ALLUVIO™
by riverbed

Business Resilience in Three Scenarios

EBOOK

Table of Contents

In a recent report, Gartner found that recovering from a ransomware attack costs 10 to 15 times more than the ransom itself. After factoring in things like downtime, lost opportunities, reputational damage, customer churn, and employee costs, Gartner places the average recovery cost at $1.5 million. These costs become even more sobering when you consider that just the first half of 2022 saw 236 million ransomware attacks globally.

With statistics like these, it's necessary to equip an organization's IT infrastructure to recover quickly and effectively from unexpected disruptions, including natural disasters, economic downturns, socio-political events, and pandemics. Companies navigating these events aim to maintain critical network functionality, or business continuity. The better option, however, is to establish resiliency in your IT infrastructure.

What is 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.” The keywords to note in the definition are survive and prosper. When business disruption happens – whether it’s the result of a cyberattack, a natural disaster, or a service outage – your organization should be situated to survive the disruption and scale during and after.

Adopting the Resilient Mindset

The first step in building resilience in your hybrid network is to shift your mindset from reactive to proactive. In other words, instead of considering how your organization will navigate through the aftermath of an attack or disruption, you should instead consider how to build a more robust, resilient network that can prevent attacks, deliver a consistent digital experience if an attack occurs, and grow in spite of disruptions.

Network resilience also requires the right tools. It’s impossible to achieve operational transformation, governance and compliance, and security across your network through manual systems and processes. Investing in the right tools, like those provided by Riverbed, can help your team efficiently and effectively build resilience in these areas.

Where to Get Started with Business Resilience

Wondering where to start building business resilience into your IT infrastructure? Together, we’ll examine three examples of fictional organizations experiencing business disruption. In the first part of each example, we’ll look at a network without any resilience strategies or tools. In the second, we’ll look at the same example of business disruption from the perspective of a resilient network that uses Riverbed tools and proactive strategies to survive disruption and thrive despite it. You can use these scenarios to understand the warning signs of a network lacking resilience and consider adopting similar resilience measures in your network infrastructure.

SCENARIO 1:

Accelerated Operational Transformation Threatens Performance

Background

Company A has a hybrid network, and its workforce used to work primarily from its headquarters in Dallas. The company went remote at the outset of the COVID-19 pandemic and has since shifted to a permanent hybrid workforce.

The Challenge

In the rush of sending employees home during the early days of the pandemic, the company invested in cloud technologies and apps that would help its employees work remotely. While Company A was already shifting to cloud technologies, the pandemic accelerated this transformational shift.

The Non-Resilient Hybrid Workforce

Our non-resilient version of Company A has taken a more reactive approach after extending its hybrid network during the pandemic. Since then, the company's NetOps teams have noticed network performance issues cropping up.

Network downtime: Employees are complaining about the unreliability of the organization's network, and network downtime is beginning to affect productivity. Gartner estimates that unplanned network downtime costs around $5,600 per minute.

Inaccessible applications: Employees are unable to access applications quickly. The NetOps team finds that migrating apps to the cloud is a slow process that often requires significant network downtime.

Mysterious slowdowns: The IT team often has difficulty pinpointing the source of slowdowns across the network, as the team must manually search the network. The lack of visibility makes it difficult for the growing company to scale and provide a consistent digital experience.

So what does the future hold for non-resilient Company A? The company's haphazard transformational shift to cloud technologies creates an increasingly complex network with low visibility and poor performance. Without resiliency measures and tools, Company A's IT team will continue manually searching for slowdowns across its networks. As a result, network issues go undetected until they become pervasive, system-wide concerns. Additionally, the network slowdowns and shutdowns will continue to affect employee productivity, driving employee satisfaction rates down and negatively impacting the company's revenue.

The Resilient Hybrid Workforce

Now, let's imagine the same scenario with Company A, but the company has a resilient network and the tools to support its operational transformation through (and beyond) the pandemic.

In an effort to be proactive instead of reactive, our resilient version of Company A considered the growing complexity of its hybrid network infrastructure ahead of and during its rollout. The company also identified Network Performance Management (NPM) as crucial to helping it optimize performance.

What is Network Performance Management?

NPM is the process of monitoring IT networks to ensure optimal performance and availability of the applications that run on them. NPM tools collect and analyze key network performance metrics such as bandwidth utilization, packet loss, and latency. With this data, NetOps teams can identify and troubleshoot problems, optimize network resources, and ensure the network performs as expected.

Company A uses Riverbed's Alluvio Unified Observability and Acceleration tools to:

Increase visibility for better performance: Alluvio NPM solutions gather packet, flow, and device data across an organization's entire network for proactive visibility and troubleshooting. Company A utilizes the tool's full-fidelity network data and monitoring features to regulate bandwidth and improve performance.

Optimize its cloud migrations: Riverbed's Cloud Accelerator will ensure that Company A's workers have fast, secure access to apps by reducing the average application migration transfer time by 64%. By taking advantage of the complete Acceleration portfolio, the company also improves data protection through data deduplication and compression in the SteelHead WAN solution, which also creates disaster recovery architecture to maintain performance in the event of a serious natural disaster or security issue.

Scale strategically: As Company A grows, Alluvio Portal's integrated network, application and user insights, and dynamic visibility dashboards allow the company's teams to see the entire digital infrastructure from a single platform for faster issue resolution.

Automate desktop issue resolution: Leveraging Alluvio Aternity DEM helps Company A's service desk teams get performance insights into the digital employee experience of both its remote and hybrid workers. The tool also automatically identifies and resolves device and user issues. The team can correlate subjective input from employees with device and app performance to determine where performance issues lie.

The future is looking much brighter for our resilient version of Company A. Moving forward with unified observability and NPM tools, the company provides a consistent digital experience to its remote workforce, positioning its IT infrastructure for growth during and beyond the pandemic, and creates more efficient processes to drive its cloud migration further.

Resilience by the Numbers

Nearly **one in four** respondents in a recent EMA report believe that network visibility solutions improved application performance and resiliency.

46% of respondents identified resilience as one of the primary desired outcomes of improving visibility in a Digital Enterprise Journal survey.

SCENARIO 2:

Cloud Transition Complicates Governance and Compliance Requirements

Background

Company B is a bank transitioning its legacy systems to the cloud. The company deals with a large amount of client capital and personal information. Consequently, Company B developed internal compliance standards in addition to the industry's current government compliance regulations.

The Challenge

Company B must stay ahead of changing government regulations and develop a strategy for meeting internal compliance requirements or face hefty fines, network configuration confusion, security issues, and more, all while transitioning to a hybrid cloud infrastructure.

The Non-Resilient Cloud

The NetOps team at the non-resilient version of Company B found that its network failed internal compliance tests, and the team raised concerns that the network won't meet external compliance requirements. Specifically, the team's struggles include:

Lack of visibility: Network visibility is an ongoing issue, as Company B's NetOps teams can't track application use and performance across the organization's infrastructure. Poor visibility also means it's difficult to spot anomalies and update applications for compliance.

Incomplete data: The company's team struggles to gather data from across the network for compliance audits. The data it collects is incomplete and uncontextualized, often resulting in unchecked network events.

Skills gaps: Compliance regulations require the company to maintain essential network functions in the case of disruption, and the team doesn't have the plan or specialized experience to do so. The NetOps team also needs help understanding exactly how a hybrid cloud environment will change its compliance obligations across jurisdictions.

If our non-resilient Company B continues down its current path, it will experience ongoing compliance issues, both internal and external. The team's struggle for network visibility will make compliance auditing difficult and put the company at risk for fines and other consequences due to its failure to meet compliance standards. Most importantly, if the company's network is compromised, it won't have a plan to ensure essential functions continue during and immediately after the event. The resulting downtime could be considerable and costly.

The Resilient Cloud

Curious about how Company B would handle governance and compliance requirements with a resilient network and compliance-supporting tools? Let's take a look:

Improved visibility: Riverbed's Alluvio Digital Experience Management (DEM) solution allows Company B to track shadow IT throughout the organization and ensure that applications are up to date, which is necessary for compliance.

Automated orchestration: Our alternative Company B leverages automated orchestration offered by Riverbed's NPM portfolio. In the case of network disruption, automated orchestration takes down Riverbed's NPM products and redeploys them automatically to a known safe state. This automated orchestration feature allows Company B to maintain compliance during and immediately after a disruptive event occurs.

Continuous monitoring: Company B uses Riverbed's NetIM continuous network monitoring to automatically monitor availability, track configuration and topology changes across its infrastructure, and map application network paths. Continuous monitoring streamlines internal/external compliance efforts and helps the NetOps team find and correct network changes negatively impacting performance.

Operational Governance & Compliance: Company B also utilizes the Alluvio NPM portfolio to stay on top of evolving, government-mandated regulations like Section 508 for federal accessibility standards and FIPS for compatible crypto support. Alluvio NPM ensures that Company B's hybrid network can easily achieve and maintain regulatory compliance requirements.

Moving forward, our resilient Company B has the tools to achieve and maintain internal and external compliance standards. The company's NetOps teams can easily visualize IT infrastructure, end-to-end. Additionally, the company is confident that it can maintain compliance should a disruption occur.

SCENARIO 3:

Increased Security Threats Highlight Resource Issues and Skills Gaps

Background

Company C is a retail organization concerned about the growing threat landscape. Knowing there was a 67% increase in retail industry ransomware attacks between 2021 and 2022, Company C wants to mitigate risk across its hybrid network. The company also wants to ensure that should an attack happen, it can respond quickly.

The Problem

Company C's NetSecOps team is understaffed and needs to close critical skills gaps. Additionally, the company wants to adopt a Zero Trust Network Architecture (ZTNA) but is concerned about the potential loss of visibility in addition to its existing network visibility concerns.

What's a Zero Trust Network Architecture (ZTNA)?

ZTNA is a strategic security approach where an organization connects workers in cloud, remote, and on-prem environments by tunneling data. While this type of data transmission is more secure, it also makes traditional monitoring more difficult.

The Non-Resilient Network

At our non-resilient Company C, the NetSecOps team faces several barriers to building a more secure network. Here are a few of the most significant security challenges:

Manual threat investigation: The team's manual threat investigations often lead to errors and alert fatigue.

Existing lack of visibility: Company C also struggles with network visibility, which means it lacks fundamental insight into security weaknesses in its network.

Upleveled security concerns: Troubleshooting efforts overwhelms the NetOps team. Failure to develop troubleshooting workflows, a consequence of being understaffed, also means that entry-level/junior IT staff uplevel security concerns to senior staff, which is inefficient and keeps senior team members from larger projects.

Failing to implement resilient security measures, Company C will continue to manually investigate threats, which means that if/when the company experiences an attack, there's a chance the team will not catch it initially due to alert fatigue. The inefficient way the company currently processes security concerns also raises the overall level of risk. While it may implement a ZTNA, the Zero Trust framework will only amplify the team's existing visibility issues. ZTNAs use a tunneled and encrypted secure network perimeter, which makes visibility a struggle for traditional network tools. Poor visibility also leaves the company open to potential loss of income due to costs associated with performance slowdowns or outages.

What are SIEMs and SOARs?

SIEMs: Security information and event management (SIEM) technology uses data collection and analysis to support threat detection, compliance, and security incident management.

SOARs: Security orchestration, automation, and response (SOAR) technologies collect data, enabling companies to define incident analysis and develop appropriate response procedures in their IT workflows.

The Resilient Network

How would Company C address the need for additional security as a resilient network operating with the necessary security tools?

ZTNA visibility: The NetSecOps team would establish a ZTNA with the necessary visibility to monitor the system. Using Riverbed's Alluvio IQ Unified Observability Service, the team can identify problems and drill down into events around user concerns, issue severity, and problem areas (ISP, VPN, or gateways).

Automated threat investigation and response: Company C can also use Alluvio IQ to automate the analysis of security threats. Using its traditional security tools, the company can request access to Alluvio's rich data to supplement its security intelligence. The NetSecOps teams could also leverage security forensics runbooks powered by Alluvio IQ's intelligent automation. These runbooks collect relevant and contextual diagnostics data from third-party sources and Alluvio NPM before sending it back to the SIEM and SOAR solution requesting it for faster, more collaborative threat mitigation.

Increased team efficiency: With automated workflows in place, Company C's junior staff passes fewer issues to senior staff members, freeing senior staff to pursue other projects that improve the network and position it to scale. The team also sees a reduction in their mean time to resolve (MTTR).

Improved digital experience: Company C uses Riverbed's Digital Experience Management features like end-user experience monitoring for automatic app discovery and performance health tracking. The company also uses the Digital Experience Index (DXI) to set customized digital experience goals, track gaps in performance, and perform root cause analysis to further reduce security risks.

Using Riverbed's tools, Company C has effectively automated much of its security and detection response, which reduced its MTTR and improved its overall security posture. Additionally, the team increased productivity for senior staff members and leveraged system data to continue making security improvements that would mitigate security risks and position them to navigate an attack successfully.

Why Real-World Resilience Matters

In each situation above, Companies A, B, and C had dramatically different experiences navigating the same issues from a non-resilient and resilient standpoint. Even though our scenarios are fictional, each is representative of real-life situations that companies navigate in optimizing performance, improving security, and ensuring compliance in increasingly complex hybrid environments.

By the end of 2025, Gartner estimates that 30% of organizations will establish new roles focused on IT resilience. Building resilience, then, is crucial to an organization's success.

Shifting from a reactive to a proactive mindset is the first step in building resilience in your organization's IT infrastructure. Equally important is equipping your NetOps teams with the right tools to build resilience – tools that provide automated security solutions, game-changing end-to-end system visibility, and continuous monitoring to ensure internal and external compliance.

Ready to build better business resiliency to your hybrid network?

CONTACT US TO SCHEDULE YOUR RIVERBED NPM DEMO >

riverbed®

About 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.