riverbed

White Paper

Accelerating Application Performance - Without Compromising Enterprise Security

Complexity breeds challenges in ensuring security and application performance

Improve your application security with Riverbed solutions − purpose-built with security in mind and based on industry-recognized security standards

Hybrid networks have improved the business user's productivity, but they have also radically pushed the limits of conventional security controls and unleashed a seemingly infinite number of new attack vectors for miscreants, criminals, and governments to exploit.

Users no longer sit behind desks on corporate issued and patched systems, and often no longer access data located in corporate-controlled data centers. Today's users might well be on a personally owned laptop, connected to an open Wi-Fi hot spot at a coffee shop, accessing data that resides in the cloud.

Despite all of these changes, the expectation is that both the user's system and the data they are accessing are still secure at all times.

Another growing threat is "shadow IT," a natural follow-on to the consumerization of IT. Users grow dissatisfied with the services offered by corporate IT and simply deploy their own. Free and ubiquitous services such as those from Dropbox (free document repository and exchange), Google (free file storage, email, chat rooms), Facebook, Evernote and others have employees setting up their own IT services completely outside the control of IT. It isn't hard to imagine corporate secrets and intellectual property being accidentally exposed.

Accelerating Application Performance - Without Compromising Enterprise

For years companies have been adding layer upon layer of threat detection tools to their arsenal, yet data compromise is accelerating, not slowing. Add to this the sprawl of data and users and it becomes a recipe for disaster.

Visibility

If you can't see it, you can't protect it

While the end goal is always to prevent intrusion, that is only part of the challenge. Consider the following:

- Do I even know everything I should be guarding?
- Am I guarding everything at the same level with the same controls, or do I have tiers of trust?
- How brittle are my controls? Will a single crack be all it takes to lose everything?

Answering these questions requires detailed visibility, including:

- Which systems are on the network
- Who is talking to whom
- What applications are running
- Over what ports/protocols
- Where the traffic is flowing

Not only is visibility into the network beneficial for understanding what we are trying to secure, it is also a common requirement across most information security regulations.

Traditional approaches to gather this data try to combine reports generated by vulnerability and patch management systems with data gathered by interviewing applications teams. Auditors often test this control through a manual review of a selected sample of the asset inventory, looking for the existence of those systems and the completeness of the recorded data set. This approach falls short because asset inventories are almost never complete and, at best, are only as current as the last scan.

Riverbed enables you to develop and maintain an ongoing, real-time, accurate view of the network including:

- ✓ Complete inventory of network assets – Riverbed shows you all of the users, applications, hosts, and devices on the network as well as all ports/protocols used with current and historical profiles. This inventory reflects a real-time view of the network and identifies even unauthorized deployments of which IT is unaware.
- ✓ Map of network dependencies – Riverbed shows you actual dependencies, which may differ from expected dependencies on the network. This very important – but sometimes overlooked – distinction is critical for ensuring an up-to-date view of the network. Riverbed also shows how traffic flow and behavior changes with revisions in dependencies, such as the addition or removal of a dependent host, application, or service.
- ✓ Actual usage – Riverbed logs all activity on the network to provide you with details about who is on the network, which systems are accessed, which ports and protocols are used, and how much bandwidth is consumed.

Context

Visibility tools are necessary for developing a baseline—an understanding of what's normal. Without this fundamental knowledge it is impossible to understand risk, impossible to identify areas where attackers might attempt intrusions, and impossible to know how to recover from a breach. Riverbed observes traffic and reports details such as:

- What a system is doing right now
- Who are a system's administrators and normal users
- What business units or processes are affected if the system goes offline
- What happens in the minutes immediately before and after a breach

Accelerating Application Performance - Without Compromising Enterprise

Attacks often cause reduced functionality or complete outages. Modeling the financial and productivity costs of outages can help you budget appropriately for information protection tools and procedures. It can also help you determine where best to place redundant systems and copies of production data.

Understanding the behaviors immediately before and after an attack is critical for remediation. This knowledge will help you determine whether an attack was just a nuisance, like a probe from a script kiddy, or a targeted intrusion specifically intended to exfiltrate your intellectual property.

The Riverbed suite of application-aware network performance monitoring (aaNPM) tools provides this exact context, and can easily integrate this data into security information and event management (SIEM) and asset management databases.

Trust but Verify

Of course we want to trust our employees, and they may in fact be trustworthy, but the reality is that the easiest way to breach network defenses is to pose as an employee. Compromising an employee's credentials can happen in many ways, a few of the more common and popular means are:

- Spear phishing
- Hostile adds on web sites and social networks
- Pineapple attacks
- Social engineering ones way into a physical office building
- Leaving a pile of malware-infested USB sticks in the corporate parking lot

The reason these are such dangerous attacks is that once any type of access to the network is gained, little stands in the way to detect or monitor the attackers actions; after all, they are assumed to be an employee.

The notion of watching and auditing connectivity inside the network perimeter is often referred to as tracking lateral movement. Historically this has been a cost-prohibitive endeavor due to the large foot-print a network has. However, Riverbed is able to leverage the network itself as a means of telemetry, keeping costs controlled while providing exceptional visibility across the entire LAN and WAN.

Riverbed is not only able to maintain a detailed history of all lateral movement, but controls can be applied against this audit trail to provide early warning to violations of acceptable use, regulatory requirements, or potentially hostile activity.

Standards and Consistency

As networks grow, routers, firewalls, proxies, and other devices seem to crop up at an amazing pace. Unfortunately, ensuring that they all function as anticipated can quickly become unmanageable.

- Are redundant network paths as secure as the primary?
- Are any paths created that were not expected?
- Do any temporary/emergency/testing holes still exist?
- Does each router, firewall, and proxy have the same and latest configuration?
- Are all these devices configured following best practices?

Riverbed's Configuration Management and Modeling technologies allow organizations to wrestle this under control. You can:

- Manage configuration changes
- Ensure configuration adheres to best practices as suggested by PCI Security Council, NIST, DoD, or others
- Plan for infrastructure lifecycle, including end of support
- Conduct robust survivability analysis
- Model the impact of common attacks such as DDoS, DNS Amplification, HTTP Amplification, and more
- Quickly document adherence to auditing frameworks

- Globally and automatically apply any of over 1,500 out-of-the-box rules based on industry best practices, security standards, and customized rules and templates for organizational standards and requirements

The Riverbed suite of Network Planning and Configuration Management tools drives workflows of this style into daily operation.

Remediation

There is an emphasis within the security industry on prevention. However, the inevitable might still happen one unfortunate day. This makes preparedness for remediation just as important. Despite multiple layers of preventative security such as firewalls, antivirus, and malware detection, security breaches can prevail. What then?

The most important steps in any remediation process are to contain the breach, narrow the scope of the attack, and get back online as soon as possible. Resist the initial urge to find out who's responsible, because this information can often be wrong and it won't help you recover from an incident.

Riverbed's network visibility tools deployed can help you answer the important questions:

- How did the attacker obtain access?
- What did the attacker examine and/or steal?
- How did the attacker conceal evidence and depart?

Attackers rarely grind against password prompts or attempt other forms of brute force intrusion methods these days. Instead, the common technique is to social engineer someone who already has a degree of access. The amount of work is less, and the reward is greater. From there, the attack can more easily spread across the network. Perhaps a privileged user once logged onto a normal workstation and failed to clear the cached credential. An attacker can discover this and use it to impersonate a privileged user, thus gaining access to many more resources on the network.

Riverbed can help you understand what items of interest an attacker pursued. Following an intruder's path across the network can reveal areas where stronger access control or additional isolation would fortify defenses in the future. Attackers regularly try to remove any traces of their presence by modifying or deleting logs. Riverbed can thwart such behavior by capturing all packets—when logs seem suspicious, packets will tell the true story.

The Riverbed suite of application-aware network performance monitoring (aaNPM) tools provides this exact functionality, and can easily integrate this data into Security Information Management (SIM) tools.

> 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 Networks and Security, Kronos'

What about the Branch

If we are to believe the saying that "a chain is only as strong as its weakest link", then we better watch the branch office, because it can be a weak link.

Branch offices, as opposed to data centers, are where the workers reside. However, branches typically have little to no IT staffing, less robust physical security compared to that of a data center, and limited budgets for security

The growth in SaaS-delivered applications such as Microsoft's' Office 365, Google Docs, Salesforce and others is creating a significant shift in the amount of branch office traffic destined for the data center vs. destined for the Internet. This combined with the price disparity between Internet bandwidth versus MPLS

bandwidth explains the rise in Internet breakout at the branch.

Visibility, context, standards and consistency, and remediation all now need to exist in the branch as well as the data center.

This is where the SteelHead appliance takes on a second persona. Traditionally deployed for WAN acceleration, SteelHead provides a host of other functions, at no additional cost, that can be leveraged by security teams.

Specifically, every SteelHead can double as a:

- Distributed packet capture appliance with access to traffic contained within the branch or destined for the Internet
- NetFlow generation appliance, producing records of every conversation in the branch and feeding that back centrally for lateral movement tracking and alarming
- Host platform on which you can run conventional security controls such as a firewall or content filter
- Tethering point for connecting the branch to cloud security services such as Zscaler

In addition, since branch offices lack the security of the data center, you must maintain local servers, storage, and backup to ensure user productivity. With Riverbed SteelFusion, you can centralize branch storage in your data center. A working set of data then is projected to your branch at any given time. SteelFusion delivers data securely from the data center using SSL and encrypts data while in use in the branch using advanced AES 256-bit encryption. Data on stolen appliances or drives is inaccessible without admin authentication. When you control and secure data centrally with SteelFusion, you reduce risk to your business, lower branch IT costs, and better utilize data center investments.

Reduce Attack Surface Area

Eliminate risks and harden security with data centralization and recovery efficiency.

Bank robber Willie Sutton reportedly said, “I robbed banks because that’s where the money is”. Today’s thief might preamble with, “I hack the branches because…”

People need access to data no matter where they or the data are located. Many jobs require people to spend time in locations that are unsuitable for possessing local copies of data. Traditional methods for supporting such constrained environments often result in poor application performance and spotty availability. When workers can’t securely access what they need when they need it, deliverables might be delayed or missed.

Data centers are purpose-built to secure systems and data, help insure integrity of intellectual property, ensure business continuity, and provide for recovery after interruptions and disasters. Even in places where it’s safe to maintain local copies of data, branches and remote offices generally lack the continuous protection mechanisms typically employed by data centers to safeguard data from risks.

By enabling consolidation and centralization of data in the data center, Riverbed solutions eliminate the operational risks and inefficiencies associated with storing data in remote locations. Virtual servers and data can be projected to remote offices over an encrypted session, keeping all data at rest encrypted, while continuously backing it up for an almost real-time recovery point objective. Users experience high performance and availability because access is local, while authoritative data sources remain in the data center. If a disaster occurs, it’s possible to recover the data to anywhere in the world in minutes.

Accelerating Application Performance - Without Compromising Enterprise

> This is all about risk mitigation. We're a law firm, and having data protection as we have it protects the client's interest."
>
> Searl Tate,
> Director of Engineering,
> Paul Hastings

Enterprises can conduct business across the globe in any location without putting data at risk. Riverbed protects data in flight with industry-standard TLS 1.2 or IPSEC encryption and secures cached in-use data with AES 256-bit encryption, compliant with FIPS 140-2 standards.

Riverbed solutions offer customers operationally feasible ways to get the data out of the branch. Collapsing all data back to the data center offers an immediate improvement in security posture and enables the focus of limited security resources to fewer locations.

Control

Security and performance matter

Disconnecting a system from all networks and locking it in a vault may be the most secure option, but the resulting user experience will be unacceptable, resulting in either no business transacting, or alternative systems being deployed in shadow-IT fashion.

Leveraging the same instrumentation and data collection methods used for security visibility and triage, Riverbed also delivers industry leading performance management.

Riverbed SteelCentral Performance Management is the only performance management suite that combines enterprise-class end-user, application and network performance management in one solution. Riverbed delivers visibility, analytics and insight empowering companies to detect and fix application performance issues before end users notice a problem, call the help desk to complain, or jump to another activity out of frustration.

By combining industry leading performance management[1] with security visibility, end users further reduce complexity and cost.

Summary

Today's IT environment is complex. Diversity of network connectivity, access devices and data repositories makes the job of securing it all while maintaining acceptable performance much more challenging than just a few years ago.

Given these changes in architecture, we must change how we think about and address security threats. No longer do we have a single data center with all the corporate jewels sitting centrally. Therefore, we must broaden where we watch for security threats, as well as how we prepare to respond to them.

Riverbed offers a unique portfolio of solutions that can:

- Help consolidate distributed data back to a limited number of high-security data centers
- Automatically document everything in the environment along with how systems are dependent upon each other for security and data availability
- Foster what-if analysis for contingency planning
- Maintain an audit trail of all lateral network activity both in the branch and in the data center
- Combine security intelligence with performance management to offer the most cost effective solutions

> "Our design engineers see the same high level performance as they were getting previously but their work is now contained within a more resilient and secure environment,"
>
> Marco Malavolta
> Head of IT Infrastructure,
> WAMGROUP

[1] Riverbed Performance Management is a leader in the 2015 Gartner Magic Quadrant for Network Performance Management and Diagnostics.

Accelerating Application Performance - Without Compromising Enterprise

Riverbed, at more than $1 billion in annual revenue, is the leader in application performance infrastructure, delivering the most complete platform for the hybrid WAN 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 WANs to transform application performance into a competitive advantage by maximizing employee productivity and leveraging IT to create new forms of operational agility. Riverbed's 26,000+ customers include 97% of the *Fortune* 100 and 98% of the *Forbes* Global 100. Learn more at www.riverbed.com/steelhead.