Riverbed Security Solutions

Strengthen Security Postures While Improving Business 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 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 business demands—without compromising security models. Moreover, even the most stringent security measures mean very little to customers and employees if they can't access 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 at a time. The average number of days it takes to discover attackers are present on a victim's network is 146 days[1].

What's more, thwarting future attacks is equally difficult due to:

- Limited insights into application and network layers, on and off the cloud, hampering IT's ability to proactively identify and respond to threats.

- Apps, networks, and device inventories that continuously change, making it difficult to audit and map the infrastructure. This also increases the risk of compliance or regulatory violations.
- Segmenting the network for different user policies and app requirements—across all locations—is cumbersome using traditional networking tools.

Cloud and Internet—Business necessities that add complexity and risk: The cloud and public Internet help deliver agility, cost-efficiency, and reliable connectivity to business services—all requirements of a digital age. But at the same time, they also introduce new levels of risk.

Internet breakouts often force IT to backhaul traffic to a data center, which adds latency and impacts application performance. On the other hand, going direct-to-net bypasses datacenter-grade security devices, and setting up the right infrastructure and policies 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.

Massive volumes of edge data are left unprotected: Data, the lifeblood of the digital enterprise, always needs to be at the tips of users' fingers. Because of this, businesses store 50% of data at remote offices and branch offices (ROBOs)[2], where most enterprise transactions and customer interactions take place.

While fast, local access to data is necessary for business execution, ROBOs often lack the protection mechanisms employed in data centers, 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 and vulnerabilities occur: Intensifying complexity even further is the age of the mobile user, where IT perimeters are continually expanding, increasing the surface area attackers can exploit while often obscuring the boundaries IT must protect.

Solutions

Riverbed can help you enhance your security posture while improving agility and performance by:

- Helping identify threats, so teams can remediate them quicker, with up-to-the-minute insights of what's running across your infrastructure.
- Centralizing and safeguarding all corporate data —without impacting its availability or application performance—for improved business continuity.
- Delivering fast, secure access to the Internet and cloud resources users need to conduct critical business activities.

Enhanced Visibility and Security Controls

Knowing what apps and devices are running on the network helps deliver metrics that matter to security and network teams—what systems are on the network, who is talking to whom, over what ports or protocols, and where the traffic is flowing. Traditional approaches to gathering this data fall short because asset inventories are almost never complete and, at best, are only as current as the last scan.

Riverbed's application and network performance monitoring solutions fill in the gaps by helping IT teams identify and respond to attacks with:

- Real-time views of network devices, dependency maps, and usage to baseline what's normal so irregularities can be identified and investigated.
- Behavioral analytics that help detect threats like malware or shadow IT apps.
- Threshold alerts and reports that offer forensics during and after attacks to assist with containment and remediation efforts.
- Workflows for managing configuration changes, tracking compliance to common security standards, performing security checks, and creating audit reports.

Once you know what apps and devices are on the network, Riverbed's SD-WAN solution simplifies the creation and enforcement of policies that control usage based on access privileges or other factors.

- Centralized, intent-based policy management means segmentation rules can be created and modified globally with only a few clicks.
- 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.

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 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.
- Eliminating manual branch backups. Data or site recovery is done 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).

> "[Riverbed] has simplified my operations. Users at remote sites are happy because their data is better protected, and performance is better. We achieved the technical benefits we needed, but also business benefits such as cost savings."
>
> Jerry Vigil
> IT Director, Bill Barrett Corporation

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

- Using snapshot technology to instantly roll back to a virus-free recovery point when data is impacted by malware, further improving recovery windows.
- Projecting working volumes of data to the edge only when and where needed while keeping data encrypted in-flight and at rest.
- Using WAN optimization to ensure apps perform as expected and that data is available when needed.

Simplified, Secure Connectivity

Enterprises need to enable users with fast, reliable access to Internet and cloud-based resources while ensuring corporate assets remain protected. Riverbed solutions simplify and automate 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 application performance.
- Dynamic, policy-driven enforcement of Internet access—combined with network segmentation rules—securely integrates BYOD and guest Wi-Fi traffic into the WAN.
- An integrated firewall with application-based controls further enforces acceptable usage to protect both users and corporate assets. Riverbed solutions also integrate with best-of-breed firewalls, offering deployment flexibility so customers can maximize existing investments.

- Integrations with leading security platforms, such as cloud access security brokers (CASBs), augment defenses while reducing the need for additional security devices at each business location.
- One-click provisioning into Microsoft Azure and Amazon Web Services automates and secures cloud connectivity back to data centers and branches or between clouds. Cloud acceleration technology then enables faster 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 Protects Your Enterprise

Category	Network and App Monitoring	SD-WAN and Cloud Networking	WAN Optimization	Software-Defined Edge
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.
- 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 organizations to layer-in additional capabilities without disrupting existing deployments.

Footnotes:
1. SecurityWeek, "Breach Detection Time Improves, Destructive Attacks Rise," Feb. 25, 2016
2. Riverbed, "Data Center and Branch Office Resiliency," Feb. 2015

About Riverbed

Riverbed, at more than $1 billion in annual revenue, is the leader in application performance infrastructure, delivering the most complete platform for the hybrid enterprise to ensure applications perform as expected, data is always available when needed, and performance issues can be proactively detected and resolved before impacting business performance. Riverbed enables hybrid enterprises to transform application performance into a competitive advantage by maximizing employee productivity and leveraging IT to create new forms of operational agility. Riverbed's 27,000+ customers include 97% of the *Fortune* 100 and 98% of the *Forbes* Global 100. Learn more at riverbed.com/security

riverbed