Gigamon®

Deep Observability für hybride Infrastrukturen

Wie Netzwerk-Teams Performance und Kosten in den Griff kriegen und in Echtzeit auf Angriffe reagieren können

Ein Whitepaper von
heise Business Services

Wie Netzwerk-Teams Performance und Kosten in den Griff kriegen und in Echtzeit auf Angriffe reagieren können

Moderne Unternehmensnetze sind hybrid. Sie umfassen neben der eigenen physischen und virtuellen Infrastruktur auch Software und Strukturen in Public und Private Clouds. Somit muss die Unternehmens-IT oft unübersichtliche, im Laufe der Zeit gewachsene Hybrid- oder gar Multi-Cloud-Umgebungen unter Kontrolle halten. Mit Deep Observability erhalten Netzwerk-Teams nun eine Möglichkeit, mit der sie ihre Netze über alle hybriden Welten hinweg intelligenter verwalten können. Durch das tiefgreifende Beobachten und Analysieren sämtlicher darin fließender Datenströme lassen sich zum einen Performance und Kosten optimieren sowie die Komplexität reduzieren. Zum anderen leiten diese Netzwerküberwachungssysteme die daraus gewonnenen Daten intelligent und in Echtzeit an vorhandene Security- und Compliance-Tools weiter. Somit kann die IT auch Sicherheits- und Compliance-Risiken in hybriden und Multi-Cloud-Infrastrukturen proaktiv, einfacher und effizienter verwalten.

Mit der zunehmenden Digitalisierung, Industrie 4.0 und dem Internet of Things (IoT) sowie mit 5G etwa für autonomes Fahren steigt die Anzahl der angebundenen Komponenten rasant. Folglich erhöht sich auch das Datenvolumen, das die Netzwerke belastet. Zudem erfordern Echtzeitanwendungen und Big-Data-Analysen sowie die Nutzung von Künstlicher Intelligenz (KI) hohe Datenraten von 100 GBit/s und mehr. Dank Cloud-Computing lassen sich IT-Infrastrukturen zwar schnell an neue Anforderungen anpassen, doch in der Cloud bleibt das Management von Apps und Verbindungen undurchsichtig.

Laut dem „State of the Cloud Report 2022“ von Flexera gaben 63 Prozent der 753 Teilnehmer dieser internationalen, jährlich stattfindenden Umfrage unter IT-Experten und Entscheidern für Cloud-Themen an, dass sie zum Zeitpunkt der Befragung Ende 2021 mehr als ein Viertel ihrer Workloads in der Cloud hielten. Zudem würden 89 Prozent der Befragten gerade eine Multi-Cloud-Strategie umsetzen, 48 Prozent sogar eine jeweils multiple Public- und Private-Cloud-Strategie. Da sich im Schnitt europäische Befragte weniger häufig (58 Prozent) als intensive Cloud-Nutzer eingeschätzt haben als die Gesamtheit der Befragten (63 Prozent), wird hier auch der Anteil mit Multi-Cloud-Strategie nicht ganz so hoch sein wie auf internationaler Ebene. Dennoch ist ersichtlich, dass heute weltweit ein Großteil der Firmen eine mehr oder weniger komplexe Multi-Cloud-Umgebung betreiben.

Bei einer Multi-Cloud-Umgebung nutzt eine Organisation mehr als eine Cloud-Plattform und dabei mehrere Public Clouds, die jeweils eine bestimmte Anwendung oder einen bestimmten Dienst bereitstellen.

Welche Herausforderungen Multi-Cloud-Umgebungen mit sich bringen

Als größte Herausforderung im Cloud-Bereich sahen die Befragten die Themenbereiche Sicherheit (85 Prozent), Verwaltung der Cloud-Ausgaben (81 Prozent) und aus Netzwerksicht Compliance (76 Prozent) sowie die Administration von Multi-Clouds (71 Prozent). Ein wesentlicher Grund für diese Einschätzung ist, dass Netzwerk-Teams oft nur Insellösungen für das Management einzelner Cloud-Plattformen nutzen können oder den Traffic in vielen Cloud-Plattformen überhaupt nicht einsehen können. Ohne Einsicht in den Traffic lassen sich diese Verbindungen aber kaum schützen, was zu ungeplanten, kaum kalkulierbaren Belastungen des Netzwerks führt. Zudem besteht die Gefahr, dass eine Abteilung ohne Absprache mit der Unternehmens-IT Cloud-Dienste nutzt, wodurch sie Compliance- und Security-Regelungen umgeht. Diese Blind Spots der Cloud-Umgebungen verhindern genau wie alle anderen Blind Spots im Unternehmensnetz einen umfassenden Blick auf die Data in Motion und stellen angesichts der immer ausgeklügelteren Cyberangriffe ein großes Sicherheitsrisiko dar.

Die aktuellen Herausforderungen der Netzwerk- und Security-Teams

- ✓ Sicherer Betrieb und Visibilität über alle Netze und genutzten Cloud-Plattformen hinweg
- ✓ Compliance-Richtlinien und DSGVO einhalten
- ✓ Einführung von Zero-Trust-Konzepten als Schutz vor Cyberattacken wie Ransomware-Angriffen, Malware, Crypto Mining etc.
- ✓ Gutes User-Erlebnis gewährleisten
- ✓ Performance optimieren: Flaschenhälse erkennen und beheben, Metadaten im Netz vermeiden
- ✓ Überblick über Anwendungen im Netz behalten
- ✓ Anzahl der genutzten Tools reduzieren zugunsten eines besseren Überblicks und um Kosten zu senken
- ✓ Blind Spots im gesamten Netzwerk inklusive Clouds erkennen und eliminieren
- ✓ Komplexität von Hybrid- und Multi-Cloud-Umgebungen in den Griff bekommen
- ✓ Die Unternehmens-IT ständig auf dem Stand der Technik halten sowie neue Technologien und Anwendungen einführen.

Wie Observability-Lösungen aus MELT-Daten ein Gesamtbild liefern

Viele Unternehmen setzen verschiedenste Netzwerk-Monitoring-Lösungen ein, um Störungen oder Anomalien aufzuspüren und zu analysieren. Auf diese Weise kann das Netzwerk-Team aber nur definierte Verbindungen überwachen und erhält keine ganzheitliche Sicht auf das Netzwerk. Gerade bei hybriden Netzen mit Virtualisierung und Multi-Cloud-Umgebungen ist es aber wichtig, dass alle verschlüsselten und unverschlüsselten Data in Motion sichtbar sind, inklusive des Ost-West-Traffics zwischen Containern sowie nicht verwalteter Geräte. Nur so lässt sich eine vollständige und konsistente Netzwerksicherheit bereitstellen.

Außerdem erlaubt das Monitoring via SPAN-Ports und TAPs lediglich Reaktionen auf erkannte Ereignisse und kein proaktives Eingreifen. Dennoch bilden diese Überwachungen die zentrale Datengrundlage für einen übergeordneten Blick auf das Netz.

Warum eine tiefe und umfassende Netzsichtbarkeit unverzichtbar ist

Wird das Netzwerk-Monitoring kombiniert mit Full-Packet-Capturing und einer Auswertung der NetFlow- sowie Log-Daten, erhalten Netzwerk- und Security-Teams eine umfassendere Sicht auf das Netzwerk. Die zugrunde liegenden Informationen setzen sich aus Messdaten, erkannten Events, Log-Daten und aufgezeichneten Traffic-Traces (Überbegriff für diese vier Bereiche: MELT) zusammen. Eine entscheidende Rolle spielt dabei, dass auch die entsprechenden Daten der Public-Cloud-Installationen sowie SaaS-Anwendungen miteinbezogen werden, sonst ergibt sich keine lückenlose Sicht auf das Netzwerk. Das erfordert detaillierte, umfassende Daten aus allen Netzwerksegmenten, die für die Suche nach sporadisch auftretenden Störungen oder die Erkennung von Anomalien aufgezeichnet und abgespeichert werden müssen.

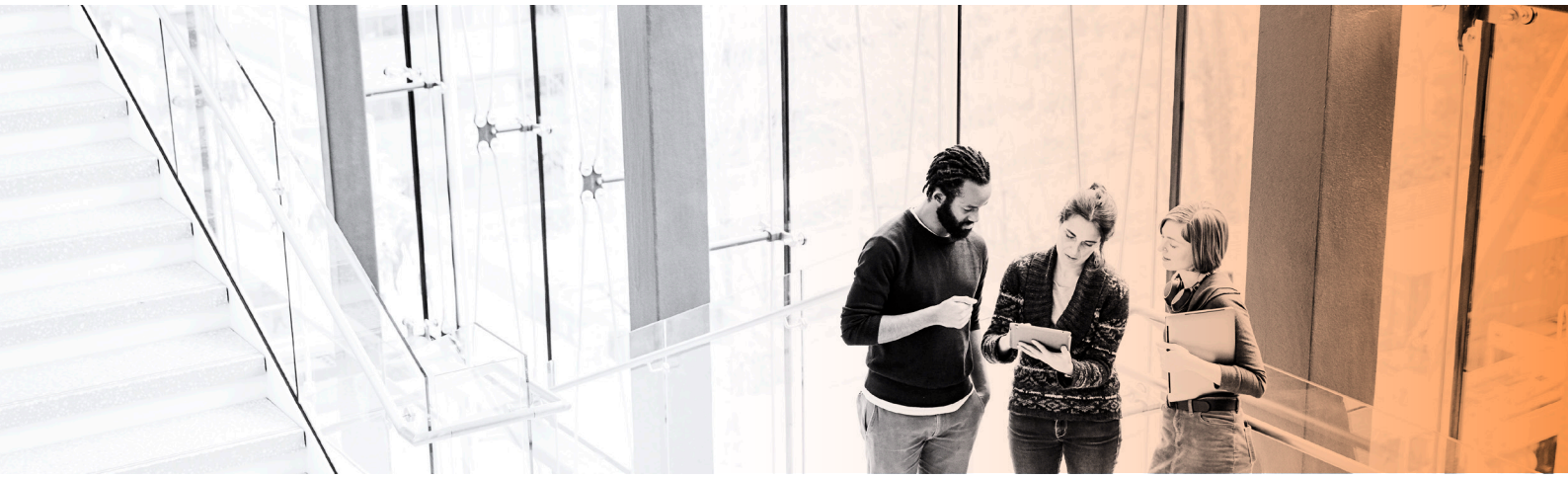
Security-Teams brauchen diese tiefe Netzwerksichtbarkeit, weil sie vollständigen Zugriff auf die Datenpakete benötigen, um Malware-Signaturen, verdächtige Verhaltensweisen sowie Bedrohungen erkennen und analysieren zu können. Auch für Network-Detection-&-Response-Lösungen (NDR) ist sie unverzichtbar.

Wie die Gesamtschau der Network Observability proaktives, strategisches Handeln ermöglicht

Network Observability liefert auf Basis dieser Daten eine übergeordnete Gesamtschau auf das Netz, bei der IT- wie Security-Teams bei Bedarf bis in die Tiefen der Bits & Bytes hinabsteigen können, um konkrete Ereignisse präzise zu analysieren. Die Metriken der über-

geordneten Network-Observability-Lösungen beziehen sich jedoch auf Verbindungen, Data in Motion und das Endanwendererlebnis, aber nicht so sehr auf die Komponenten dieser Verbindungen. Sie bilden die Basis für strategisches Handeln und die Einführung von automatisierten, proaktiven Prozessen.

Mit einer Network-Observability-Lösung sollen Netzwerk- und Security-Teams Netzwerkabhängigkeiten und -probleme proaktiv erkennen können, bevor sie sich auf die User oder Dienste auswirken. Sie entdeckt Troubleshooting-Probleme und Anomalien automatisch und entlastet so Netzwerk- und Security-Teams. Viele Observability-Tools sind speziell für Cloud-Umgebungen konzipiert.
Bei der Umsetzung wies Gartner in einem Report aus dem Jahr 2020 auf die Gefahr hin, dass zu viele, sich überlappende Tools die Komplexität und Kosten in die Höhe treiben. Demnach hätten viele Unternehmen bereits 15 und mehr Monitoring-Tools im Einsatz und wollten nicht noch weitere Komplexität hinzufügen. Bei der Einführung einer Observability-Lösung sollte deshalb untersucht werden, ob die bestehenden Lösungen nicht so angepasst werden könnten, dass sie auch Observability-Konzepte unterstützen. Andere Lösungen könnten zum Beispiel durch die neue Architektur ersetzt werden.



Wie Observability und vorhandene Monitoring-Tools miteinander verschmelzen

Nicht umsonst erkennt die Enterprise Strategy Group in ihrem aktuellen „Lagebericht Observability 2022“, dass Observability und vorhandene Monitoring-Tools miteinander verschmelzen. Auf diese Weise lassen sich Überlappungen und übermäßige Komplexität vermeiden. Die Marktforscher befragten im Auftrag von Splunk 1.250 Führungskräfte, die sich mit dem Thema Observability befassen. In diesem Rahmen ermittelten sie zudem die für Organisationen entscheidenden Faktoren für Observability-Lösungen. Das sind für etwa drei Viertel der Befragten das Monitoring der Netzwerkleistung (74 Prozent) sowie Sicherheit (73 Prozent). Außerdem nannten 59 Prozent von ihnen noch Log-Management-Lösungen.

Entscheidende Faktoren für Observability-Lösungen

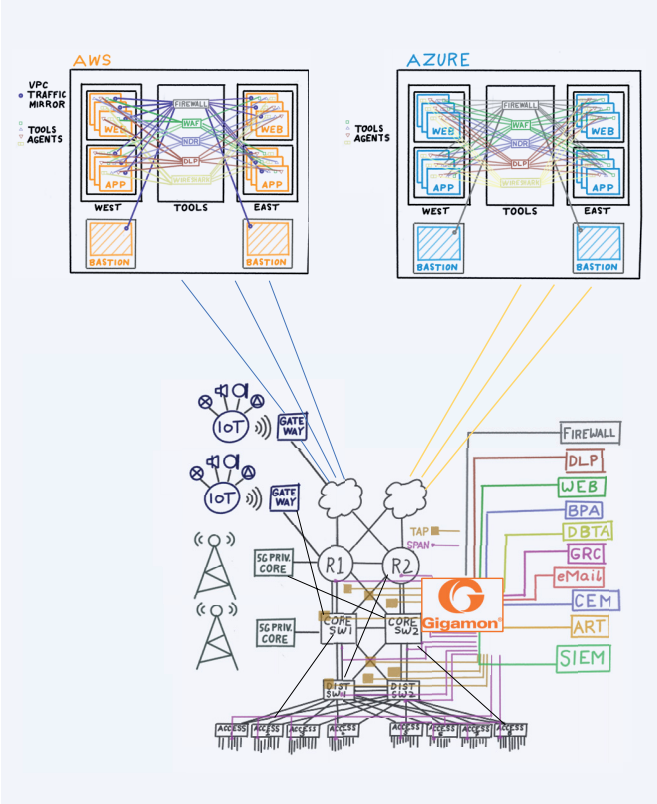
- ✓ Monitoring der Netzwerkleistung (74 Prozent der Befragten)
- ✓ Security-Monitoring (73 Prozent der Befragten)
- ✓ Log-Management (59 Prozent der Befragten)

Quelle: Lagebericht Observability 2022 der Enterprise Strategy Group im Auftrag von Splunk

Die Verschmelzung von Observability mit den vorhandenen Monitoring-Teams und -Lösungen zeigt sich beim Log-Management, dem Network-Performance- sowie dem Security-Monitoring: Bei 22 Prozent der befragten Unternehmen seien die Tools und Teams für das Log-Management bereits zusammengeführt, bei 51 Prozent geschehe dies gerade oder sei absehbar. Ähnliches gilt für das Network-Performance- sowie das Security-Monitoring: Hier seien demnach etwa ein Viertel der Tools und Teams (25 und 24 Prozent) schon eine Einheit, bei fast der Hälfte (49 Prozent) geschehe dies gerade oder sei in Planung.

Weshalb Netze mit Deep Observability effizienter und sicherer werden

Wer außerdem das Netzwerk- und Security-Management effektiver gestalten möchte, vereint nicht nur die Cloud-Observability mit den vorhandenen Netzwerk- und Security-Monitoring-Tools, um eine Übersicht über das Gesamtnetz zu erhalten, sondern integriert diese komplett in seine Netzwerk- und Security-Management-Umgebung. Dann kann eine Wächterinstanz für eine Deep Observability des Netzes in Form eines Next Generation Network Packet Brokers (NGNPB) eingeführt werden. In Cloud-Plattformen übernimmt das eine Software-Appliance. Deep Observability bietet den Blick von außen oder die netzbasierte Perspektive, die bei der Observability (MELT) fehlt. Sie extrahiert Netzwerkinformationen aus dem Datenverkehr und füllt die Sicherheitslücken. Wenn es um die Reaktion auf Vorfälle geht, führt der netzwerkbasierte Ansatz zu einer viel schnelleren Erkennung und Bekämpfung von Risiken. Deep Observability findet mit Hilfe von Data in Motion die Spuren, die zu verdächtigen Aktivitäten führen. Auf diese Weise vereinfacht Deep Observability das Management selbst hochkomplexer Multi-Cloud-Umgebungen.



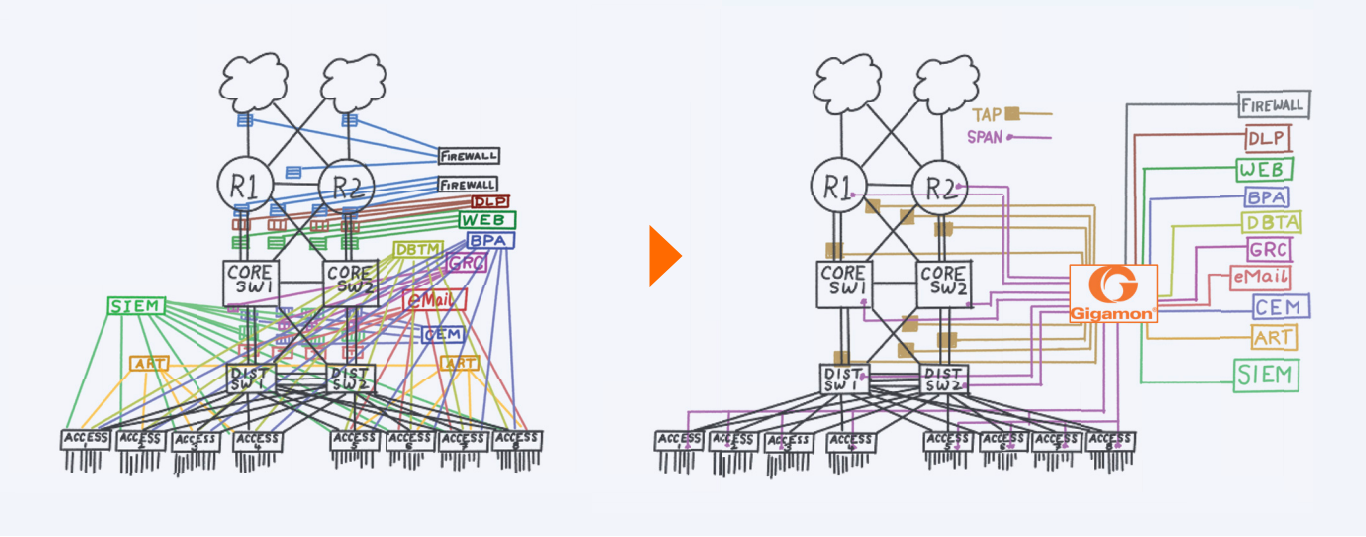
Deep Observability bindet die Traffic-Überwachung in den Clouds in die Gesamtsicht des Netzwerks ein.

Die Wächterinstanz kann einerseits in Echtzeit reagieren und stellt Administratoren andererseits einen Überblick über ihre gesamte IT-Umgebung bereit. Sie sichtet über alle Cloud-Plattformen und Netze der Unternehmens-IT hinweg die erfassten Daten und gemeldeten Ereignisse, filtert sie und leitet sie an die jeweils dafür prädestinierten Security- oder Netzwerkmanagement-Tools (NWM) weiter. Diese erhalten somit nur den für sie relevanten Traffic.

Damit muss nicht jede Monitoring-Lösung eine eigene Infrastruktur errichten, um ihre jeweilige Sicht auf das Netzwerk bereitstellen zu können. Vielmehr nutzen alle Tools eine gemeinsame und lückenlose Infrastruktur für die Netzwerksichtbarkeit. Das sorgt für eine übersichtliche Installation und schont die Ressourcen für NWM- und Security-Infrastruktur.

Zudem reduzieren sich mit dem maßgeschneidert zugeteilten Traffic die Kapazitätsanforderungen der Tools und Lösungen. Anmeldungen an Endpunkten erzeugen beispielsweise riesige, oft irrelevante Datenmengen, die das Endpoint-Analyse-Tool auswerten muss. Mit der Datenmenge steigen aber die Kosten für die Security-Infrastruktur. Außerdem verlängert sich die Zeitspanne bis zur Erkennung und Prüfung eines Vorfalls, weil die Abfragen länger dauern. Somit beschleunigt der passgenau gefilterte Traffic die Prüfung und das Reaktionsvermögen der Lösungen, was bei Cyberangriffen großen Schaden abwenden kann.

Davon profitieren zahlreiche Security-Monitoring-Systeme, etwa Next-Generation- und Web-Application-Firewalls, die E-Mail-Überwachung sowie Advanced-Threat-Detection und Access-Rights-Management-Lösungen. Gleiches gilt für das SIEM (Security Information and Event Management), das Access-



Herkömmliche Monitoring-Ansätze sind unflexibel, lassen Blind Spots zu und kosten viel Geld. Deep Observability macht das Netz sicherer, effizienter und agiler.

Control- und Security-Management sowie für Intrusion-Detection-Systeme (IDS), Data-Leak-Prevention-Software und Forensik-Tools. Zudem lässt sich zum Beispiel Behavioral-Analytics-Software, die das User-Verhalten auf Plattformen analysiert, integrieren. Auch Software, die den Umgang mit vertraulichen Informationen oder die Einhaltung von Business Partnership Agreements überwacht, kann mit einfließen.

Warum eine netzwerkbasierte Sichtbarkeit verdächtige Aktionen schnell entdeckt

Der NGNPB aggregiert, analysiert, filtert und übermittelt den Traffic nicht nur. Er blockt und isoliert außerdem sofort Daten bei Verdacht auf Mal- oder Ransomware und alarmiert automatisch das Security-Management-System. Darüber hinaus ergänzt er bei erkannten Sicherheitsverletzungen den Input für Security-Tools mit Telemetriedaten aus dem Netzwerk. Da die Security-Lösungen jeweils getrennte Sichten auf die IT bieten, sind manche Auffälligkeiten ansonsten nicht erkennbar oder nur schwer zu deuten. Ein Endpoint-Detection-&-Response-System beispielsweise erkennt Sicherheitsverletzungen an Endpunkten, kann aber keine Aussage über ihre Ursachen treffen. Ohne die zugehörigen Telemetriedaten bleiben sowohl das Ausmaß der Verletzung als auch die Absicht des Zwischenfalls unbekannt. Dank der integrierten Intelligenz kann der NGNPB aus den Netzwerkverkehrsdaten die Detailinformationen aufspüren, die auf verdächtige Aktivitäten hinweisen. Anschließend leitet er diese an das jeweilige Security-Tool weiter – in diesem Fall an das Endpoint-Detection-&-Response-System.

Wie Sie mit Deep Observability Zero-Trust-Architekturen in Cloud-Umgebungen integrieren

Immer mehr Organisationen setzen auf Zero-Trust-Architekturen in Cloud-Umgebungen. Für deren Umsetzung müssen Security-Teams zunächst die Abhängigkeit zwischen Anwendungen und Workloads verstehen, damit sie darauf abgestimmte Richtlinien für die Zugriffskontrolle festlegen können. Ohne die netzwerkbasierte Sichtbarkeit, die ihnen ein Netz mit Deep Observability bereitstellt, gelingt das kaum.

Wie Sie mit Deep Observability Ransomware-Angriffe abwehren können

Laut dem „Verizon Data Breach Investigations Report 2022“ stiegen Verstöße durch Ransomware in nur einem einzigen Jahr um 13 Prozent an. Dieser Anstieg sei größer als in den letzten fünf Jahren zusammen, so die Verfasser. Während Kriminelle immer raffiniertere Formen von Malware einsetzen, erweise sich Ransomware als besonders erfolgreich, wenn es darum gehe, den illegalen Zugriff auf private Informationen auszunutzen. Die Angreifer seien in der Regel sehr gut über die Angriffs-

fläche ihres Opfers informiert. Dieses Wissen umfasst zum Beispiel:

- Systeme und Dienste mit Internetzugriff
- Schwachstellen oder ungepatchte Systeme
- Die Nutzung spezifischer Technologien, etwa von Sicherheitslösungen oder Drittanbietern
- Den potenziellen Cloud-Footprint

Hier lässt sich das Angriffsrisiko schon mindern, wenn keine veraltete oder anderweitig anfällige Software im Netz verwendet würden und regelmäßige Software-Updates gemacht würden.

Ungepatchte Schwachstellen gehören zu den größten Risiken; Kriminelle nutzen sie als erste Angriffsvektoren. Deshalb sollten Security-Teams diese Sicherheitslücken schnell und automatisch nach einer vorgegebenen Priorisierung schließen. So gelingt zunächst die effiziente Abwehr der größten Risiken. Lässt sich eine neue Bedrohung nicht sofort patchen, bietet es sich als Notlösung an, das Netz über das Netzwerk-Monitoring und Endpunkt-Management zu schützen, etwa über eine schnell umgesetzte Netzwerkregel oder eine Endpunktsignatur in Kombination mit einem verhaltensorientierten Schutz.

Ransomware-Angriffe erfolgen zunehmend automatisiert, sodass Angreifer heute in wenigen Stunden die Kontrolle über ein Netzwerk oder eine Domäne erhalten. Entsprechend wichtig ist es, dass das Security-Team solche Attacken umgehend entdeckt und abwehrt. Meist sind sie vorhersehbar und leicht zu erkennen, deshalb können sie größtenteils ebenfalls automatisiert abgewehrt werden. Sie sind zum Beispiel per Deep Observability informationsbasiert über verschiedene Tools hinweg erkennbar. Die zugehörigen automatischen Aktionen und Reaktionen sollten angepasst an die Schwere des Angriffs und die Kritikalität des angegriffenen Systems sein.

Viele Ransomware-Angreifer dringen über offene Tools und Lösungen für den Remote-Zugriff in das Firmennetz ein. Deshalb sollten diese per Multi-Faktor-Authentifizierung sowie VPN- oder Zero-Trust-Architektur geschützt sein. Außerdem sollte das Security-Team zwischen Perimeter und innerem Netzwerk eine Schutzschicht errichten. Der unbefugte Zugriff auf diese Bereiche lässt sich zum Beispiel mit Defense-in-Depth-Strategien verhindern. Darüber hinaus erkennen bei Deep Observability auch Netzwerk- und Endpunktprävention Angriffe und können entsprechend auf sie reagieren. So tragen sie dazu bei, dass Malware, Command-and-Control-Kommunikation (C2) von Hackern sowie Ransomware keine Chance haben.

Endpoint- und Network-Detection-&-Response-Tools gelten auch als adäquates Mittel, um

böswillig verwendete eigene Dateien als plötzlich auftretende Anomalien aufzuspüren. Das gilt auch für den lateralen Wechsel des Angreifers zu einem anderen System oder seine C2-Kommunikation nach außen. Beides lässt sich mit diesen Tools entdecken und unterbinden. Selbst wenn Angreifer ihren Datenverkehr verschlüsseln, lassen sich zumindest aus den Metadaten Informationen und Muster ermitteln und Angriffe als solche identifizieren. So trägt Deep Observability dazu bei, Unternehmensnetze vor Schaden zu schützen.

Damit ein NGNPB eine derart umfassende Deep Observability bereitstellen kann, sollte er über folgende Funktionen verfügen:

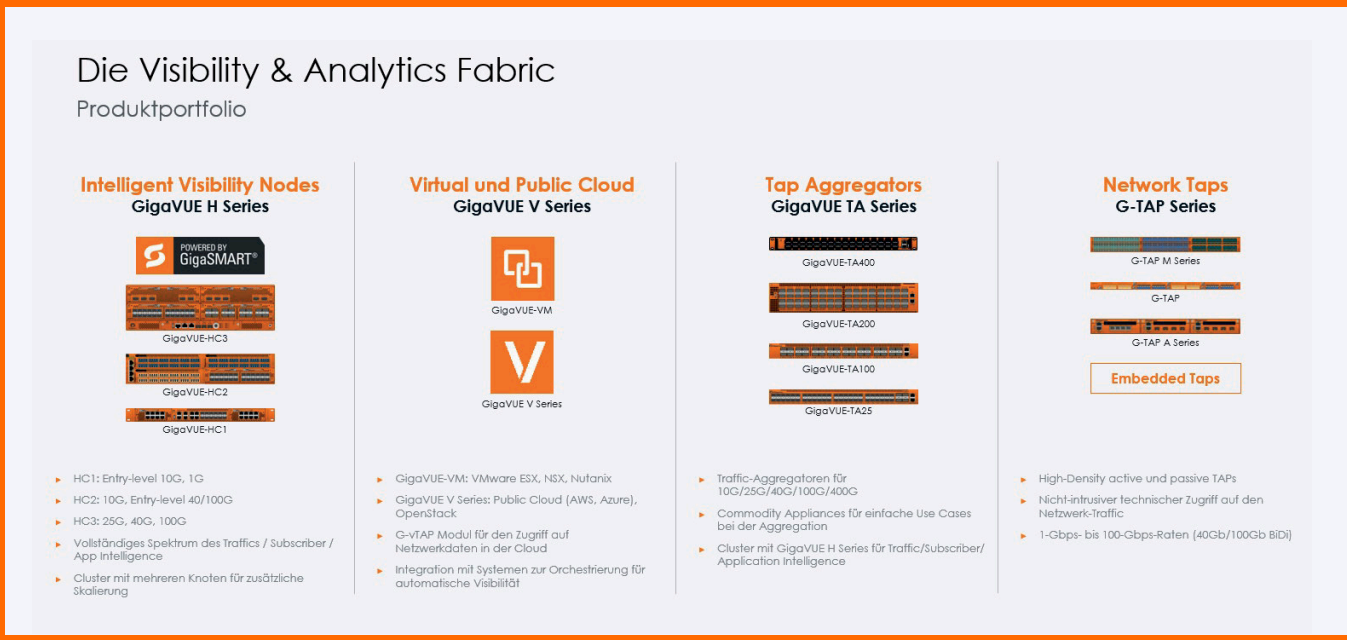
Funktionen der Wächterinstanz NGNPB

- ✓ Bedrohungsabwehr (Threat Prevention)
- ✓ Loadbalancing
- ✓ Ausfallsichere Inline-Netzwerk-Security-Tools
- ✓ Zahlreiche Tools zur Erkennung von Bedrohungen von außen
- ✓ Präzise Netzwerk-Monitoring-Lösungen
- ✓ Analyse der Netzwerk-Performance
- ✓ Bündelung von High-Speed-Netzwerk-TAPs

Damit ermöglicht er eine umfassende Sichtbarkeit der physikalischen, virtuellen und cloudbasierten Infrastruktur. Er kann Netzwerk-Traffic bündeln, per Loadbalancing die Verfügbarkeit und Reaktionszeit von Anwendungen verbessern und verschlüsselte Kommunikation entschlüsseln, während er zugleich Dienste für andere Management- und Security-Tools ausführt. So stellt er zum Beispiel den Security-Tools die notwendigen Kontextinformationen in Form von Telemetriedaten aus dem Netzwerk zur Verfügung. Auf diese Weise lassen sich selbst mehrschichtige digitale Anwendungen komfortabel überwachen und absichern. Das verbessert die Leistungsfähigkeit der Anwendungen und die Netzwerksicherheit. Die gesamte Unternehmens-IT erhält eine elastische Sichtbarkeit und Analysen für alle Data in Motion über das gesamte Hybrid-Cloud-Netzwerk hinweg und kann schnell, sicher und innovativ agieren.

Da mit Deep Observability ein NGNPB eine strategische Komponente des Netzwerks ist, spielt es eine entscheidende Rolle, dass das Produkt auf innovative Partnerlösungen setzt, über eine aktive Anwender-Community sowie ein globales Support-Netz verfügt.

Wie eine Deep-Observability-Lösung in der Praxis aussieht



Als Next-Generation Network Packet Broker (NGNPB) optimiert die Gigamon Visibility and Analytics Fabric das Monitoring der Performance sowie der Security und verringert zugleich die Komplexität in der Infrastruktur. NetOps- und InfoSec-Teams maximieren damit die Sichtbarkeit für das Netzwerk-Monitoring und die Security unabhängig davon, ob Unternehmen überwiegend in der Cloud, On-Premises oder in einer Mischung aus beidem arbeiten. Das System bietet Deep Observability des Netzwerk-Traffics für Applikationen und Services, die in der Hybrid Cloud laufen. Das einheitliche Management stellt eine allumfassende Sichtbarkeitsschicht bereit, die die Data in Motion aggregiert und in intelligenter Weise erweiterte Informationen nutzt, bevor ausgewählter Traffic an Monitoring- und Security-Tools weitergeleitet wird.

MEHR ERFAHREN ÜBER NGNPB

MEHR ERFAHREN ÜBER DEEP OBSERVABILITY

Über Gigamon

Gigamon bietet mit seiner Deep Observability Pipeline eine Plattform, die auf der Netzwerkebene verwertbare Informationen nutzt, um die Performance von Cloud-, Sicherheits- und Observability-Tools zu steigern.

Damit geht der Anbieter über aktuelle Beobachtungsansätze hinaus, die ausschließlich auf der Aufzeichnung von Metriken, Ereignissen, Logs und Tracks (MELT) beruhen.

Das Unternehmen erweitert den Wert der Cloud-, Sicherheits- und Observability Tools seiner Kunden um Echtzeit-Netzwerkinformationen, die aus Paketen, Flows und Anwendungs-Metadaten abgeleitet werden, um so eine tiefgreifende Verteidigung und ein umfassendes Performancemanagement hybrider und Multi-Cloud-Infrastrukturen zu ermöglichen.

Gigamon betreut mehr als 4.000 Kunden weltweit, darunter über 80 Prozent der Fortune-100-Unternehmen, 9 der 10 größten Mobilfunkanbieter und hunderte Regierungs- und Bildungseinrichtungen.

MEHR ERFAHREN

©2022 Gigamon. Alle Rechte vorbehalten. Gigamon und das Gigamon-Logo sind Marken von Gigamon in den USA und/oder anderen Ländern. Gigamon Trademarks finden Sie unter www.gigamon.com/legal-trademarks. Alle anderen Marken sind Marken der jeweiligen Eigentümer. Gigamon behält sich das Recht vor, diese Publikation ohne Vorankündigung zu ändern, zu modifizieren, zu übertragen oder anderweitig zu revidieren.

Gigamon®

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