riverbed

Solution Brief

Riverbed Security Solutions

Strengthen security postures without compromising agility and performance

Corporate applications, data, and devices are everywhere in today's digital economy as a result of cloud-first strategies, the Internet of Things (IoT), mobile workforces, and other technical transformations. But while these initiatives are important for competitive differentiation, the resulting IT perimeter is becoming more distributed and complex to secure.

At the same time, security can't be done at the expense of performance or agility. In a disrupt-or-be-disrupted landscape, IT needs to evolve legacy operations to keep pace with digital business demands—without compromising security. Moreover, having the most stringent security measures means little to customers and employees if they don't have fast and reliable access to their apps and data.

What enterprises need is an integrated set of solutions that treat security, agility, and performance as complementary goals—mitigating threats and protecting corporate assets while still enabling the business to innovate quickly.

Challenges

CISOs face greater pressure to manage risk end-to-end across the digital enterprise, prompting them to employ more security staff and additional layers of technology.

Even so, high-profile breaches continue to happen at an alarming rate, diminishing business reputations and disrupting consumer confidence. So while calculated steps are taken to harden security perimeters, attacks continue to happen for a number of reasons.

If you can't see it, you can't protect or control it: While the end goal is to prevent intrusion, that's only part of the equation. Understanding activity before and after attacks is just as vital. Unfortunately, new threats can go undetected for weeks or months at a time. In fact, the average number of days it takes to discover attackers are present on a victim's network is 101 days[1].

Thwarting future attacks is equally difficult. IT must manage a highly dynamic environment where apps, network, and device inventories continuously change, making it difficult to audit and map the infrastructure and increasing the risk for compliance or regulatory violations. Controlling access and usage is equally difficult, as segmenting networks for different user policies and application requirements—across all locations—is cumbersome with traditional networking tools.

Cloud, Internet, and Wi-Fi access—Business necessities that add complexity and risk: The near ubiquity of Wi-Fi, broadband Internet, and cloud services helps connect users to business services from anywhere—a critical requirement of the digital age. But they also introduce tradeoffs and higher levels of risk.

Internet breakouts at branch locations often force IT to backhaul cloud or SaaS traffic to a data center, which adds latency and impacts user experience. On the other hand, going direct-to-net bypasses datacenter-grade security, and setting up the right security infrastructure at every site is costly and often impractical.

Enabling cloud connectivity is equally time-consuming, as commonly used VPNs involve complex setups and negotiating policies between IaaS providers and all sites. Lastly, BYOD policies force IT to securely onboard more devices to the corporate Wi-Fi, and employees who wish to access corporate assets on public Wi-Fi networks introduce additional security and access concerns.

Massive volumes of edge data are left unprotected: Data, the lifeblood of the digital enterprise, always needs to be at our fingertips. The age of IoT—where real-time analysis is needed for faster, smarter decision-making—will only intensify this need for instant data accessibility.

Because of this, 75% of enterprise data will be created and processed outside the data center or cloud, up from less than 10% today[2]. But while fast access to data is a digital-age necessity, most business locations lack the proper data protection measures, putting critical assets at risk for theft or loss. Compounding the problem are traditional approaches to backing up data, which are expensive, error prone, and tedious.

Even with stringent instrumentation, security gaps will occur: One additional layer of complexity is the age of the mobile-and-always-connected user, where IT perimeters are continually expanding, surface areas attackers can exploit are enlarging, and the boundaries IT must protect are blurring.

Solutions

Riverbed provides a unified, integrated Digital Performance Platform that optimizes the way customers deliver the apps and services that power today's digital transformation efforts. Customers leveraging our platform not only achieve new levels of business performance and operational agility, but also gain a number of capabilities that strengthen security postures.

> With Riverbed products "you can quickly identify unauthorized network traffic patterns" and it's "a must have for any security-conscious business."
>
> -Chief IT Architect/Director of Network Security, Kronos

Enhanced Visibility and Security Controls

Security practitioners must be able to quickly detect threats that slip through typical prevention measures, and they need to arm response teams with the forensics that help investigate an attack. Riverbed's network and security monitoring solution fills in the visibility and analytics gaps by providing:

- Threat intelligence, which alerts on known indicators of compromise (e.g., malware, viruses, spyware) so teams can investigate and respond before the threat does real harm.
- DDoS detection, which quickly identifies a wide range of DDoS attacks and automatically triggers mitigation efforts.
- Cyber threat hunting, which proactively seeks out advanced, persistent threats that have gained access to your environment.
- Security analytics to examine traffic and detect irregularities that could represent a threat, such as unexpected spikes in traffic or new hosts or services.
- Incident forensics that assist with remediation and containment efforts by providing full historical details about the scope of the attack.

Once you understand and address existing threats, Riverbed's SD-WAN solution helps prevent future issues that stem from unwanted or unlawful access:

- Centralized policy automation and orchestration enables teams to create and publish granular rules that govern network access in only a few clicks. Ease of segmenting the network minimizes security

events that occur due to human error and limit blast radiuses if/when attacks do occur.

- Visibility into network or application usage helps validate that polices are being enforced, while insights into network health allow IT to more easily balance performance and security requirements.
- An integrated firewall with application-based controls further enforces acceptable usage to protect both users and corporate assets.

Data Centralization and Protection

Storing data at the edge not only puts critical information at risk for theft or loss, but the infrastructure required to support local copies is also costly and operationally complex. Riverbed's software-defined edge computing solution simplifies IT operations and safeguards corporate data—without compromising business execution—by:

- Reducing reliance on edge servers, storage, and backup equipment and centralizing data in the secure data center, cloud, or a hybrid mix.
- Projecting working volumes of data to the edge only when and where needed while keeping data encrypted in-flight and at rest.
- Eliminating manual branch backups. Data or site recovery is done continuously from the data center or cloud in minutes for a low recovery time objective (RTO), with limited loss of critical data for a near zero recovery point objective (RPO).
- Using snapshot technology to instantly roll back to a virus-free recovery point when data is impacted by malware, further improving recovery windows.

Simplified, Secure Connectivity

Enterprises need to enable users with fast, reliable access to Wi-Fi, the public Internet, and cloud-based resources while ensuring corporate assets remain protected. Riverbed's cloud networking solution—which combines SD-WAN, WAN optimization and visibility, and cloud-enabled Wi-Fi—simplifies and automates connectivity across the enterprise while eliminating the trade-offs that often exist between security and performance.

- AutoVPN functionality provides end-to-end encryption, simplifying and securing the use of any transport. Direct-to-Internet can now be used with confidence, so traffic is steered over the optimal path for better performance and user experiences.
- Cloud-enabled Wi-Fi provides easy and secure access for all types of users, including BYOD employees, guests, and customers. Single sign-on with Microsoft Azure and Google provides role-based access to apps and data. Policies governing access and security then follow users across all Wi-Fi-enabled locations.
- One-click connectivity into Microsoft Azure and Amazon Web Services automates and secures connections between branch offices, data centers, and clouds.
- WAN optimization accelerates cloud, SaaS, and on-premises apps for performance and productivity improvements.

> "We don't have to worry about security or reliability; we now have a fully encrypted backbone that we've deployed using Riverbed at on- and off-ramp points. We literally have an automated solution we can dial up what we need and it's on demand."
>
> -Rob Gillan, CTO, SimplePay

How Riverbed Helps Protect Your Digital Business

Category	Network and Security Monitoring	SD-WAN/Cloud Networking/WANOP	Software-Defined Edge
Plan/Identify	X	X	
Protect	X	X	X
Detect	X		
Respond	X		X
Recover		X	X

In addition, our solutions:

- Are designed with security built-in, not bolted-on, and are trusted in some of the most security-minded verticals like finance and government.
- Minimize appliance sprawl, including the need for physical servers and routers at branch locations, helping reduce potential attack surfaces.
- Offer an extensible services platform to run virtualized security functions, further simplifying branch infrastructure and management complexity.
- Work well with existing security solutions, allowing you to layer-in added capabilities without disrupting existing deployments.

Learn More

IT leaders today often face trade-offs between security, performance, and agility when enabling the business's need to innovate digitally. Embrace new technologies quickly, or seek stability? Offload more to the cloud for scale and simplicity, or preserve control over the hosting infrastructure? Evolve legacy ops despite complexity or risk, or work within current constraints?

The Riverbed Digital Performance Platform delivers a suite of capabilities to eliminate these compromises, accelerating your digital business outcomes while maintaining tighter control over apps, networks, and data.

To learn more, please visit riverbed.com/security.

Footnotes:
1. "M-Trends 2018," Mandiant, a FireEye Company
2. Gartner, "Technology Insight: Edge Computing in Support of the Internet of Things," July 13, 2017

About Riverbed

Riverbed®, The Digital Performance Company™, enables organizations to maximize digital performance across every aspect of their business, allowing customers to rethink possible. Riverbed's unified and integrated Digital Performance Platform™ brings together a powerful combination of Digital Experience, Cloud Networking and Cloud Edge solutions that provides a modern IT architecture for the digital enterprise, delivering new levels of operational agility and dramatically accelerating business performance and outcomes. At more than $1 billion in annual revenue, Riverbed's 30,000+ customers include 98% of the *Fortune* 100 and 100% of the *Forbes* Global 100. Learn more at riverbed.com.

riverbed®