Enterprise Strategy Group | Getting to the bigger truth.™

ESG-Whitepaper

Einheitliches NPM von Riverbed kann die Netzwerksicherheit und den Netzwerkbetrieb unterstützen und verbessern

Autor: Jon Oltsik, Senior Principal Analyst and Fellow, Enterprise Strategy Group

Juni 2021

Dieses ESG-Whitepaper wurde in Auftrag gegeben von Riverbed und wird unter Lizenz von ESG veröffentlicht.

Inhalt

Kurzzusammenfassung

ESG-Untersuchungen zeigen, dass 43 % der Unternehmen als erste Verteidigungslinie bei der Erkennung und Reaktion auf Bedrohungen Tools zur Netzwerk-Traffic-Analyse (NTA) einsetzen.[1] Diese Strategie entspricht dem alten Leitsatz zum Thema Sicherheit: „Das Netzwerk lügt nicht“. Bei Cyberangriffen werden Netzwerke unauffällig abgetastet und Verbindungen zu externen Ressourcen wie C2- und Malware-Servern hergestellt. Dies ist Teil umfassender Angriffskampagnen. Die Identifizierung schädlicher Verbindungen und Payloads im Netzwerk kann die Bedrohungserkennung beschleunigen und die Auswirkungen minimieren.

Unternehmen setzen heute zwar auf NTA und Technologien für Netzwerkerkennung und Reaktion, aber die Daten von ESG deuten darauf hin, dass trotzdem nicht alles optimal läuft. Viele Firmen haben Probleme damit, die Netzwerksicherheit nach Bedarf zu skalieren, zu optimieren und zu operationalisieren. Warum ist die Netzwerksicherheit so ein schwieriges Thema und wie können Unternehmen diese Komplexität in den Griff bekommen? Das Fazit dieses Whitepapers lautet wie folgt:

- **Die Netzwerksicherheit wird Jahr um Jahr schwieriger.** Unternehmen nutzen interne und cloudbasierte Netzwerke (z. B. mit hybrider Infrastruktur) für Initiativen wie die Digitalisierung und die Unterstützung mobiler Mitarbeiter. Netzwerke sind für Unternehmen eindeutig geschäftskritisch. Daher ist es jedoch umso alarmierender, dass 85 % der Sicherheitsexperten der Meinung sind, die Netzwerksicherheit sei in den letzten zwei Jahren schwieriger geworden. Grund dafür seien immer gefährlichere Bedrohungen, eine wachsende Angriffsfläche und eine steigende Anzahl von Netzwerksicherheitstools.[2] Diese Probleme führen zu immer höheren Cyberrisiken, die Unternehmen anfällig gegenüber folgenschweren Cyberangriffen machen.

- **Die Zusammenarbeit von Sicherheits- und Netzwerkteams lässt oft zu wünschen übrig.** Sicherheits- und Netzwerkteams müssen sich der Aufgabe der Netzwerksicherheit gemeinsam annehmen, aber fast die Hälfte der Unternehmen glaubt, dass diese zwei Abteilungen oft Probleme bei Kommunikation und Zusammenarbeit haben.

- **Zur Lösung dieser Probleme können Unternehmen gemeinsam genutzte Datenquellen und durchgängige Netzwerktransparenz einsetzen.** Netzwerk- und Sicherheitsteams verwenden oft unterschiedliche Tools zur Netzwerküberwachung. Dies kann zu Verwirrung führen und Redundanz sowie hohe Kosten zur Folge haben. Da beide Abteilungen im Endeffekt auf dieselben Daten zugreifen, können Unternehmen laut ESG von Lösungen profitieren, mit denen sich Netzwerkdaten für sicherheits- und betriebsrelevante Anwendungsfälle erfassen, verarbeiten und analysieren lassen. Hier tritt das einheitliche NPM von Riverbed auf den Plan. Die Kombination aus NetProfiler und AppResponse sorgt für umfassende Netzwerktransparenz, hochpräzise Netzwerkdaten und die Möglichkeit, aus vielen Perspektiven (interne Netzwerke, cloudbasierte Netzwerke, WAN usw.) Einblicke in das Netzwerkverhalten zu erlangen. In den letzten Jahren hat Riverbed seine NPM-Tools für Sicherheitsanforderungen instrumentiert und bietet eine ambitionierte Roadmap, um die Unterstützung für Sicherheitsfunktionen künftig zu beschleunigen. Dadurch kann das einheitliche NPM von Riverbed als zentrale Datenquelle dienen und die Effizienz und die Produktivität von Sicherheits- und Netzwerkteams erhöhen.

Der Stand der Netzwerksicherheit

Netzwerksicherheitstechnologien gibt es bereits seit den 1980ern. Damals brachte das US-Unternehmen Digital Equipment Corporation die erste kommerzielle Firewall auf den Markt. Mehr als 30 Jahre später sollte man davon ausgehen, dass die Sicherheit in diesem Bereich ausgereift und unter Kontrolle ist, doch Daten von ESG zeichnen ein anderes Bild. Laut ESG-Untersuchungen glauben 85 % der Unternehmen, dass die Netzwerksicherheit heute eine

[1] Quelle: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.
[2] Quelle: ESG Research Report, *The State of Network Security: A Market Poised for Transition*, März 2020.

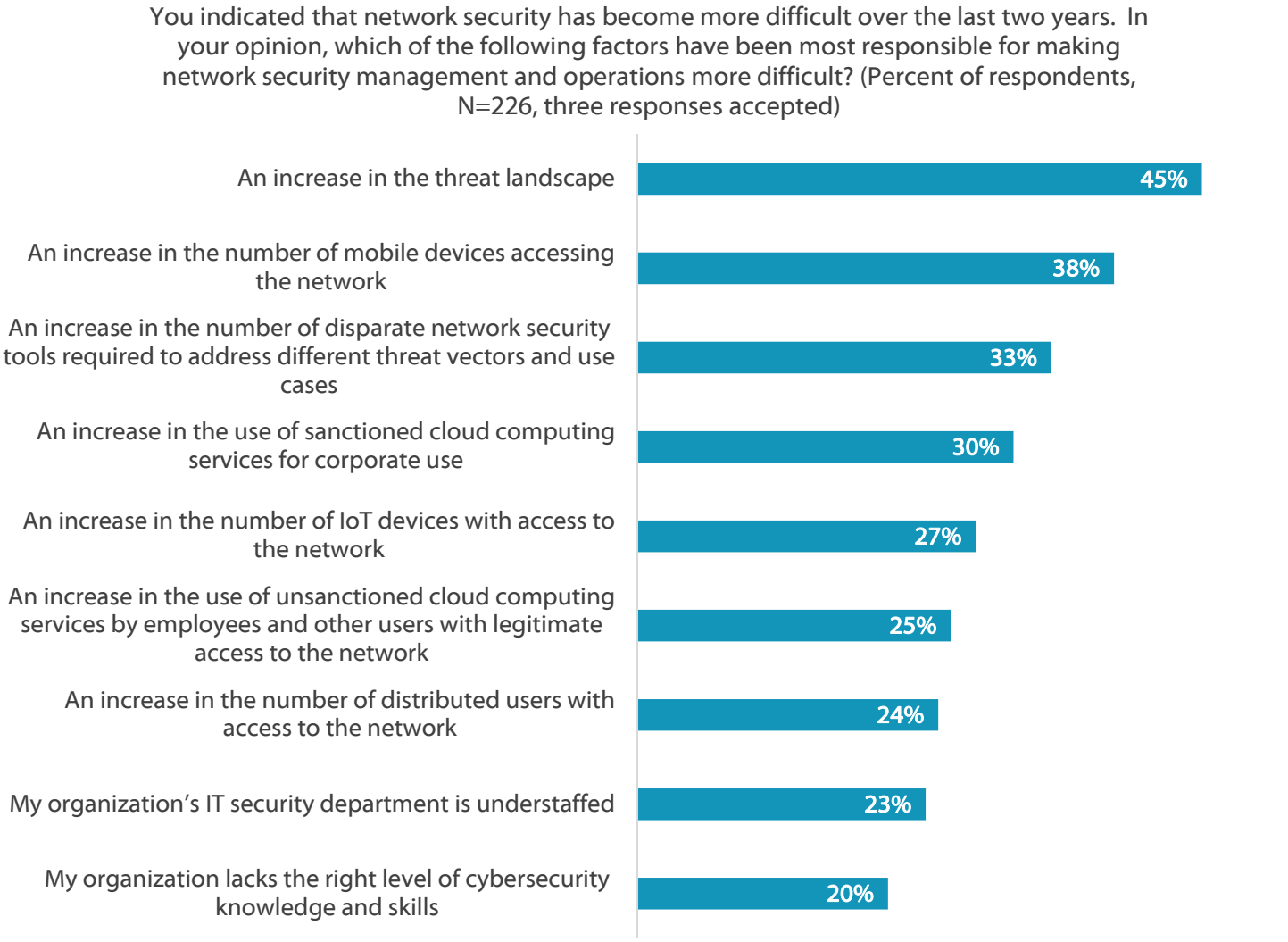
größere Herausforderung darstellt als noch vor zwei Jahren. Warum? Hierfür gibt es mehrere Gründe, unter anderem folgende (siehe Abbildung 1):[3]

- **Die Zahl der Cyberbedrohungen hat zugenommen.** In den ersten sechs Monaten des Jahres 2021 kam es zu groß angelegten Cyberangriffen wie SUNBURST und Attacken, die auf bestimmte Organisationen ausgerichtet waren, z. B. die südkoreanische Atombehörde, Carnival Cruise Lines, Fleischfabriken des Konzerns JBS, Colonial Pipelines und die Supermarktkette Wegmans. Anhand dieser unvollständigen Liste wird deutlich, dass jede Region, Branche oder Organisation von Angriffen betroffen sein kann. Um dieser Entwicklung entgegenzuwirken, benötigen Sicherheitsexperten umfassende Einblicke in Netzwerke, konkrete Erkennungsregeln und fundierte forensische Daten für zeitgerechte und präzise Untersuchungen.
- **Die Angriffsfläche wächst.** ESG-Untersuchungen zeigen einen Anstieg bei der Anzahl der eingesetzten Mobilgeräte, IoT-Geräte, nicht genehmigten Anwendungen und Cloud-Services. Zusammengenommen ergeben diese Trends eine immer größere Angriffsfläche. Im Hinblick auf die Netzwerksicherheit benötigen SOC-Teams detaillierte Einblicke in sämtliche Anwendungen, Geräte, Verbindungen und Protokolle. Da viele Unternehmen nicht über dieses Maß an Transparenz verfügen, sind SOC-Teams gezwungen, auf den begrenzten Einblicken und den verfügbaren historischen Daten beruhende Vermutungen anzustellen – dies ist im besten Fall eine Notlösung.
- **Es werden immer mehr Netzwerksicherheitstools eingesetzt.** Angesichts der Kombination aus komplexen Bedrohungen und einer wachsenden Angriffsfläche setzen viele Unternehmen neue Arten von Sensoren und Erkennungstools ein. Dies hat jedoch zu einem erheblichen Anstieg bei der Zahl der Sicherheitswarnungen geführt. Jetzt wird von SOC-Analysten erwartet, dass sie sich der wachsenden Menge von Sicherheitsmeldungen annehmen und diese mit hoher Dringlichkeit untersuchen – eine unmögliche Aufgabe für die meisten Unternehmen.

Erwähnenswert ist außerdem, dass 23 % der Befragten angaben, dass ihre IT-Sicherheitsabteilung unterbesetzt ist. 20 % wiederum sind der Ansicht, dass ihrem Unternehmen das erforderliche Maß an Wissen und Kompetenz im Bereich der Cybersicherheit fehlt. Da Cybersicherheitskompetenzen weltweit Mangelware sind, werden sich diese Trends voraussichtlich fortsetzen.

[3] Ebd.

Abbildung 1. Gründe dafür, dass die Netzwerksicherheit komplexer geworden ist



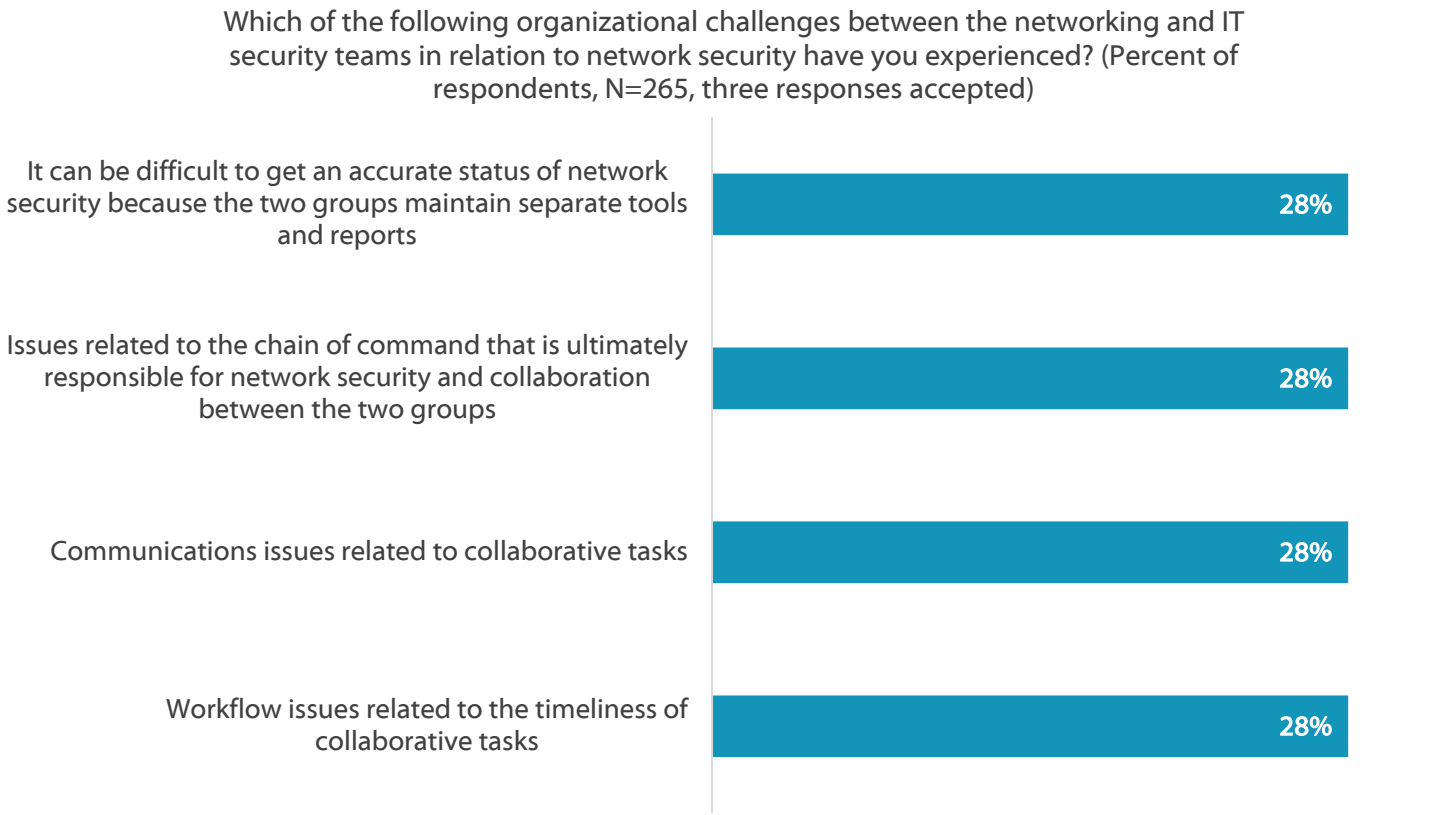
Quelle: Enterprise Strategy Group

Die organisatorische Kluft zwischen Netzwerk und Sicherheit

Schutz, Erkennung und Problembehebung sind eine gemeinsame Aufgabe von Sicherheits- und Netzwerkteams. Die Zusammenarbeit zwischen diesen Abteilungen ist jedoch nicht immer von Harmonie geprägt. 44 % der Unternehmen gaben an, dass diese Beziehung oft dadurch belastet ist, dass Teams separate Daten und/oder Tools nutzen, voneinander unabhängigen Vorgesetzten unterstehen und bei gemeinsamen Aufgaben schlecht kommunizieren. Zudem sorgen Probleme im Prozessablauf oft für Verzögerungen (siehe Abbildung 2):[4]

[4] Quelle: ESG Master Survey Results, *Network Security Trends*, März 2020.

Abbildung 2. Die vier größten organisatorischen Probleme zwischen Netzwerk- und IT-Sicherheitsteams



Quelle: Enterprise Strategy Group

Die ESG-Daten beschreiben eine besorgniserregende Situation, in der die Netzwerksicherheit immer komplexer wird und die zwei Abteilungen, die vornehmlich für die Netzwerksicherheit zuständig sind, nicht gut zusammenarbeiten. Wenn sich dieser Zustand nicht ändert, wird es zu einem sprunghaften Anstieg der Cyberrisiken kommen, da Netzwerk- und Sicherheitsteams kaum mit den Aufgaben des täglichen Betriebs, den Prozessen zur Bedrohungserkennung und der Reaktion auf Vorfälle fertig werden. Um dieser alarmierenden Entwicklung Einhalt zu gebieten, müssen CISOs sich mit ihren Kollegen aus IT- und Netzwerkabteilung zusammensetzen, um so schnell wie möglich eine Lösung zu finden.

Netzwerktransparenz bietet eine Grundlage für den Sicherheitsbetrieb

Kluge CISOs wissen, dass es zur Bewältigung der Netzwerksicherheitsprobleme erforderlich ist, an entscheidenden Punkten im Netzwerk (z. B. Eingangs-/Ausgangspunkten, Rechenzentren, innerhalb von Public Clouds) den gesamten Datenverkehr zu überwachen. Laut den Ergebnissen von ESG findet diese Überwachung bereits statt – 87 % der Unternehmen nutzen bereits NTA-Tools zur Bedrohungserkennung und -reaktion und 43 % geben an, NTA als „erste Verteidigungslinie“ einzusetzen, um ungewöhnliche/verdächtige/bösartige Netzwerkaktivitäten wie laterale Bewegungen, Network Enumeration, C2-Traffic und Datenexfiltration zu erkennen und entsprechende Maßnahmen einzuleiten.[5] Viele Firmen setzen für Folgendes zudem auf Netzwerktransparenz:

- **Netzwerk- und Anomalieerkennung.** Wie der Marketing-Guru Peter Drucker einmal sagte: „You can‘t manage what you can‘t measure“ – Was man nicht messen kann, kann man auch nicht managen. Diese Aussage trifft definitiv auf die Netzwerksicherheit zu. Mithilfe umfassender Netzwerktransparenz können unberechtigte

[5] Quelle: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

Geräte im Netzwerk erkannt, Traffic-Muster überwacht und außergewöhnliche Datenbewegungen identifiziert werden. Das gilt für den gesamten Datenverkehr – Nord-Süd und Ost-West – und ebenso für den Traffic innerhalb einer Public-Cloud-Infrastruktur. Idealerweise sollten CISOs Einblicke in den gesamten Traffic haben, um komplexe mehrstufige Angriffe erkennen zu können.

- **Fundierte forensische Details.** Mit führenden Netzwerktransparenztools kann der Verlauf aller Verbindungen erfasst werden. So können Informationen darüber abgerufen werden, welche Assets kommuniziert haben, wann diese Kommunikation stattfand und welche Ports, Protokolle, Payloads usw. beteiligt waren. Diese Details sind entscheidend für die Bedrohungserkennung, die Untersuchungspriorisierung und die Untersuchungen selbst. Wenn Sicherheitsanalysten eine Meldung von einer Erkennungstechnologie erhalten (IDS/IPS, EDR, SIEM usw.), setzen sie in der Regel Netzwerktransparenztools, NetFlow/IPFIX und Paketerfassungstools ein, um einen Einblick darin zu gewinnen, was passiert ist, wann es passiert ist und welche Netzwerkknoten involviert waren. Anschließend können mit der Bedrohungssuche beauftragte Mitarbeiter Flow- und Paketdaten nutzen, um eine lückenlose Aufstellung historischer Ereignisse abzurufen. Um sicherzustellen, dass diese fundierten forensischen Daten auf Abruf verfügbar sind, sollten Unternehmen eine hochpräzise Always-on-Überwachung und -Erfassung betreiben. Es ist nachvollziehbar, dass Unternehmen einfach eine stichprobenartige Untersuchung durchführen wollen, die schneller vonstatten geht und günstiger ist. Dabei entstehen jedoch erhebliche Lücken im Ereignisverlauf, die möglicherweise nicht geschlossen werden und weitaus kostspieliger sein können, wenn eine vollständige forensische Analyse für einen Aufpreis erhältlich ist.

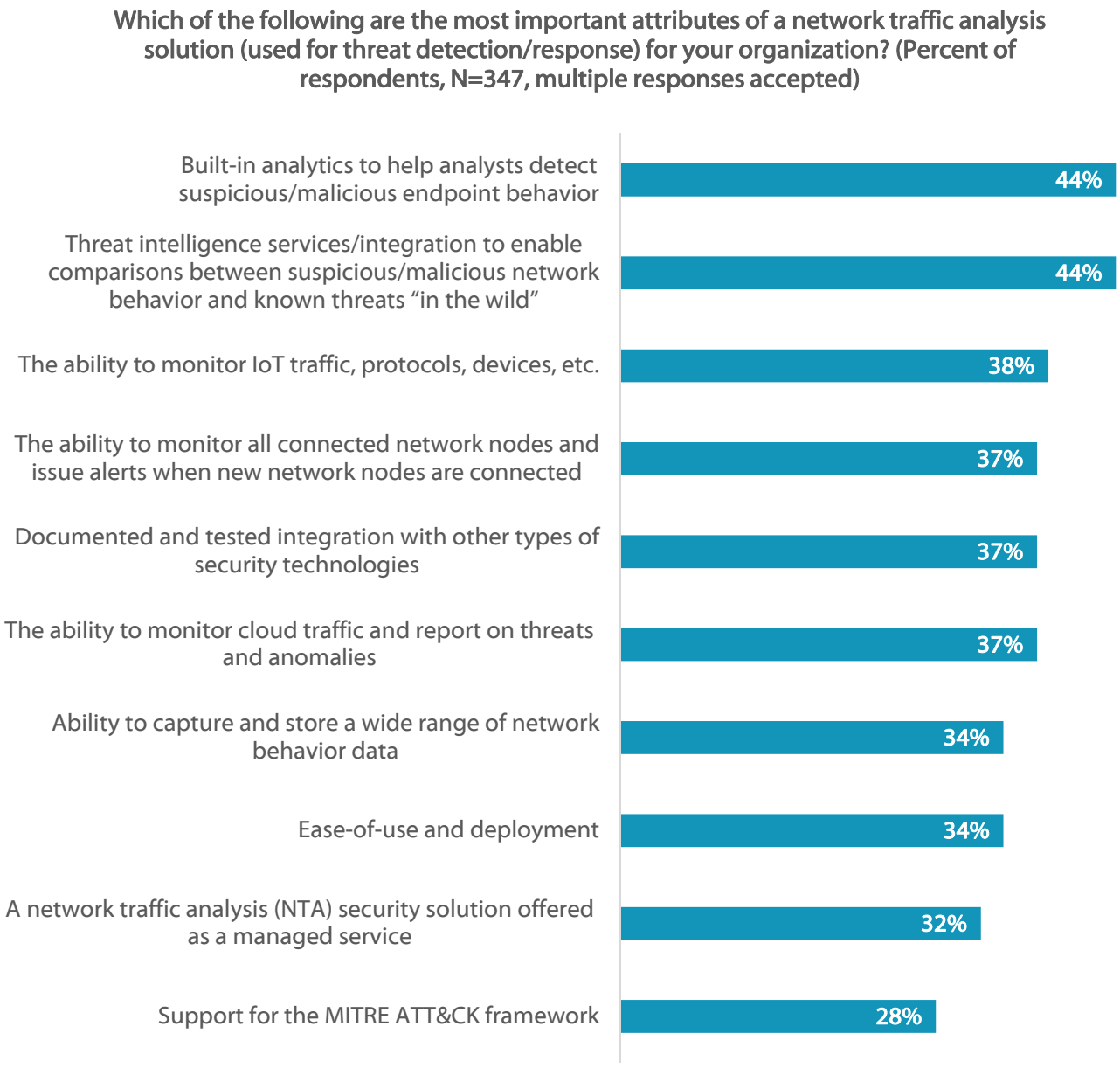
- **Sicherheitsstrategie.** Da die Netzwerktransparenz Einblicke in Netzwerkkommunikationsmuster ermöglicht, können Sicherheitsentwickler diese Daten als Orientierungshilfe für laufende Projekte in Bereichen wie Mikrosegmentierung und Zero Trust verwenden. Das kann zur Reduzierung der Angriffsfläche und damit zur Risikominimierung beitragen.

Wie zuvor erwähnt, wird die Netzwerktransparenz oft durch NTA-Tools (Netzwerk-Traffic-Analyse) unterstützt. Aus den Untersuchungen von ESG geht hervor, dass Netzwerk- und Sicherheitsexperten eine lange Liste von Anforderungen für diese Art von Technologie haben. Zu den wichtigsten Eigenschaften von NTA-Tools zählen integrierte Analysefunktionen für die Bedrohungserkennung, Bedrohungsinformationen für die Anreicherung von Netzwerkdaten, die Möglichkeit zur Überwachung von IoT-Geräten/-Traffic und die Möglichkeit zur Überwachung von Netzwerkknoten, um die Netzwerksicherheit zu wahren (siehe Abbildung 3).[6]

Führende Netzwerktransparenztools sollten außerdem dazu beitragen, die Lücke zwischen Sicherheits- und Netzwerkteams zu schließen. Dazu müssen sie ein gemeinsames Daten-Repository bereitstellen, das sowohl Netzwerkanwendungsfälle wie Anwendungs- und Netzwerk-Performance-Management unterstützt, als auch Sicherheitsanwendungsfälle wie Bedrohungserkennung, Reaktion auf Vorfälle, forensische Untersuchungen und Bedrohungssuche. Die besten Lösungen erfassen, verarbeiten und analysieren 100 % der Daten an strategischen Punkten im Unternehmens- und Cloud-Netzwerk, bieten Transparenz und Analysen aus mehreren Blickwinkeln des Netzwerks und stellen hochpräzise Netzwerkdaten bereit.

[6] Quelle: ESG Brief, Key Attributes of a Network Traffic Analysis Solution, September 2019.

Abbildung 3. Die wichtigsten Eigenschaften von NTA-Lösungen



Quelle: Enterprise Strategy Group

Netzwerktransparenz mit Riverbed

CISOs steht eine Fülle von Netzwerktransparenztools zur Auswahl. Wenn sie die Lücke zwischen Sicherheits- und Netzwerkteams schließen wollen, hilft ihnen ein weiteres Sicherheitstool jedoch nicht weiter. Eine Alternative, von der Unternehmen profitieren können, sind Netzwerktransparenztools, die den Anforderungen und Anwendungsfällen beider Teams gerecht werden.

Der Branchenveteran Riverbed bietet eine hybride Lösung, die die Anforderungen sowohl von Sicherheits- als auch von Netzwerkteams erfüllen. Eine Riverbed-Lösung kann auf den Produkten zur Überwachung der Netzwerk-Performance (NPM) aufgebaut werden: NetProfiler für Aufzeichnungen zum Datenfluss und AppResponse zur vollständigen Paketerfassung. Mit dieser Kombination können Unternehmen Daten aus dem gesamten Netzwerk erfassen, um umfassende Einblicke in die Netzwerkaktivitäten zu erzielen. Außerdem erhalten sie dadurch die Möglichkeit, das Netzwerk aus mehreren Blickwinkeln zu überwachen – z. B. am Netzwerkrand, in der Cloud und in den eigenen Rechenzentren, innerhalb des Ost-West-Traffics in internen Netzwerken und an Remote-Standorten, die mit dem WAN verbunden sind. Neben der Transparenz bietet Riverbed spezielle Funktionen für die Netzwerksicherheit:

- **Aktive Bedrohungserkennung.** Riverbed-Sicherheitslösungen unterstützen IoC-Sperrlisten, verarbeiten Bedrohungs-Feeds, um Daten anzureichern und in einen Kontext zu setzen, und erfassen Netzwerk-Baseling für die Anomalieerkennung. Das verbessert den Schutz und die Erkennung von Bedrohungen.

- **Forensische Untersuchungen.** Wenn Sicherheitsanalysten einen Verdacht bezüglich eines möglichen Cyberangriffs haben, müssen sie die Möglichkeit haben, detaillierte, historische Netzwerkaktivitäten in Echtzeit abzurufen. Für diese Aufgabe ist das einheitliche NPM von Riverbed ausgelegt und bietet hochpräzise Flow- und Paketdaten für Anwendungsfälle wie Sicherheitsuntersuchungen und die Suche nach Bedrohungen. Riverbed hat sogar eine API erstellt, die SOC-Teams ermöglicht, Pakete basierend auf bestimmten Auslösern zu erfassen, beispielsweise Verbindungen zu unzulässigen IP-Adressen oder Internetdomänen.

- **Erkennung und Schutz vor DDoS-Angriffen.** Anders als viele NTA-Tools bietet Riverbed außerdem DDoS-Erkennung und -Schutz. Durch die Konsolidierung dieser Funktionalität in die einheitliche NPM-Lösung kann Riverbed dazu beitragen, die organisatorische Lücke zwischen Sicherheits- und Netzwerkteams zu schließen.

Dank hochpräziser Transparenz kann das einheitliche NPM von Riverbed Unternehmen zudem helfen, die Netzwerkkommunikation zusammenzuführen, wenn „Low-and-slow"-Cyberangriffe wie Advanced Persistent Threats (APTs) angezeigt werden. Bei diesen Kampagnen werden vielfältige Taktiken, Techniken und Verfahren angewendet, die einer bestimmten Angriffskette folgen, um in Systeme einzudringen, sich unauffällig in Netzwerken zu bewegen, Anmeldeinformationen abzugreifen und letztlich wertvolle Daten zu exfiltrieren. Riverbed sorgt außerdem für durchgängige Transparenz, um Unternehmen dabei zu unterstützen, das MITRE ATT&CK-Framework für typische MITRE ATT&CK-Anwendungsfälle zu operationalisieren, z. B. für die Vorfallserkennung, die Sicherheitsbewertung und -entwicklung, die Analyse von Informationen zu Cyberbedrohungen und realitätsnahe Bedrohungsszenarien. Darüber hinaus kann die Netzwerk- und Sicherheitsfunktionalität des einheitlichen NPM von Riverbed Unternehmen dabei helfen, Architekturlösungen für Zero Trust zu planen, zu testen und zu implementieren.

Das Fazit

Cybersicherheitsteams müssen Geschäfts- und IT-Initiativen unterstützen und gleichzeitig dafür sorgen, dass digitale Assets vor Angreifern geschützt sind. Die Aufgabe ist klar – trotzdem wird sie Tag für Tag schwieriger. Eine Flut an Sicherheitswarnungen und eine lückenhafte Netzwerktransparenz hindern SOC-Teams daran, mit dem Umfang und der Komplexität dieser Aufgabe Schritt zu halten. Sicherheitsteams benötigen eine synchronisierte Übersicht des Netzwerkbetriebs, mit klaren und umfassenden Einblicken in alle Vorgänge im Netzwerk.

Auch wenn Riverbed im Allgemeinen nicht als Anbieter von Sicherheitslösungen gehandelt wird, nutzen immer mehr Kunden die einheitlichen NPM-Lösungen des Unternehmens. Die Kombination aus NetProfiler und AppResponse ermöglicht Unternehmen, umfangreiche, lückenlose Einblicke in NetFlow/IPFIX- und Paketdaten im gesamten Netzwerk zu gewinnen. Mithilfe dieser Tools können Riverbed-Kunden verdächtige Verhaltensmuster identifizieren, Netzwerkdaten mit Informationen zu Cyberbedrohungen anreichern, schädliche IoCs sperren, DDoS-Angriffe abwehren und gleichzeitig die Voraussetzungen für das Netzwerk-Performance-Management erfüllen. Diese Kombination kann eine wertvolle Ergänzung für Sicherheits- und Netzwerkteams darstellen und ihnen ermöglichen, die Wirksamkeit der Cybersicherheit zu erhöhen, den Betrieb zu optimieren und die Zusammenarbeit zu stärken. Außerdem sind diese Daten von unschätzbarem Wert für ausführliche forensische Untersuchungen, mit denen Ursachen, Einstiegspunkte und Zeitachsen von Cyberangriffen offengelegt werden. Dies ist unerlässlich, wenn ein Angriff erkannt wurde.

The Enterprise Strategy Group ist ein Unternehmen für IT-Analysen, -Untersuchungen, -Tests und -Strategien, das marktrelevante Einblicke und Erkenntnisse für die globale IT-Community bereitstellt.

www.esg-global.com

contact@esg-global.com

+1 508 482 0188