfolgen das Ziel, zu lernen, zusammenzuarbeiten und zu innovieren, um Lösungen bereitzustellen, die Unternehmen vor Cyberbedrohungen schützen. In Zusammenarbeit mit Mitarbeitern, Partnern und Kunden haben wir eine Pipeline entwickelt, die ein Höchstmaß an Sicherheit in der Hybrid Cloud bietet.

Lassen Sie Gigamon Ihre Cloud-, Sicherheits- und Observability-Tools aufwerten, indem Sie ihnen etwas geben, was sie nicht haben: **umsetzbare, aus dem Netzwerk abgeleitete Informationen und Erkenntnisse.**

Erfahren Sie mehr über Deep Observability

Gigamon®

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