riverbed®

EXECUTIVE PERSPECTIVE

Security Resilience in the AI Era

Strengthening Enterprise Security Through Deep Observability Insights.



Understand exposure. Reduce risk.
Protect business continuity.

riverbed

Security Resilience in the AI Era

Strengthening enterprise security through deeper technology intelligence.

Airlines grounded. Banking services disrupted. Critical government systems unavailable. Business productivity tools brought to a standstill.

A wave of major technology outages is affecting some of the world's largest and most sophisticated IT organizations. These disruptions are raising concerns in boardrooms around the globe, and IT leaders are being asked a deceptively simple question:

Are we ready?

Sometimes the cause is a cyberattack. Sometimes it is aging or outdated technology. And sometimes it is the unintended consequence of the very technology changes intended to make enterprises more secure.

Compounding the challenge, many IT organizations continue to operate in functional silos, with disconnected tools, data and processes. Yet applications, devices, operating systems and networks are increasingly interconnected and interdependent. An issue in one domain can have far-reaching consequences.

Too often, IT teams remain unaware of emerging issues until critical services are disrupted. Without a unified view, identifying root cause can take days or even weeks. In the meantime, the business remains exposed, productivity suffers and the risk of further disruption persists.

Despite decades of investment in cybersecurity and IT management, even the best-resourced organizations are finding it increasingly difficult to stay ahead of these risks.

Artificial intelligence is intensifying these risks — accelerating technology change, enabling increasingly sophisticated cyberattacks and compressing response times.

Nowhere is this pressure more evident than in enterprise patching. IT teams must keep pace with security updates while ensuring that the actions intended to protect the enterprise do not disrupt critical business operations.

Addressing these challenges requires a broader approach to enterprise security. Cybersecurity technologies play an essential role in protecting the enterprise. Observability technologies provide the intelligence needed to understand the technology environment being protected.

Cybersecurity		Intelligent Observability
Protect the enterprise		**Understand the enterprise**
Identify threats Discover vulnerabilities Prevent attacks Contain threats	+	Understand exposure Detect emerging issues Identify root cause Accelerate remediation

Together, a foundation for enterprise security resilience.

Together, they provide a more complete foundation for identifying risk, detecting emerging issues, accelerating root-cause analysis and taking corrective action before further disruption occurs.

Riverbed combines endpoint, application and network observability with AI-powered intelligence and automated remediation to help enterprises understand exposure and reduce operational risk.

riverbed

Security Begins with Visibility

Technology Intelligence for Enterprise Security Resilience.

You cannot effectively protect what you do not fully understand.

Enterprises have invested significantly in cybersecurity, vulnerability management, endpoint protection and patch management solutions. Each plays an essential role in protecting the organization.

Effective security requires more than an understanding of threats and vulnerabilities. It requires deep, continuous intelligence across the technology environment — connecting devices, applications, operating systems and networks to understand where risks exist, how they are evolving and their potential impact on the business.

Riverbed brings together cross-domain observability, AI-powered intelligence and automated remediation to extend the value of existing cybersecurity investments across five critical dimensions of enterprise security resilience.

Understand exposure. Reduce risk. Protect business continuity.

Technology Discovery and Asset Intelligence

Understand what is deployed across the enterprise — devices, operating systems, applications, software versions and configurations — and how these technologies are being used. Establish the intelligence necessary to make informed security decisions.

Attack Surface Reduction and Vulnerability Intelligence

Identify outdated, unsupported and unnecessary technologies, assess vulnerability exposure and prioritize opportunities to eliminate potential points of vulnerability.

Continuous Policy Compliance and Remediation

Use continuous technology intelligence to assess alignment with established enterprise policies, identify and report deviations, unauthorized software and configuration inconsistencies, and support authorized corrective actions.

Technology Change and Patch Assurance

Map affected technologies, inform risk-based patch prioritization, assess deployment readiness and validate operational health before, during and after security-related changes.

Network Security and Behavioral Intelligence

Leverage packet, flow, endpoint and infrastructure intelligence to understand network communications, investigate anomalous behavior, assess encryption and trust, identify dependencies and uncover potential security risks.

AI-Powered Intelligence Across All Five Dimensions

Riverbed IQ connects intelligence across domains to proactively identify emerging issues, accelerate root-cause analysis and orchestrate authorized corrective actions.

riverbed

Bringing Cybersecurity and Intelligent Observability Together

Three Categories of Leadership. One Unified Platform.

Enterprise security challenges rarely exist within a single technology domain. Devices, applications and networks are increasingly interconnected and interdependent. Yet the intelligence needed to understand and address security risks often remains fragmented across tools and organizational silos.

Riverbed brings together independently recognized leadership across three critical technology categories on one unified data and intelligence platform:

Digital Employee Experience (DEX) — recognized as a Leader by Gartner, Forrester and IDC, delivering intelligence across devices, operating systems and applications.

Network Observability — recognized as a Leader by GigaOm, delivering comprehensive packet, flow and infrastructure intelligence.

AIOps — recognized as a Leader by GigaOm, bringing AI-powered intelligence, cross-domain correlation, root-cause analysis and automated remediation together.

From Visibility to Understanding

Collectively, these capabilities help IT teams understand in real time what is happening, where it is happening, why it is happening and the potential impact on the business. This is especially important when symptoms appear in one domain but the underlying cause resides in another.

Understand exposure. Anticipate risk. Prevent disruption. Accelerate recovery.

Proactive Defense and Risk Reduction

By understanding technology exposure, dependencies and emerging risks, IT teams can make more informed decisions about defensive planning and take preventative action before issues impact the business.

This includes mapping affected technologies against vulnerability data, assessing patch readiness, monitoring rollouts and validating operational health. Riverbed complements existing patch management tools; it does not deploy patches.

Unified intelligence also helps teams reduce the attack surface by identifying unnecessary or unsupported software, investigate anomalous network traffic and configuration changes, and address overlooked technology risks. Emerging opportunities include browser extensions and device drivers.

From Reactive Response to Intelligent Action

When incidents occur, time matters. Riverbed helps IT teams accelerate root-cause analysis, identify appropriate corrective actions and orchestrate governed automated remediation at machine speed and scale.

Together, these capabilities extend the value of existing cybersecurity investments, helping enterprises move toward proactive security resilience and protect business continuity.

riverbed

The Path Forward

Building a More Secure and Resilient Enterprise.

The increasing pace of technology change, the growing sophistication of cyber threats and the complexity of today's interconnected technology environments are fundamentally changing the challenge of enterprise security.

For management, the question is no longer simply whether the organization has invested sufficiently in cybersecurity. It is whether the organization has the visibility, intelligence and operational capabilities necessary to manage security risk in an environment of continuous change.

Addressing this challenge requires a broader approach to enterprise security — and a shift in how organizations think about protecting the business.

Break Down IT Silos

The organizational structures, technologies and processes that have historically separated security, network operations, application management and end-user computing can limit an enterprise's ability to effectively manage risk.

Security risks do not respect these organizational boundaries. Neither should the intelligence used to address them.

A unified understanding of the technology environment provides a stronger foundation for collaboration, more informed decision-making and coordinated action across the enterprise.

Understand Exposure. Reduce Risk. Protect Business Continuity.

Extend Security Investments

Enterprises have made significant investments in cybersecurity, vulnerability management, endpoint protection and other security technologies. These investments remain essential.

Intelligent observability complements these technologies by providing a deeper understanding of the environment being protected, the risks that exist within it and the operational implications of security-related decisions.

The opportunity is not to replace existing cybersecurity investments, but to make them more effective.

Establish Proactive Defenses

Too often, organizations are forced to respond to security and operational issues after they have already impacted the business.

By combining comprehensive observability with AI-powered intelligence, enterprises can better anticipate emerging risks, inform defensive planning, prioritize preventative actions and improve their ability to respond when incidents occur.

This represents an opportunity to fundamentally change the economics of managing technology risk — reducing the operational burden of incident response while minimizing the potential for costly business disruption.

Advance Toward Zero Disruption

Ultimately, the objective of enterprise security extends beyond protecting technology. It is about protecting the business.

As enterprises reassess their security strategies for the AI era, management must consider not only how effectively they are protecting their technology environments, but how well they understand them, anticipate emerging risks and respond to accelerating change.

Riverbed's unified data and intelligence platform brings together independently recognized leadership in Digital Employee Experience, Network Observability and AIOps to help enterprises address this challenge.

By combining intelligent observability with existing cybersecurity investments, enterprises can establish stronger defenses, reduce operational costs and better protect business continuity.

In an era of accelerating technology change and increasingly sophisticated security threats, the question every IT leader should be asking is:

Are we ready?

riverbed®

Understand Exposure. Reduce Risk. Protect Business Continuity.

Advancing toward Zero Disruption IT.



riverbed.com

Copyright and trademarks

© 2026 Riverbed Technology LLC. All rights reserved.

Riverbed and the Riverbed logo are trademarks or registered trademarks of Riverbed Technology LLC. Other company and product names may be trademarks of their respective owners.