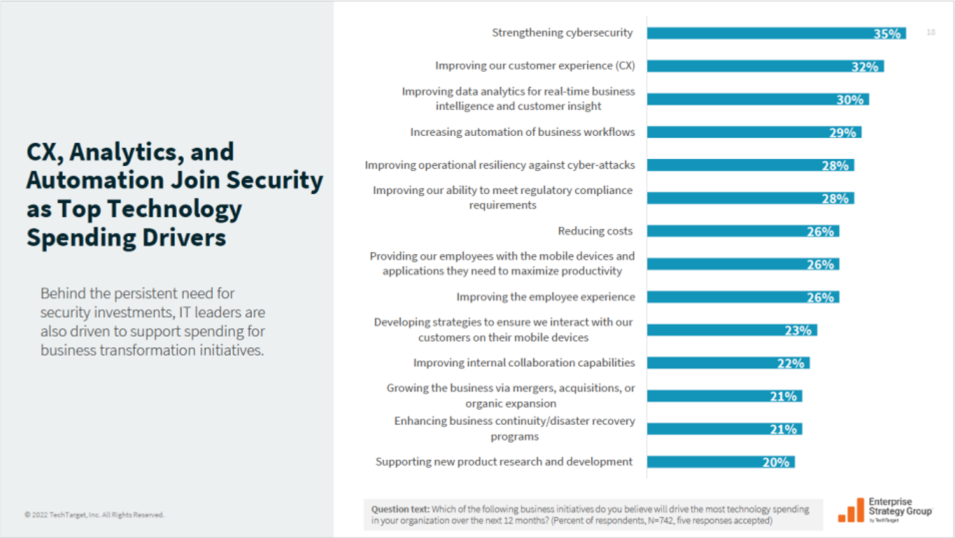
riverbed

WHITE PAPER

Achieve Business Resilience With Alluvio's Network Performance Management (NPM) Portfolio

Networks are evolving rapidly to keep up with an endless parade of external challenges, such as the shift to remote work in response to the pandemic, as well as internal objectives, like increasing performance and scale with stagnant budgets. NetOps teams need to adapt and innovate, now more than ever, in response to these challenges. This is the driver behind what is known as business resilience. The International Organization for Standardization (ISO) defines organizational or business resilience as: "The ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper."

Modern hybrid networks continue to change rapidly in response to internal and external challenges. The pace of change has stressed the foundations of business resilience, and the demands for levels of flexibility have only grown with the advent of hybrid networks and SaaS adoption. IT teams are under constant scrutiny to drive operational transformation. A failure to do so may lead to lost revenue, customer churn, negative brand perception, and losing pace with competitors that nimbly handle external and internal challenges. Plus, more and more companies are starting to realize the importance of evolving their business: The Enterprise Strategy Group (ESG) survey on 2023 Technology Spending Intentions found that over 28% of NetOps professionals surveyed listed improving operational resilience against cyberattacks as one of their top spending drivers for 2023. Greater operational resilience was secondary only to spending drivers like improving customer experience (32%), data analytics (30%), and automation (29%).



CX, Analytics, and Automation Join Security as Top Technology Spending Drivers

Behind the persistent need for security investments, IT leaders are also driven to support spending for business transformation initiatives.

Question text: Which of the following business initiatives do you believe will drive the most technology spending in your organization over the next 12 months? (Percent of respondents, N=742, five responses accepted)

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

Operational change in a hybrid IT environment can look vastly different depending on your organization, industry, and team needs. This problem is compounded by how modern networks have evolved yet still rely on IT infrastructure that predates the evolution. However, the process for building better business resilience — no matter your organization's shape or size — is largely the same. First, you must identify the challenges your hybrid network faces. Then, you should address each area of concern, identifying the solutions and operational processes your team can adopt to meet challenges while simultaneously improving your hybrid network. In this paper we'll walk through the most common challenges faced by modern networks, as well as three areas organizations can improve to build more resilience into their networks.

The challenge of hybrid networks

Most hybrid networks are the result of organizations upgrading their network technology piecemeal, as it's too costly and disruptive to upgrade everything at once. Instead, businesses often introduce new networking technologies while simultaneously phasing out the old technology over a period of time. While this piece-by-piece approach is common (and understandable), it often comes with challenges that prompt fragility, rather than resiliency.

Transitional to remote work comes with gaps in visibility

Network hybridization isn't new, but it got a huge boost during the pandemic as NetOps teams rushed to quickly transition their networks to support remote work. Unfortunately, this often also created gaps in network visibility, compliance, and security. For example, on-premise legacy technology may have different security considerations than cloud-based systems. If a NetOps team fails to notice this, it may be easier for threat actors to exploit security vulnerabilities.

Resource concerns

A lack of manpower, time, and/or money, makes it challenging to build a successful network – let alone a resilient one. The situation has become an industry-wide issue. In the recent Enterprise Strategy Group (ESG) 2023 Technology Spending Intentions Report, 54% of IT professionals cite operational inefficiencies as the main impetus for digital transformation initiatives.

Not only is this lack of resources hard on NetOps teams, but it also leaves many hybrid networks vulnerable. A lack of appropriate resources makes it difficult for teams to do more strategic work and find proactive strategies needed to keep complex hybrid networks running — let alone resilient. As a result, many NetOps teams faced with an increasingly complex network but limited resources are stuck in an endless cycle of putting out fires.

NPM: The baseline for business resilience

The first step all organizations should take to build better business resilience into their hybrid networks is to implement a robust NPM solution. Network performance management (NPM) is a proactive approach to visualizing, monitoring, optimizing, troubleshooting and reporting on the health and availability of your hybrid network. This approach recommends a combination of tools and operational processes that teams can adopt that will help them quickly find and remediate existing problem areas in their hybrid network, as well as position their network to address and avoid these issues in the future. A team correctly utilizing NPM in their hybrid network can expect to navigate internal and external challenges while also accomplishing their goals of growth and performance. But a common pitfall for NetOps teams is the incorrect value they put on the speed of insights vs. the depth of insights. Fast does not mean thorough and often misses important details that could impact your network.

Hybrid Network Growth by the Numbers:

- Remote/branch offices are increasing – 35% of organizations operate 25-100 remote offices/branches worldwide. *
- Multi-cloud usage is on the rise – 40% of organizations utilizes at least 3 public cloud providers. **
- Post-pandemic network complexity – 33% of IT professionals say their network environments are more complex than before the pandemic. ***

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

* Approximately how many remote offices/branch offices does your organization operate worldwide? How many do you expect your organization to have 24 months from now?
** Approximately how many unique public cloud infrastructure service providers does your organization currently use?
*** In general, how complex is your organization's end-to-end network environment relative to two years ago?

Where to build business resilience into your hybrid networks

As we mentioned before, a resilient network will look different for each company. However, here are three common areas of concern for NetOps teams managing hybrid networks, and how NPM can help them build business resilience into each.

Performance

While every type of network struggles with common performance issues stemming from device malfunction, high bandwidth usage, and DNS problems, hybrid networks have unique considerations when it comes to network performance management and enhancement. Optimizing your hybrid network for better performance is a key component of business resilience. After all, network performance is the lifeblood of modern organizations. If the network doesn't work, the business doesn't work. Building resilience into your performance means your company can keep operating, no matter what's thrown at it.

Let's look at some of the distinct concerns impacting performance in hybrid networks and where NPM can step in.

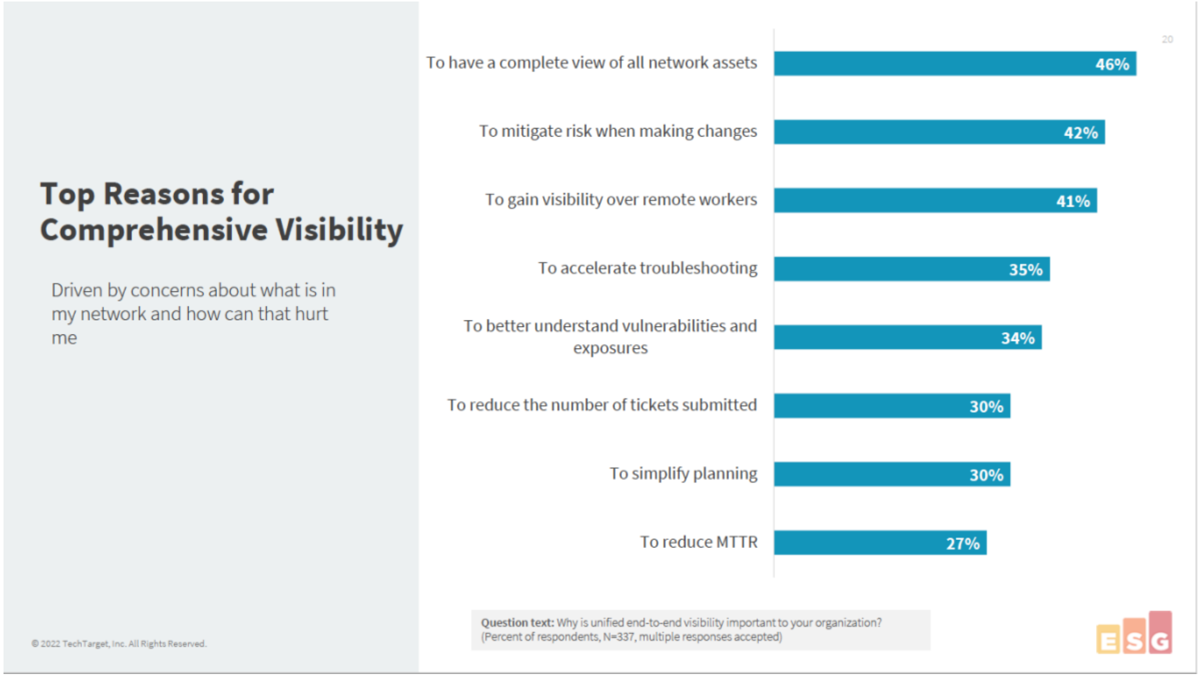
Operating in the dark

When a NetOps team lacks visibility into their applications, servers, and cloud-native environments, they're unable to correctly troubleshoot network issues like unchecked security threats, application slowdowns and other performance issues. And the speed and clarity with which insights are delivered can be the difference between prompt action and a large outage. For hybrid networks, a lack of visibility often stems from insight latency. This occurs when insights are too summarized and miss critical details, too slow for teams to react or come from siloed sources and/or tools that provide conflicting or incomplete data. In the EMA report, Network Observability: Delivering Actionable Insights to Network Operations, 46% of NetOps professionals cited data conflicts between individual tools as one of the most painful data-related challenges in their NetOps toolsets.

Why visibility matters:

- **68%** of IT professionals say that unified visibility is **very important** in their network environment. *

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



Top Reasons for Comprehensive Visibility

Driven by concerns about what is in my network and how can that hurt me

Question text: Why is unified end-to-end visibility important to your organization? (Percent of respondents, N=337, multiple responses accepted)

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

- **42%** believe comprehensive visibility helps mitigate risk when making changes.
- **35%** believe comprehensive visibility accelerates troubleshooting.
- **34%** believe comprehensive visibility helps IT teams better understand vulnerabilities and exposures.

Exponential data growth

Hybrid networks are generating and processing more data than ever before. A Statista-published report found that the total amount of global data is set to double in the next five years from 64.2 zettabytes to 180. Inadequate processing capabilities in your hybrid network can lead to network congestion, overburdened network nodes, and packet loss. Packet loss can cause network disruption, slow service and even loss of network connectivity.

Where NPM meets performance

Optimizing hybrid network performance is key to building better business resilience. NPM solutions offer NetOps teams the ability to access crucial device metrics, network flow data, and packet data — eliminating confusion and shining light onto network blind spots to accurately diagnose and address issues sooner. Not having access to full-fidelity NPM telemetry ensures performance issues are missed or resolved too slowly. Ideally, your chosen NPM tools should scale to meet your hybrid network's growing data generation and intake.

Compliance

What compliance looks like for your hybrid network depends on your industry: for example, highly-regulated industries like government, medical and financial services usually have more stringent compliance requirements. Careful adherence to security and operational standards, however, is a necessity to some degree in every hybrid network.

When your network fails to meet internal and external compliance requirements, you risk creating security gaps and incurring fines. A hybrid network actively managed to operational and security standards, however, is able to remain compliant, even in instances of network disruption, and scale, effectively maintaining resilience on older applications/services while introducing new technologies.

Why hybrid networks struggle with compliance and what that means for business resilience

Companies often struggle with compliance because their hybrid networks' cloud and on-premise services are supported by third-party vendors. The variety of vendors can make it difficult to create audit trails, execute timely updates, establish clear data governance rules, and complete other tasks integral to internal and external compliance requirements. Companies that aren't resilient in this area risk business disruptions, productivity loss, penalties and reputational damage. Enterprises regardless of industry on average spend millions resolving noncompliance issues.

Where NPM meets compliance

Organizations police themselves internally and follow governmental regulations around compliance. These internal and external standards provide crucial guidance, oversight, and structure in their networks. While NPM products offers network visibility, failure to ensure compliance in these products can negatively impact visibility and, ultimately, network performance. A lack of visibility can cause a number of issues, including slowdowns and shutdowns.

Security

The concept of business resilience centers around adaptation – and adapting to your hybrid network's evolving security needs can be challenging. In contrast to a typical network, hybrid network workflows combine both on-premise data centers and cloud environments, as well as users accessing applications from various devices and locations. All of these elements, as well as the data that passes through them, need to be protected. Improving your network's security, making it more adaptable, can help it respond favorably to a rapidly evolving threat landscape. Not only will you weather potential attacks better, recovering faster and with less damage, but you may be able to avoid others altogether.

The vulnerability of hybrid networks

The complexity of hybrid networks can make them more vulnerable to attacks. Cloud-based services, a common feature of hybrid networks, introduce additional security concerns such as insecure access control points and security system misconfiguration. As the threat landscape grows, so does the likelihood of a data breach; in fact, 45% of businesses have experienced a cloud-based data breach in the past 12 months. Data breaches and system attacks are costly. The average organization in the US spends approx $9.44M on the aftermath of a data breach. This figure increases by an average of $1M when remote work is a factor in causing the breach, and doesn't include other effects like revenue loss from negative customer experiences, as well as legal liability.

Where NPM meets security

NPM solutions offer monitoring, visualization and reporting recommendations that help NetOps and SecOps teams find and remediate security breaches faster. These recommendations also equip teams with forensic data, giving them the visibility necessary to be proactive in a highly complex environment and stop threats sooner rather than later — when it might be too late.

Building business resilience with Alluvio's Network Performance Management (NPM) portfolio

Large enterprises are often working with several individual NPM tools. Not only is this expensive, but it can create communication challenges (different teams using different tools within the organization). This can impact a team's ability to build resiliency. Each team is evaluating different data sets, identifying different problems and solutions, and operating in silos.

Your team needs a single, interoperable solution that will provide the performance, compliance and security support needed to deliver a consistent digital experience across your organization's hybrid network. Alluvio's NPM portfolio can help you eliminate surplus technology and improve communication between your teams. Alluvio's NPM portfolio offers AppResponse, NetProfiler, NetIM, and Portal. These products work together to help your team create an IT environment that is nimble, able to accommodate new business requirements, and scale quickly while delivering accelerated insights and integration enhancements that increase performance.

Alluvio AppResponse

- Delivers packet-based network and application analysis for rapid troubleshooting.
- Can be deployed on-premises and in private and public cloud environments.
- Modular design to quickly tap into meaningful performance data and metrics.
- Streamlines troubleshooting workflows and analyzes high fidelity data to diagnose root causes in minutes.

Alluvio NetProfiler

- Offers end-to-end visibility of hybrid network traffic.
- Quick access to traffic data: amount of traffic, users, flow, and how traffic is being prioritized.

Alluvio NetIM

- Automates analytics and offers real-time infrastructure monitoring.
- Offers holistic network perspective, eliminating blind spots.

Alluvio Portal

- Creates a centralized dashboard for teams to easily access hybrid network's performance data.
- Eliminates the frustration of multiple tools producing conflicting data and enables better communication/collaboration between teams.

Elevate your network's visibility and performance

Organizations often report problems connecting workers to company resources whether on premise, campus, branch or cloud. Performance management is key to keeping workers connected in a hybrid network and improving the end-user's digital experience. Network performance is intrinsically tied to product performance. Real-time full fidelity visibility is key to identifying and preventing network performance issues that can directly impact business. The Alluvio™ portfolio has evolved to include the following product performance improvements:

Alluvio™ AppResponse:

- 50% increase packet captures write to disk (WTD) from 20 Gbps to 30 Gbps for the 8180 appliance
- Greater cloud scalability, visibility, and capacity
- Higher performance for NetProfiler integration
- Oracle 19c support

Alluvio™ NetProfiler:

- Over 30% increase flow capacity from 30M to 40M flow per minute
- Google VPC and SD-WAN support

Alluvio™ NetIM:

- Streaming Telemetry, Cisco ACI, and ServiceNow support

Together, these tools empower your team to find and fix network traffic issues faster, automate workflows for rapid incidents remediation, and easily access holistic data analysis on cloud and on-premise infrastructure elements. The result is a more stable network that provides an improved digital experience to each use.

In addition, full-fidelity NPM visibility drives more accurate AIOps models and automation results. AIOps collects and aggregates large amounts of cross-domain data and typically leverages multiple analytics techniques for best results. Alluvio™ NPM data sources provide rich and deep data for accurate event identification. Alluvio IQ, Riverbed's SaaS-based Unified Observability service, leverages full-fidelity Alluvio NPM and DEM data, AIOps, and intelligent automation to speed incident response and security forensics.

Ensure operational governance and compliance

Companies today are under considerable scrutiny when it comes to compliance requirements, whether it is imposed organizationally or governmentally. All too often the media is reporting on catastrophic corporate breaches due to non-compliant applications or operating systems. Threat actors target these vulnerabilities to penetrate a network causing expensive or irreparable damage. In fact, as noted above in the recent Enterprise Strategy Group (ESG) survey from Figure 1, IT professionals were asked which business initiatives would drive the most technology spending in their organization over the next 12 months. One of the top answers was regulatory compliance initiatives. If your team is looking to increase your security posture or operational efficiency by meeting compliance requirements, the Alluvio NPM portfolio provides network teams compliance-ready products, supporting accessibility, automation and data management.

Automated orchestration for compliance

Organizations in highly regulated industries like financial services and healthcare are implementing internal regulatory policies in advance of developing governmental regulations. This vigilance in compliance also extends to their third-party vendors. Network product vendors are expected to support organizational or governmental compliance standards in their products. With automated orchestration, IT teams can stand up, take down, and redeploy Alluvio NPM products to a known safe state seamlessly. This feature provides the oversight and data management you need to achieve and maintain compliance in your network.

Governmental compliance support

The Alluvio NPM portfolio is constantly evolving its products to support compliance requirements for accessibility, automation and data management like the Federal Information Processing Standard (FIPS) and Section 508.

Engage intelligent security methods against cyber threats

According to the Enterprise Strategy Group (ESG) 2023 Technology Spending Intentions Survey, 65% of IT professionals anticipate spending more on cybersecurity than any other area. Many NetOps and SecOps teams will spend their budgets on security solutions and tools from a variety of vendors. This can create a patchwork system that prevents the IT team from quickly diagnosing and resolving security concerns.

Alluvio's NPM products offer automated processes in data collection, analysis, and detection so teams can quickly identify potential risk exposures that traditional, patchwork security tools might miss. The portfolio's security tools seamlessly integrate into an organization's existing automated processes, offering the solid security competencies that drive business resilience by reducing both the risk of negative network events and the magnitude of events when they occur.

Automated orchestration for security

In the event of a security breach, your hybrid network needs to remain operational. NetOps Teams, however, often struggle to maintain network uptime when there is an attack. This is due to the multiple devices and applications on their network, each of which is supported by a product vendor that may or may not be equipped to function when the network is compromised. The Alluvio NPM product portfolio can be operated and provisioned via automated-orchestration: a practice of manual-intervention-free updating, installing, resetting, configuring, and restoring hardware or virtual appliances. This means that regardless of your network's current security state, whether it's affected by an external ransomware attack or compromised by internal threats, you will be able to access your NPM data and ensure that your network is up and running for end users.

Forensic data

The forensic data provided by the NPM tools establishes better channels of communication and collaboration between NetOps and SecOps teams. Intelligent forensic analysis from Alluvio NPM and Alluvio IQ enables NetOps and SecOps teams to automate threat identification and reduce future risks.

Powerful anomaly detection

Alluvio's NPM's anomaly detection is backed by artificial intelligence and machine learning (AI/ML) powered tools that automate and expedite the data analysis workflow process to diagnose root causes, empowering your team to find (and fix) security issues faster.

Full-fidelity data

The full-fidelity data offered by Alluvio NPM captures every packet, flow, and device metric — without sampling, which means that you'll be able to catch security issues as they form across your network without blind spots or the inconvenience of multiple tools by different vendors.

Alluvio NPM offers the building blocks for business resilience

NetOps teams can easily become overwhelmed by the complexity of their hybrid networks. Building business resilience into the DNA of your network can cut through the complexity, significantly improving your team's ability to adapt, innovate, and even scale in the face of disruptions. Organizations are realizing the importance of better business resilience and investing accordingly. In fact, when asked about securing funding for projects, IT professionals listed improving business resilience as one of the main considerations.

The Alluvio NPM portfolio focuses on optimizing your hybrid network in three key areas — performance, compliance, and security. Each of the three pillars is key to building a more resilient network. Optimized performance can help you deliver a consistent user experience, even in the face of disruptions. A stronger, more adaptable security posture can help protect your system against, and remediate the effects of cyberattacks; and the ability to remain compliant saving your organization from paying hefty fines. A fragile hybrid network is ripe for disaster, but building resilience in each of these areas offers greater end-to-end visibility, helps you harness meaningful data that inspires greater cross-team collaboration, and effectively shifts your NetOps team's mindset from reactive to proactive.

Ready to build better business resilience to your hybrid network?

Contact us to schedule your Network Performance Management demo today.

riverbed

Riverbed is the only company with the collective richness of telemetry from network to app to end user, that illuminates and then accelerates every interaction, so organizations can deliver a seamless digital experience and drive enterprise performance. Riverbed offers two industry-leading portfolios: Alluvio by Riverbed, a differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless, secure digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of partners, and market-leading customers globally – including 95% of the FORTUNE 100 –, we empower every click, every digital experience. Riverbed. Empower the Experience. Learn more at riverbed.com. MSHD-1096_Business-Resilience_WP_US_040323