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 business transformations. But while these initiatives are essential to drive positive business outcomes, the expanding attack surface 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—managing vulnerabilities, hunting and 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, impacting 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: 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 time it takes to identify and contain a breach is 280 days[1].

The lack of full-fidelity visibility—the ability to capture and store all flow, packet and device metrics all the time —hampers IT's ability to see threats or to have necessary data on hand for threat hunting, incident response or forensics analysis.

Thwarting future attacks is equally difficult. IT must manage a highly dynamic environment where apps, network, and device configurations 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.

[1] https://www.ibm.com/downloads/cas/RZAX14GX Ponemon, 2020

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, while 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.

Visibility and Performance of Encrypted Apps: For years, organizations have relied upon encryption to secure digital communications. SSL (Secure Socket Layer), and more recently TLS (Transport Layer Security), have been the preferred encryption protocols. Today, the vast majority of customer network traffic is encrypted, with some estimating more than 90% of all digital traffic is encrypted (Netmarketshare). But encryption is a double-edged sword. On the positive side, encryption protects our customers' most sensitive and critical data. At the same time, it blocks their ability to monitor and inspect network traffic, masking their ability to detect errant traffic patterns, anomalous behavior and malicious threats. In fact, 71% of malware installed through phishing is hiding by encryption. (F5 Labs Threat Intelligence)

Encryption also complicates customers' ability to optimize network bandwidth and accelerate applications over long distance—capabilities that are needed more than ever to assure the performance, productivity and user experience of a workforce that is more distributed and dynamic than ever before. Users now work-from-anywhere, connect to networks with less predictable performance, and interact with applications over longer distances, spread out across on-premises, SaaS and Cloud environments.

"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

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

The Riverbed® Network and Application Performance Platform enables customers to visualize, identify and mitigate cybersecurity threats and accelerate the performance of any network for any application. 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.

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 full-fidelity flow and packet data enables the in-depth visibility and analytics to detect and investigate performance problems and security threats by providing:

- Incident response to assist with remediation and containment efforts by providing full historical details about the scope of the attack
- 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
- 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

Secure Cloud Migration and Access: As enterprise enable branch to internet access as part of their cloud journey, Riverbed® SteelConnect™ EX WAN-edge solution provides the ability to "software-define" security functions and operations (e.g. policy creation and enforcement)Our software-defined security architecture provides greatest flexility to deploy various advanced security functions on-demand or service chain with on-prem or cloud-based 3rd party security services. Riverbed integrated advanced security includes:

- NextGen Firewall
- IPS/IDS
- Anti-Virus/Malware Protection
- Content and URL filtering
- Unified Threat Management

Simplified, Secure Connectivity: Enterprises need to enable users with fast, reliable access to 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, simplifies and automates connectivity across the enterprise while eliminating the trade-offs that often exist between security and performance.

- WAN optimization accelerates cloud, SaaS, and on premises apps for performance and productivity improvements
- Now, IT can enable SSL/TLS acceleration once and select which apps to accelerate with zero-touch acceleration of encrypted apps, eliminating the burden and risk associated with collecting, creating and distributing encryption certificates and keys. Boost the performance for any SSL/TLS application by up to 10x or more while simultaneously reducing bandwidth requirements by up to 99%.

How Riverbed Helps Protect Your Digital Business

Category	Network and Security Monitoring	SD-WAN	App Acceleration/ WANOP
Plan/Identify	×	×	×
Protect	×	×	×
Detect	×		
Respond	×		
Recover		×	×

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
- Offer an extensible WAN Edge 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.

About Riverbed

Riverbed enables organizations to maximize performance and visibility for networks and applications, so they can overcome complexity and fully capitalize on their digital and cloud investments. The Riverbed Network and Application Performance Platform enables organizations to visualize, optimize, remediate and accelerate the performance of any network for any application, and helps to identify and mitigate cybersecurity threats. The platform addresses performance and visibility holistically with best-in-class WAN optimization, unified network performance management (NPM), application acceleration (including Office 365, SaaS, client and cloud acceleration), and enterprise-grade SD-WAN. Riverbed's 30,000+ customers include 99% of the *Fortune* 100. Learn more at at riverbed.com.

riverbed®