



Ein resilienteres Business mit dem ALLUVIO NPM PORTFOLIO

Warum wird IT immer komplexer?



der IT-Entscheidsträger verweisen auf die Zunahme von Remote- und Hybridarbeit.¹



Netzwerkhybridisierung als Antwort auf Remotearbeit und sich weiterentwickelnde Technologien veranlasst NetOps-Teams dazu, bessere und effizientere Tools und Lösungen zu suchen, mit denen die Unternehmen anpassungsfähig und innovativ sein und gleichzeitig Benutzern und Kunden ein ausgezeichnetes digitales Benutzererlebnis bieten können.

Wenn NetOps im Dunkeln arbeiten, lassen sich resiliente Netzwerke nur schwer schaffen

Wirksames Netzwerk-Performance-Management (NPM) ist der Schlüssel zu einem resilienteren Unternehmen.



Welche sind die wichtigsten Ziele für Initiativen zur digitalen Transformation?



der Senior-IT-Fachkräfte nannten die operative Effizienz.¹

Anzeichen für mangelnde Resilienz in hybriden Netzwerken

Wie können Unternehmen ihre hybriden Netzwerke resilient machen?

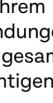


Die Anzeichen dafür, dass Ihr Netzwerk nicht resilient genug ist



der NetOps-Fachleute nannten Datenkonflikte zwischen einzelnen Tools als eines der gravierendsten datenbezogenen Probleme in ihren NetOps-Toolsets.²

1. Langsame Anwendungen und Performance-Probleme



Widersprüchliche Daten aus Lösungen und verschiedenen Elementen in Ihrem hybriden Netzwerk können Anwendungen langsamer machen und damit die gesamte Netzwerk-Performance beeinträchtigen.

2. Verfehlte interne und externe Compliance-Anforderungen



In allen möglichen Branchen zahlen Unternehmen im Schnitt Millionen für die Behebung von Problemen im Zusammenhang mit Noncompliance. Angesichts der Vielzahl der Anbieter, Anwendungen und Überwachungstools, auf die NetOps-Teams setzen, ist es schwer, behördliche und unternehmensinterne Compliance-Vorgaben einzuhalten.



der Unternehmen waren in den vergangenen 12 Monaten von Datenpannen im Zusammenhang mit der Cloud betroffen.³

3. Datenpannen und Sicherheitslücken



NetOps-Teams kombinieren für ihre hybriden Netzwerke lokale Rechenzentren mit Cloud-Umgebungen. Weil bei jedem dieser Bestandteile unterschiedliche Anforderungen bei der Sicherheit herrschen, kann es schwierig sein, wirksame Schutzmaßnahmen zu implementieren. Dadurch werden sie anfällig für Ransomware-, DDoS- und Man-in-the-Middle-Angriffe.

Wo im Netzwerk Resilienz schaffen

Tappen Sie mit Ihrem hybriden Netzwerk nicht länger im Dunkeln. Mit den richtigen NPM-Tools und -Prozessen können Ihre NetOps-Teams souverän auf mögliche Netzwerkprobleme reagieren und gleichzeitig das hybride Netzwerk des Unternehmens pflegen und optimieren.



Alluvio NPM ermöglicht Performancesteigerungen, operative Governance und auf Forensik beruhende Sicherheit

AppResponse
Paketbasierte Netzwerk- und Anwendungsanalyse für eine schnelle Fehlerbehebung.

NetProfiler
Transparenz des Flusses von Traffic im Netzwerk.

NetIM
IT-Infrastrukturüberwachung und Fehlerbehebung.

Portal
Zentrales Dashboard gegen blinde Flecken im Netzwerk und für bessere Kommunikation zwischen Teams.



Das Portfolio von Alluvio NPM bietet Ihrem Team die Tools für die nötige Transparenz, mit denen sich Ihre hybriden Netzwerke resilienter machen lassen.

Für mehr Netzwerktransparenz und Performance

- Durch neue Performanceverbesserungen wie bessere Datenfunktionen und schnellere Datenverarbeitung bringt Alluvio NPM so viel Telemetrie wie noch nie.
- Alluvio NPM hat zusätzliche Support-Verbesserungen für Drittanbieter wie Cisco ACI, Google Cloud und ServiceNow.



Gesicherte operative Governance und Compliance

- Automatische Orchestrierung bringt den Überblick und die Datenverwaltungsmöglichkeiten, die Sie brauchen, sowie die Fähigkeit, NPM-Produkte nahtlos in einen bekannten sicheren Zustand zu versetzen, außer Betrieb zu nehmen und wieder einzusetzen.
- Zum Alluvio NPM-Portfolio kommen ständig neue Produkte für Compliance-Vorgaben wie den Federal Information Processing Standard (FIPS) und Section 508 hinzu.



Intelligente Sicherheitsmethoden gegen Cyberbedrohungen

- Hochpräzise Daten ermöglichen die Erfassung aller Datenflüsse, Pakete und Gerätekenntzahlen, um blinde Flecken im Netzwerk zu beseitigen und Sicherheitsprobleme schneller zu erkennen.
- KI/ML-gestützte Anomalieerkennung unterstützt bei der Automatisierung der Datenanalyse und der schnellen Ursachendiagnose.
- Forensische Daten unterstützen NetOps und SecOps-Teams bei der Zusammenarbeit und der Risikominimierung.



Sie möchten endlich Licht ins Dunkel Ihrer hybriden Netzwerke werfen und Ihr Unternehmen resilienter machen?

Dann lernen Sie das NPM-Portfolio von Alluvio kennen. Um mehr zu erfahren, besuchen Sie:

www.riverbed.com/de/business-resilience



¹ Enterprise Strategy Group (ESG), Technology Spending Intentions Survey 2023. Was sind die wichtigsten Ziele Ihres Unternehmens für seine Initiativen zur digitalen Transformation? (Anteil der Befragten in Prozent)
² EMA-Bericht, Network Observability: Delivering Actionable Insights to Network Operations, Datenbezogene Probleme, die bei der Netzüberwachung oder Netzbeobachtung die größten Herausforderungen darstellen.
³ 2022 Thales Cloud Security Study, The Challenges of Data Protection in a Multicloud World.