riverbed

WHITEPAPER

Unternehmen resilient machen – mit dem Portfolio für Netzwerk-Performance-Management (NPM) von Alluvio

Netzwerke entwickeln sich ständig weiter, um mit schier unendlich vielen externen Entwicklungen zurecht zu kommen, etwa der Zunahme von Remote-Arbeit seit der Pandemie, aber auch mit internen Zielvorgaben wie Performance-Verbesserungen und der Skalierung bei stagnierenden Budgets. Angesichts dieser Herausforderungen müssen NetOps-Teams mehr denn je Netzwerke anpassen und neue Ansätze entwickeln können. Das ist der Treiber hinter dem, was als Resilienz für Unternehmen bezeichnet wird. Die Internationale Organisation für Normung (ISO) definiert Resilienz als: „die Fähigkeit, Veränderungen in der Umgebung aufzunehmen und sich an diese anzupassen, um ein Unternehmen in die Lage zu versetzen, Belastungen zu überstehen, dabei die gesteckten Ziele zu erreichen und sich vorteilhaft zu entwickeln."

Moderne hybride Netze verändern sich als Reaktion auf interne und externe Herausforderungen immer schneller. Das Tempo der Veränderungen hat die bis dato bestehenden Grundlagen für Unternehmensresilienz infrage gestellt. Seit dem Siegeszug von hybriden Netzwerken und SaaS ist außerdem zusätzliche Flexibilität gefragt. IT-Abteilungen stehen aufgrund ihrer zentralen Rolle bei der operativen Transformation unter ständigem Druck. Gelingt sie nicht, kann das Umsatzeinbußen, unzufriedene Kunden, Rufschädigung für die Marke und ein schlechtes Abschneiden im Vergleich zur Konkurrenz bedeuten, die interne und externe Erwartungen womöglich viel besser erfüllt. Darüber hinaus wird immer mehr Unternehmen bewusst, wie wichtig es ist, ihr Business weiterzuentwickeln: Die Umfrage der Enterprise Strategy Group (ESG) zu geplanten Investitionen für Technologie im Jahr 2023 ergab, dass mehr als 28 % der befragten NetOps-Experten die Verbesserung der operativen Resilienz gegen Cyberangriffe als einen ihrer wichtigsten Ausgabentreiber für das Jahr 2023 nannten. Die operative Resilienz liegt damit nur knapp hinter Kostenfaktoren wie der Verbesserung des Kundenerlebnisses (32 %), Datenanalyse (30 %) und Automatisierung (29 %).

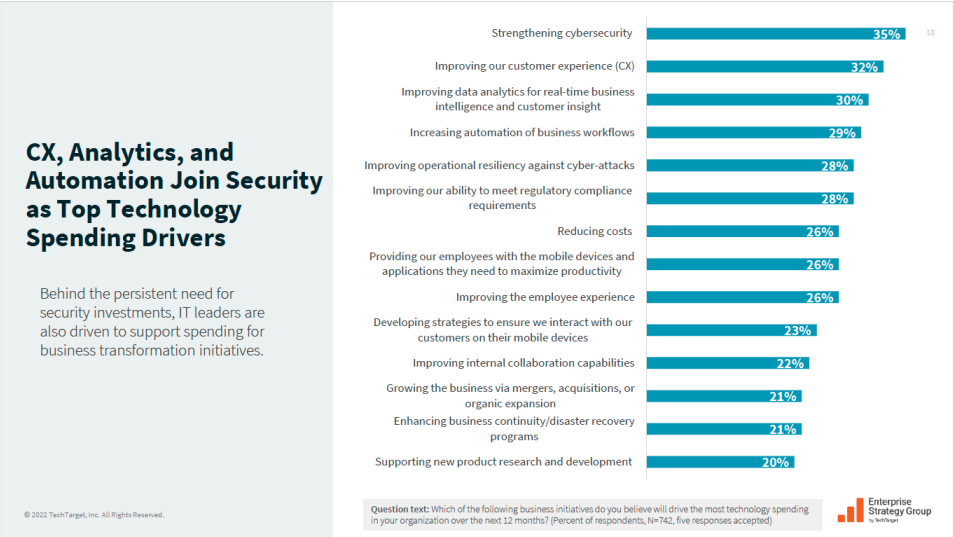

Abbildung 1 Enterprise Strategy Group (ESG) 2023 Technology Spending Intentions Survey

Operative Veränderungen in einer hybriden IT-Umgebung können je nach Unternehmen, Branche und den Anforderungen in den Abteilungen ganz unterschiedlich aussehen. Zu diesem Problem kommt hinzu, dass sich moderne Netzwerke weiterentwickelt haben, jedoch immer noch auf IT-Infrastrukturen aus der Zeit vor diesen Entwicklungen aufbauen. Der Weg hin zu mehr Resilienz ist jedoch im Großen und Ganzen immer derselbe – egal wie Ihr Unternehmen strukturiert ist. Zunächst müssen Sie die Herausforderungen im Zusammenhang mit Ihrem hybriden Netzwerk erkennen. Danach sollten alle problematischen Bereiche angegangen, Lösungen gefunden und operative Prozesse bestimmt werden, mit denen Ihr Team sich an die Herausforderungen anpassen und gleichzeitig Ihr hybrides Netzwerk optimieren kann. In diesem Artikel beleuchten wir die häufigsten Herausforderungen für moderne Netzwerke sowie drei Bereiche, die Unternehmen verbessern können, um ihre Netzwerke resilienter zu machen.

Die Herausforderung von hybriden Netzwerken

Die meisten hybriden Netzwerke sind das Ergebnis davon, dass Unternehmen ihre Netzwerktechnologie nur stückchenweise auf einen neuen Stand gebracht haben und eine Modernisierung aller Aspekte auf einmal zu radikal und zu teuer wäre. Stattdessen führen Unternehmen häufig neue Netzwerktechnik ein und nehmen gleichzeitig ältere Technik über einen längeren Zeitraum langsam außer Betrieb. Nun ist diese allmähliche Umstellung zwar weit verbreitet (und auch durchaus nachvollziehbar), sie bringt jedoch häufig Herausforderungen mit sich, die zu Anfälligkeit anstelle von Resilienz führen.

Der Wandel hin zu Remote-Arbeit führt zu Transparenzlücken

Dass Netzwerke hybrider werden, ist nicht neu. Während der Pandemie hat diese Entwicklung jedoch einen enormen Schub bekommen, da NetOps-Teams ihre Netzwerke in kürzester Zeit umgestellt haben, um Fernarbeit zu ermöglichen. Leider entstehen dabei auch oft Lücken bei Netzwerktransparenz, Compliance und Sicherheit. Beispielsweise kann veraltete lokale Technik andere Sicherheitsanforderungen haben als cloudbasierte Systeme. Wenn das einem NetOps-Team entgeht, können Angreifer Schwachstellen mitunter leichter ausnutzen.

Bedenken hinsichtlich der Ressourcen

Fehlende Arbeitskräfte, Zeit oder Geld machen es schwierig, ein leistungsstarkes Netzwerk aufzubauen – geschweige denn ein resilientes. Die Situation ist zu einem branchenweiten Problem geworden. Im aktuellen Enterprise Strategy Group (ESG) 2023 Technology Spending Intentions Report geben 54 % der IT-Fachleute operative Ineffizienzen als Hauptgrund für Initiativen zur digitalen Transformation an.

Durch diesen Mangel an Ressourcen werden jedoch nicht nur NetOps-Teams belastet, sondern es kann hybride Netzwerke auch anfällig machen. Ein Mangel an geeigneten Ressourcen macht es für Teams schwierig, sich ausreichend auf strategische Arbeit zu konzentrieren und proaktive Strategien zu finden, um komplexe hybride Netzwerke am Laufen zu halten, geschweige denn deren Resilienz sicherzustellen. Als Folge davon stehen viele NetOps-Teams immer komplexeren Netzwerken bei begrenzten Budgets gegenüber und sind bei der Arbeit hauptsächlich mit der reinen Schadensbegrenzung beschäftigt.

NPM: Die Grundlage für Resilienz in Unternehmen

Der erste Schritt für alle Unternehmen, um ihre hybriden Netzwerke widerstandsfähiger zu machen, ist die Implementierung einer robusten NPM-Lösung. Netzwerk-Performance-Management (NPM) ist ein proaktiver Ansatz zum Visualisieren, Überwachen, Optimieren, Beheben von Fehlern sowie zur Berichterstellung über Integrität und Verfügbarkeit Ihres hybriden Netzwerks. Bei diesem Ansatz wird eine Kombination von Tools und operativen Prozessen empfohlen, anhand derer Teams bestehende Problembereiche im hybriden Netzwerk schnell finden und beheben und das Netzwerk so positionieren können, dass diese Probleme in Zukunft vermieden werden. Wenn NPM in hybriden Netzwerken korrekt eingesetzt wird, können Herausforderungen von innen und außen bewältigt und gleichzeitig Wachstums- und Performanceziele erreicht werden. Leider tappen viele NetOps-Teams in die Falle, zu viel Wert auf schnelle Einblicke anstelle von tiefen Einblicken zu legen. Schnell heißt nicht gründlich, und wer dem Gewinnen von Einblicken nicht genug Zeit einräumt, dem entgehen mitunter wichtige Details, die für den Betrieb des Netzwerks relevant sind.

Die Ausbreitung hybrider Netzwerke in Zahlen:

- Die Zahl der Remote-Büros/Remote-Außenstellen nimmt zu – 35 % der Unternehmen betreiben weltweit 25–100 Remote-Büros/Remote-Außenstellen.*
- Multi-Cloud ist auf dem Vormarsch – 40 % der Unternehmen nutzen mindestens 3 öffentliche Cloud-Anbieter.**
- Komplexere Netzwerke seit der Pandemie – 33 % der IT-Fachleute geben an, dass ihre Netzwerkumgebungen komplexer sind als vor der Pandemie.***

Enterprise Strategy Group (ESG) End-to-end Network Visibility and Management Trends

* Wie viele Remote-Büros/Remote-Außenstellen betreibt Ihr Unternehmen weltweit (ungefähr)? Wie viele wird es in Ihrem Unternehmen voraussichtlich in 24 Monaten geben?
** Wie viele Anbieter von öffentlichen Cloud-Infrastrukturdiensten nutzt Ihr Unternehmen derzeit?
*** Wie komplex ist die durchgängige Netzwerkumgebung in Ihrem Unternehmen im Vergleich zu vor zwei Jahren?

Wie Sie in Ihren hybriden Netzwerken Resilienz für Ihr Unternehmen schaffen

Wie bereits erwähnt, sieht der Weg hin zur Schaffung resilienter Netzwerke in jedem Unternehmen etwas anders aus. Es gibt jedoch drei Bereiche, die für NetOps-Teams beim Umgang mit hybriden Netzwerken besonders wichtig sind und bei denen NPM dabei helfen kann, in jedem davon Resilienz für das Unternehmen sicherzustellen.

Performance

Bei jedem Netzwerktyp treten die typischen Performance-Probleme auf, die von fehlerhaften Geräten, hoher Bandbreitennutzung und DNS-Problemen herrühren. Dennoch gibt es bei hybriden Netzwerken einige besondere Punkte, die beim Performance-Management und der Performance-Optimierung zu beachten sind. Die Optimierung Ihrer hybriden Netzwerke für bessere Performance ist für die Resilienz zentral – schließlich hängt es bei modernen Unternehmen von der Netzwerk-Performance ab, wie gut es läuft. Läuft das Netzwerk nicht, läuft auch das Geschäft nicht. Wenn Sie Ihre Performance durch Resilienz absichern, kann Ihr Betrieb weiterlaufen, egal, mit welchen Widrigkeiten Ihre Systeme konfrontiert werden.

Sehen wir uns einige typische Knackpunkte an, die die Performance in hybriden Netzwerken beeinträchtigen können und wo sich mit NPM dem entgegenwirken lässt.

Arbeiten im Dunkeln

Wenn ein NetOps Team nicht die nötige Transparenz bei Anwendungen, Servern und cloudnativen Umgebungen hat, kann es Netzwerkprobleme nicht richtig beheben, etwa ungeprüfte Sicherheitsbedrohungen, Anwendungsausfälle und andere Performance-Probleme. Dabei hängt es maßgeblich von der schnellen Verfügbarkeit und Aussagekraft der Einblicke ab, ob ein Problem schnell behoben werden kann oder ein längerer Ausfall entsteht. Bei hybriden Netzwerken rührt mangelnde Sichtbarkeit häufig von Latenz bei den Einblicken her. Das tritt auf, wenn Einblicke zu stark zusammengefasst sind und entscheidende Details vernachlässigt werden, wenn sie zu langsam kommen oder wenn sie aus Silos bzw. Tools stammen, die widersprüchliche oder lückenhafte Daten liefern. Im EMA-Bericht Network Observability: Delivering Actionable Insights to Network Operations, nannten 46 % der NetOps-Fachleute Datenkonflikte zwischen einzelnen Tools als eines der gravierendsten datenbezogenen Probleme in ihren NetOps-Toolsets.

Warum Transparenz so wichtig ist:

- **68 %** der IT-Fachleute gaben an, dass Transparenz für ihre Netzwerkumgebung **sehr wichtig** ist. *

  * Enterprise Strategy Group (ESG) End-to-end Network Visibility and Management Trends

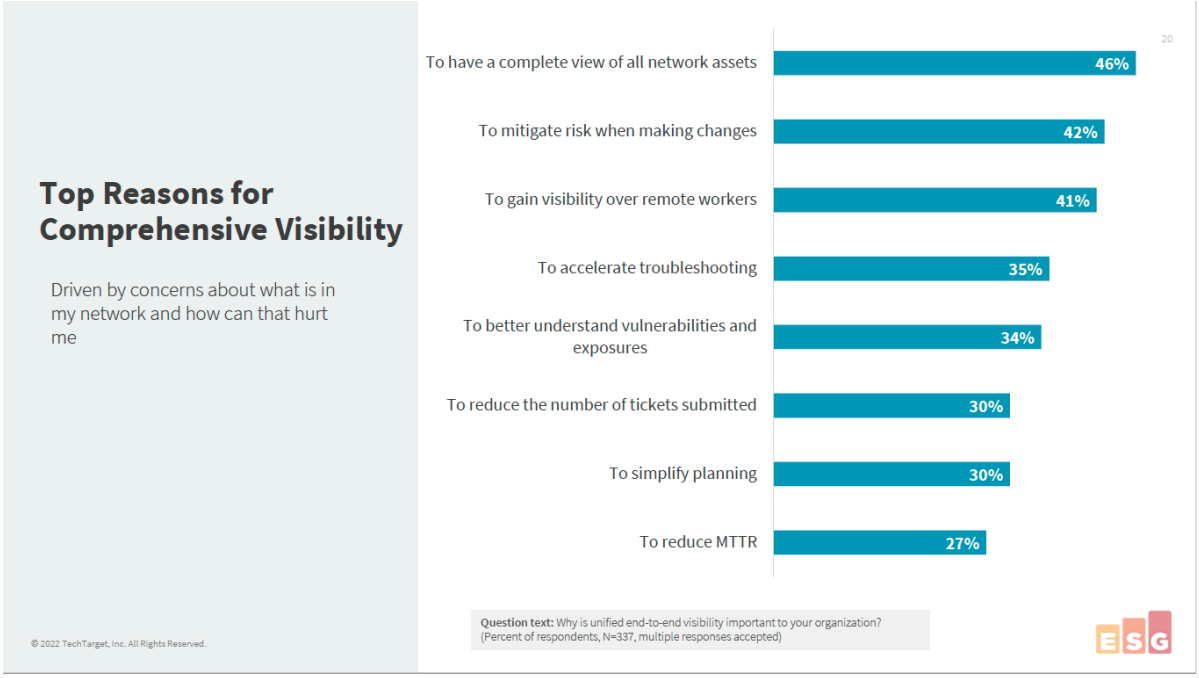

Abbildung 2 Enterprise Strategy Group (ESG) End-to-end Network Visibility and Management Trends

- **42 %** betrachten umfassende Transparenz als Schutz vor Risiken beim Vornehmen von Änderungen.
- **35 %** glauben, dass umfassende Transparenz eine schnellere Fehlerbehebung ermöglicht.
- **34 %** sind überzeugt, dass IT-Teams mit umfassender Transparenz Sicherheitslücken und Schwachstellen besser verstehen können.

Exponentielles Wachstum der Datenmengen

In hybriden Netzwerken werden mehr Daten als jemals zuvor erzeugt und verarbeitet. Laut einem Bericht von Statista wird erwartet, dass die globale Menge an Daten in den nächsten fünf Jahren von 64,2 Zettabyte auf 180 ansteigen wird. Wenn Ihr hybrides Netzwerk die anfallenden Daten nun nicht entsprechend verarbeiten kann, kann das zu Netzwerkengpässen, überlasteten Netzwerkknoten und Paketverlust führen. Paketverlust kann Netzwerkstörungen verursachen, Dienste verlangsamen und sogar zu Unterbrechungen bei der Netzwerkkonnektivität führen.

NPM und Performance

Die Optimierung Ihrer hybriden Netzwerke für bessere Performance ist für die Resilienz zentral. Mithilfe von NPM-Lösungen haben NetOps Zugang zu entscheidenden Gerätekennzahlen, Netzwerk-Verkehrsflussdaten sowie Paketdaten. Damit werden Unklarheiten beseitigt und bisher blinde Flecken im Netzwerk sichtbar, sodass Probleme korrekt und in kürzerer Zeit behandelt werden können. Ohne hochpräzise NPM-Telemetrie werden Performance-Probleme übersehen oder zu langsam behoben. Im Idealfall entscheiden Sie sich für ein NPM-Tool, das sich skalieren lässt und mit dem hybriden Netzwerk und den anfallenden Datenmengen mitwächst.

Compliance

Wie die Einhaltung der Vorschriften für Ihr hybrides Netzwerk aussieht, hängt von Ihrer Branche ab: In stark regulierten Branchen wie Behörden, Medizin und Finanzdienstleistungen etwa gelten in der Regel strengere Vorschriften. Die genaue Einhaltung von operativen und Sicherheits-Standards ist jedoch bis zu einem gewissen Grad in jedem Netzwerk notwendig.

Wenn Ihr Netzwerk die internen und externen Compliance-Anforderungen nicht erfüllt, besteht die Gefahr von Sicherheitslücken und Geldstrafen. Ein hybrides Netz, das aktiv nach operativen und Sicherheitsstandards verwaltet wird, kann jedoch selbst bei Netzstörungen Vorschriften einhalten und ist skalierbar, sodass ältere Anwendungen und Dienste auch bei der Einführung neuer Technologien resilient bleiben.

Warum hybride Netzwerke oft Probleme mit der Compliance haben und die Folgen für die Resilienz von Unternehmen

Unternehmen haben häufig Compliance-Probleme, weil die Cloud-Dienste und lokalen Dienste für ihre hybriden Netzwerke von Drittanbietern stammen. Die Vielzahl von Anbietern kann es schwierig machen, Audit Trails zu erstellen, zeitnahe Aktualisierungen durchzuführen, klare Regeln für die Daten-Governance aufzustellen und alles andere, was für die Einhaltung interner und externer Vorschriften unerlässlich ist. Unternehmen, die in diesem Bereich nicht resilient sind, riskierten Betriebsstörungen, Produktivitätsverluste, Geldstrafen und Rufschäden. In allen möglichen Branchen zahlen Unternehmen im Schnitt Millionen für die Behebung von Problemen im Zusammenhang mit Noncompliance.

Wo NPM auf Compliance trifft

Unternehmen setzen sich selbst interne Maßgaben, deren Einhaltung sie selbst kontrollieren, und gleichzeitig folgen sie behördlichen Vorgaben für Compliance. Diese internen und externen Standards bieten unerlässliche Anhaltspunkte, Überblick und Struktur in den Netzwerken. NPM-Produkte bieten zwar Netzwerktransparenz, aber wenn die Einhaltung der Vorschriften bei diesen Produkten nicht gewährleistet ist, kann sich das negativ auf die Transparenz und letztlich auf die Netzwerk-Performance auswirken. Mangelnde Transparenz kann zu verschiedenen Problemen führen, darunter langsame Performance und Ausfälle.

Sicherheit

Das Konzept der Unternehmensresilienz beruht auf Anpassungsfähigkeit. Dabei kann die Anpassung der sich ständig ändernden Sicherheitsanforderungen Ihres hybriden Netzwerks eine Herausforderung sein. Im Gegensatz zu herkömmlichen Netzwerken kombinieren hybride Netzwerk-Workflows lokale Rechenzentren mit Cloud-Umgebungen und Benutzern, die von verschiedenen Geräten und Standorten aus auf Anwendungen zugreifen. All diese Elemente sowie die Daten, die durch sie laufen, müssen geschützt werden. Wenn Sie die Sicherheit Ihres Netzwerks verbessern und es damit anpassungsfähiger machen, kann es besser auf die sich wandelnde Bedrohungslandschaft reagieren. Potenzielle Angriffe können Sie dann nicht nur besser und mit weniger Schaden überstehen, sondern eventuell sogar ganz vermeiden.

Die Anfälligkeit von hybriden Netzwerken

Die Komplexität von hybriden Netzwerken kann sie anfälliger für Angriffe machen. Cloudbasierte Dienste, ein typisches Merkmal von hybriden Netzwerken, bringen zusätzliche Sicherheitsrisiken mit sich, etwa unsichere Zugriffskontrollpunkte und falsch konfigurierte Sicherheitssysteme. Die Bedrohungslandschaft wächst, und damit auch die Wahrscheinlichkeit einer Datenpanne. Tatsächlich haben 45 % der Unternehmen in den vergangenen 12 Monaten eine Datenpanne im Zusammenhang mit der Cloud erlebt. Datenpannen und Angriffe auf Systeme sind teuer. Im Schnitt geben US-Unternehmen für die Folgen einer Datenpanne 9,44 Millionen USD aus. Ist Remote-Arbeit ein Faktor für die Entstehung der Datenpanne, ist diese Zahl um durchschnittlich 1 Million USD größer. Dabei noch nicht berücksichtigt sind andere Folgen wie Umsatzverlust durch den resultierenden schlechten Kundenservice sowie rechtliche Folgen.

Wo NPM auf Sicherheit trifft

NPM-Lösungen bieten Empfehlungen für Überwachung, Visualisierung und Berichterstellung, mit denen NetOps- und SecOps-Teams Sicherheitsverletzungen schneller erkennen und beheben können. Diese Empfehlungen statten Teams außerdem mit Forensik-Daten aus, mit denen sie die Transparenz erhalten, um in hochkomplexen Umgebungen proaktiv agieren zu können und Bedrohungen schneller etwas entgegen zu setzen, bevor es zu spät ist.

Unternehmen resilient machen – mit dem Portfolio für Netzwerk-Performance-Management (NPM) von Alluvio

Große Unternehmen arbeiten häufig mit mehreren einzelnen NPM-Tools. Das ist nicht nur kostspielig, sondern kann auch die Kommunikation erschweren, wenn verschiedene Abteilungen unterschiedliche Tools nutzen. Das kann es für die Teams schwierig machen, Resilienz aufzubauen. Jedes Team arbeitet mit verschiedenen Datasets, sieht unterschiedliche Probleme und Lösungen und arbeitet in Silos.

Viel besser wäre es, eine einzige, gemeinsam nutzbare Lösung zu haben. Eine solche Lösung unterstützt Sie bei Performance, Compliance und Sicherheit, sodass Ihr gesamtes hybrides Netzwerk im gesamten Unternehmen überall gleich gut funktioniert. Mit dem NPM-Portfolio von Alluvio können Sie überflüssige Lösungen ersetzen und die Kommunikation zwischen Ihren Teams verbessern. In seinem NPM-Portfolio bietet Alluvio die Lösungen AppResponse, NetProfiler, NetIM und Portal. All diese Produkte helfen Ihrem Team, eine IT-Umgebung zu schaffen, die flexibel ist, sich neuen Geschäftsanforderungen anpasst und schnell skaliert werden kann und gleichzeitig schnellere Einblicke und Integrationsverbesserungen für bessere Performance liefert.

Alluvio AppResponse

- Bietet paketbasierte Netzwerk- und Anwendungsanalyse für eine schnelle Fehlerbehebung.
- Kann lokal sowie in öffentlichen und privaten Cloud-Umgebungen bereitgestellt werden.
- Modulares Design macht relevante Daten und Kennzahlen zur Performance schnell verfügbar.
- Optimiert die Workflows zur Fehlerbehebung und analysiert hochpräzise Daten zur Diagnose von Ursachen innerhalb von einigen Minuten.

Alluvio NetProfiler

- Bietet durchgängige Transparenz des Traffics im hybriden Netzwerk.
- Schneller Zugang zu Traffic-Daten: Umfang des Datenverkehrs, Benutzer, Fluss und Priorisierung.

Alluvio NetIM

- Automatisiert die Analyse und bietet Echtzeit-Infrastrukturüberwachung.
- Bietet einen ganzheitlichen Blick auf das Netzwerk und beseitigt blinde Flecken.

Alluvio Portal

- Erstellt ein zentrales Dashboard, auf dem Teams leicht auf Performancedaten für das hybride Netzwerk zugreifen können.
- Vermeidet, dass widersprüchliche Daten von mehreren Tools erzeugt werden und ermöglicht bessere Kommunikation und Zusammenarbeit zwischen den Teams.

Für mehr Netzwerktransparenz und Performance

Viele Unternehmen haben Schwierigkeiten, Mitarbeiter mit Unternehmensressourcen zu verbinden, sei es lokal, auf einem Campus, mit einer Außenstelle oder in der Cloud. Performance-Management ist entscheidend dafür, dass Mitarbeiter in einem hybriden Netzwerk zuverlässig verbunden sind, und verbessert das digitale Benutzererlebnis. Netzwerk-Performance geht Hand in Hand mit Produkt-Performance. Hochpräzise Echtzeittransparenz ist ein Schlüssel zur Erkennung von Vorbeugung von Problemen mit der Netzwerk-Performance und kann direkte Auswirkungen auf das Geschäft haben. Das Portfolio von Alluvio™ umfasst mittlerweile die folgenden Produkte zur Performance-Optimierung:

Alluvio™ AppResponse:

- 50 % mehr erfasste Pakete write-to-disk (WTD) von 20 GB/s auf 30 GB/s für das 8180er-Gerät
- Größere Skalierbarkeit, Transparenz und Kapazität mit der Cloud
- Bessere Performance für die NetProfiler-Integration
- Unterstützt Oracle 19c

Alluvio™ NetProfiler:

- Über 30 % größere Flusskapazität (von 30 M auf 40 M pro Minute)
- Unterstützung von Google VPC und SD-WAN

Alluvio™ NetIM:

- Unterstützung von Streaming-Telemetrie, Cisco ACI und ServiceNow

Zusammen ermöglichen diese Tools Ihrem Team, Probleme mit dem Netzwerk-Traffic schneller zu finden und zu beheben, Workflows für die schnelle Behebung von Vorfällen zu automatisieren und einfach auf ganzheitliche Datenanalysen zu Cloud- und On-Premise-Infrastrukturelementen zuzugreifen. Das Ergebnis ist ein stabileres Netzwerk, das bei jeder Art der Nutzung ein besseres digitales Erlebnis bietet.

Darüber hinaus sorgt die umfassende Transparenz durch NPM für genauere AIOps-Modelle und Automatisierungsergebnisse. AIOps sammelt und aggregiert große Mengen an bereichsübergreifenden Daten und setzt in der Regel mehrere Analysetechniken ein, um optimale Ergebnisse zu erzielen. Die NPM-Datenquellen von Alluvio™ liefern umfangreiche und aussagekräftige Daten zur genauen Erkennung von kritischen Ereignissen.

Alluvio IQ, der SaaS-basierte Unified-Observability-Service von Riverbed, nutzt hochpräzise Alluvio NPM- und DEM-Daten, AIOps sowie intelligente Automatisierung. Dadurch kann schneller auf Vorfälle reagiert werden.

Gesicherte operative Governance und Compliance

Unternehmen stehen heute unter erheblicher Beobachtung, wenn es um die Einhaltung von Vorgaben geht, ob sie nun selbst auferlegt sind oder sich aus gesetzlichen Vorschriften ergeben. Allzu oft wird in den Medien über katastrophale Sicherheitsvorfälle in Unternehmen berichtet, die auf nicht Compliance-widrige Anwendungen oder Betriebssysteme zurückzuführen sind. Bösartige Akteure nutzen diese Schwachstellen, um in ein Netzwerk einzudringen und teure oder irreparable Schäden zu verursachen. In der bereits erwähnten, neuen Umfrage der Enterprise Strategy Group (ESG) (siehe Abbildung 1) wurden IT-Experten gefragt, welche Geschäftsinitiativen in den nächsten zwölf Monaten die meisten Ausgaben für Technologie in ihrem Unternehmen verursachen werden. Eine der häufigsten Antworten waren Initiativen zur Compliance. Wenn Ihr Team die Sicherheitslage oder die operative Effizienz durch die Erfüllung von Compliance-Anforderungen verbessern möchte, bietet das Alluvio NPM-Portfolio Netzwerkteams für Compliance geeignete Produkte, die Barrierefreiheit, Automatisierung und Datenverwaltung unterstützen.

Automatisierte Orchestrierung für Compliance

Unternehmen in stark regulierten Branchen wie dem Finanzdienstleistungssektor und dem Gesundheitswesen implementieren interne Regulierungsrichtlinien schon bevor es kraft gesetzlicher Vorschriften verpflichtend wird. Diese Sensibilität für Compliance wenden diese Unternehmen auch auf ihre Drittanbieter an. Von Anbietern für Netzwerkprodukte wird erwartet, dass ihre Produkte interne und gesetzliche Standards erfüllen. Dank der automatisierten Orchestrierung können IT-Teams die NPM-Produkte von Alluvio nahtlos einrichten, abschalten und wieder in einen sicheren Zustand versetzen. Diese Funktion bietet Ihnen die Übersicht und die Datenverwaltungsmöglichkeiten, die Sie benötigen, um die Compliance in Ihrem Netzwerk zu erreichen und aufrechtzuerhalten.

Unterstützung bei der Einhaltung gesetzlicher Vorschriften

Das NPM-Portfolio von Alluvio wird ständig weiterentwickelt, um Compliance-Anforderungen für Barrierefreiheit, Automatisierung und Datenverwaltung wie den Federal Information Processing Standard (FIPS) und Section 508 zu unterstützen.

Intelligente Sicherheitsmethoden gegen Cyberbedrohungen

Laut der Technology Spending Intentions Survey 2023 von der Enterprise Strategy Group (ESG) erwarten 65 % der IT-Fachleute, dass sie mehr für Cybersicherheit ausgeben werden für jeden anderen Bereich. Viele NetOps- und SecOps-Teams geben ihre Budgets für Sicherheitslösungen und -tools von mehreren Anbietern aus. Dadurch kann ein Flickenteppich entstehen, der es IT-Teams erschwert, Sicherheitsprobleme schnell zu diagnostizieren und zu beheben.

Die NPM-Produkte von Alluvio bieten automatisierte Prozesse bei der Datenerfassung, -analyse und -erkennung, so dass Teams schnell potenzielle Risiken erkennen können, die herkömmliche, flickwerkartige Sicherheitstools möglicherweise übersehen. Die angebotenen Sicherheitstools fügen sich nahtlos in die bestehenden automatisierten Prozesse von Unternehmen ein und bieten solide Sicherheitskompetenzen, die die Widerstandsfähigkeit des Unternehmens fördern. Dabei wird sowohl das Risiko von kritischen Vorfällen gesenkt, als auch das Ausmaß solcher Vorfälle reduziert, wenn sie doch eintreten.

Automatische Orchestrierung für Sicherheit

Im Falle einer Sicherheitsverletzung muss Ihr hybrides Netz zuverlässig laufen. NetOps-Teams haben jedoch oft Schwierigkeiten, das Netzwerk am Laufen zu halten, wenn es zu einem Angriff kommt. Der Grund dafür ist die Vielzahl an Geräten und Anwendungen im Netzwerk, die alle von einem anderen Anbieter unterstützt werden. Dabei ist ein einzelner Anbieter möglicherweise nicht funktionsfähig, wenn das Netzwerk gefährdet ist. Das NPM-Produktportfolio von Alluvio kann über eine automatisierte Orchestrierung betrieben und bereitgestellt werden. Das ist eine Praxis, bei der Hardware oder virtuelle Appliances ohne manuelle Eingriffe geupdatet, installiert, zurückgesetzt, konfiguriert und wiederhergestellt werden. Das bedeutet, dass Sie unabhängig vom aktuellen Sicherheitsstatus Ihres Netzwerks auf Ihre NPM-Daten zugreifen und sicherstellen können, dass Ihr Netzwerk für die Benutzer nutzbar ist – ob es nun von einem externen Ransomware-Angriff betroffen oder durch interne Bedrohungen gefährdet ist.

Forensik-Daten

Die von den NPM-Tools bereitgestellten Forensik-Daten ermöglichen eine bessere Kommunikation und Zusammenarbeit zwischen NetOps- und SecOps-Teams. Die intelligente forensische Analyse von Alluvio NPM und Alluvio IQ ermöglicht es NetOps- und SecOps-Teams, die Bedrohungserkennung zu automatisieren und zukünftige Risiken zu reduzieren.

Leistungsstarke Anomalieerkennung

Die NPM-Anomalieerkennung von Alluvio profitiert von Tools mit künstlicher Intelligenz und maschinellem Lernen (KI/ML), durch die der Datenanalyse-Workflow automatisiert wird und schneller läuft. So lassen sich die Ursachen diagnostizieren und Sicherheitsprobleme schneller finden und beheben.

Hochpräzise Daten

Die von Alluvio NPM gebotenen Daten erfassen jedes Paket, jeden Datenfluss und jede Gerätekennzahl ohne Stichproben. Das bedeutet, dass Sie Sicherheitsprobleme schon erkennen, sobald sie in Ihrem Netzwerk entstehen. Dabei gibt es keine blinden Flecken oder die Nachteile durch die Nutzung mehrerer Tools von verschiedenen Anbietern.

Alluvio NPM bietet die Bausteine für Unternehmensresilienz

NetOps-Teams können von der Komplexität der hybriden Netzwerke leicht überfordert werden. Resilienz zu einem Teil der DNA Ihres Netzwerks zu machen, hilft, Komplexität abzubauen, und erleichtert Ihrem Team Anpassung, Innovation und sogar Skalierung trotz Störungen. Die Unternehmen erkennen, wie wichtig eine bessere Resilienz für Unternehmen ist, und investieren entsprechend. Auf die Frage nach der Finanzierung von Projekten nannten die IT-Fachleute die Verbesserung der Resilienz für Unternehmen als einen der wichtigsten Punkte.

Das NPM-Portfolio von Alluvio konzentriert sich auf die Optimierung des hybriden Netzwerks in drei Schlüsselbereichen: Performance, Compliance und Sicherheit. Jede dieser drei Säulen ist der Schlüssel zum Aufbau eines resilienten Netzwerks. Eine optimierte Performance ermöglicht ein konsistentes Benutzererlebnis, selbst bei Störungen. Ein stärkerer, anpassungsfähigerer Sicherheitsstatus kann Ihr System vor den Auswirkungen von Cyberangriffen schützen und sie beheben, und lückenlose Compliance bewahrt Ihr Unternehmen vor hohen Geldstrafen. Bei einem anfälligen hybriden Netzwerk sind schwere Zwischenfälle kaum zu vermeiden. Haben Sie in jedem dieser Bereiche jedoch Resilienz, erreichen Sie eine bessere, durchgängige Transparenz, erleichtern sich die Nutzung aussagekräftiger Daten für bessere teamübergreifende Zusammenarbeit und bringen Ihre NetOps-Teams dazu, proaktiv zu agieren anstatt nur zu reagieren.

Sie möchten mehr Resilienz für Ihr Unternehmen in Ihrem hybriden Netzwerk?

Dann kontaktieren Sie uns und vereinbaren Sie eine Demonstration zum Netzwerk-Performance-Management.

riverbed