

Security for the Borderless Era

Riverbed Cascade Delivers Universal Visibility & Control

Bigger, more complex networks. More serious actors – insiders, cyber criminals and nation states. More serious threats – advanced persistent threats (APTs), fraud and espionage.

Network defenses such as intrusion detection / prevention systems (IDS/IPS), firewalls, and antivirus are critical first measures of defense, but have limitations that prevent complete protection of enterprise networks. These tried and true security solutions fail to defend against advanced persistent threats, internally instigated or credentialed attacks, or zero-day threats. Further, they add expense and management complexity, especially in highly meshed (MPLS), 10gig and virtualized networks, and can introduce performance bottlenecks and points of failure into the very networks they are trying to secure.

Riverbed Cascade is a next-generation monitoring platform that provides enterprises an omnipresent view of all activity on the network. With Cascade, Information Security (InfoSec) teams can address a broad range of security and governance challenges, including targeted malware, APTs, fraud, espionage and forensic audit.

Network behavior analysis

Cascade takes a different approach to security by analyzing network behavior in real time instead of relying on signatures to identify attacks. Utilizing network flow data from routers and switches, as well as packet data collected from network SPANs, Cascade provides real-time, enterprise-wide network visibility, context, and control. Cascade passively monitors network traffic to build a model of the behavior of applications, systems, and users. These models automatically adjust and adapt to changes in network traffic patterns over time. Cascade then compares real-time traffic to these historical models to identify changes in behavior indicative of security violations as well as usage and access policy violations. Cascade can then respond to these violations with a number of passive and active measures, leveraging your existing enforcement points on the network, including network access control (NAC), firewalls, routers, switches and IPS.

Out of the box Cascade security analytics classify threats into these broad categories:

- **Suspicious connection** – when two hosts that do not normally communicate with one another start communicating (for example, a maintenance department host connecting to a finance department host)
- **Worm** – a pattern of scanning among hosts, where systems previously scanned suddenly become scanners themselves. Identification of patient zero, infected hosts and means of propagation are reported
- **New host** – a host that has not been previously identified has sent enough traffic to be regarded as having joined the network
- **New service** – a host or an automatic host group is providing or using a service over a new port
- **Host scan** – a series of hosts on the monitored network being interrogated on the same port
- **Port scan** – a host or series of hosts on the monitored network being interrogated across a range of ports
- **Bandwidth surge** – a significant increase in traffic that conforms to the characteristics of a Denial of Service (DoS) or a Distributed Denial of Service (DDoS) attack

BENEFITS

- Identify threats typically missed by traditional perimeter-based solutions
- Identify what is and is not in scope from a regulatory perspective
- Accelerate assessment and remediation of security and compliance issues
- Maintain a forensic trail for incident post-mortem and audits
- Cost-effective to deploy and maintain

Governance, Risk and Compliance (GRC)

PCI, FIPS 200, SB-1386, GLBA, HIPAA... all require a GRC approach, backed with continuous monitoring. Riverbed Cascade provides that continuous monitoring framework, observing communications between all nodes on the network in order to report on compliance with control objectives.

Because credentialed insiders have permission to be on the network and do not need to exploit a vulnerability to compromise assets, simply watching for known patterns of hostile activity is not enough. Cascade provides the information you need to develop, monitor and enforce usage and access policies.

Cascade can monitor for the occurrence or absence of an activity of interest, such as those mentioned in the section above or using user-defined policies. For example, Cascade can identify connections occurring within specified time periods (nights and weekends) or when any connection using a specified port or to a specific IP occurs. This granular level of control helps ensure that developers do not connect to production environments, that access to regulated servers is not made via insecure protocols or more insidiously, that unauthorized personnel do not access personally identifiable information (PII), such as credit card or healthcare information. In addition, Cascade provides an audit trail of traffic between any two systems over a specific time period, allowing you to provide auditors with proof of what did or did not happen.

What's in scope?

"If I knew what the problem was, I could fix it." Security scope definition is not dissimilar. Finding all the systems that are actually necessary to deliver a service is typically much more challenging than securing and auditing the service itself. Servers involved with multiple applications, production systems still living under developers desks, firewalls left with any-any-any rules, branch facilities that house data, and a litany of other items makes defining scope for a regulated service painful. The tighter the rein on what is in scope versus what isn't, the more cost and overhead can be driven out of security programs.

Cascade's automated discovery and dependency mapping capabilities can assist when establishing and reviewing what is and is not in scope. Cascade helps uncover all the moving parts of an application – the hosts, paths, ports, and protocols – that need to be secured or monitored for compliance. It helps identify any gaps in coverage that might have been overlooked and also finds unrelated systems that need to be treated at the same trust level due to proximity.

Incident response, forensics and post-mortem analysis

The sheer volume of alerts and logs has become so overwhelming that when the security operations center (SOC) begins an investigation, they often don't know where to begin. How do they quickly answer these critical questions?

- What was the exact traffic that triggered the alarm?
- Was the target compromised?
- What other systems were affected?
- Was any reconnaissance present?

Whether investigating an incident in real time or post mortem, it is important to have the evidence stored on hand for back-in-time analysis. Long-term recall of full packet data enables InfoSec to reconstruct the event, determine the scope of the damage, and diagnose root cause to more quickly restore the network to normal operations. In this roll, Cascade acts like a surveillance camera, continuously recording, indexing and archiving everything on the network on a 24x7 basis.

Integration with third-party solutions

Cascade supports bi-directional integration with several different layers of network and security infrastructure. Through the sharing of intelligence and control with other products on the network, Cascade enables greater situational awareness, faster threat detection, better understanding the event's impact on the network as well as the business, and more comprehensive incident response and triage. Currently Cascade has documented workflows integrating with security event managers SEMs, routers and switches, vulnerability scanners, IPS, NAC, DNS/DHCP and Active Directory, as well as a robust API for additional use cases. See Figure 1 for a list of supported integrations.

User identification and location

Cascade integrates with numerous infrastructure services in order to resolve an IP address to its user name (active directory), MAC address (DHCP or SNMP to routers), system name (DNS) and physical switch port (SNMP to switches). The ability to resolve IP addresses to readily identifiable information on employees, customers or partners saves an amazing amount of time in the SOC, helping to expedite troubleshooting, and simplifying the enforcement of acceptable usage policies and regulatory mandates.

Routers & Switches		<ul style="list-style-type: none"> Flow collection Switch port integration Interface names
Network Management Systems		<ul style="list-style-type: none"> Export events via SNMP Contextually drill down into evidence
CMDB		<ul style="list-style-type: none"> Export dependency data
Security Event & Log Management		<ul style="list-style-type: none"> Profiler event export Situational awareness
Vulnerability Management		<ul style="list-style-type: none"> Intelligently trigger scans Manually trigger scans
Mitigation		<ul style="list-style-type: none"> Revoke IP leases Turn off switch ports Black hole traffic
Identity Management		<ul style="list-style-type: none"> Match MAC address and user name to IP address

Figure 1: Cascade integrates with the third-party solutions listed above.

Security event managers

Cascade can send security events to SEM solutions, ensuring that operators have "a single pane of glass" from which to prioritize and triage incidents. Cascade exports behavior- and policy-based events to the SEM, providing centralized notification of alarms, as well as supplemental data to enhance event correlation. An API into Cascade's behavioral baseline and system dependencies is also exposed to the SEM, enabling the operator to contextually drill down into Cascade to gain perspective and intelligence about an event in question, and to accelerate remediation.

Vulnerability management

Cascade enables intelligent vulnerability scanning through integration with leading vulnerability management (VM) solutions. Cascade's knowledge of when hosts first appear on the network, or when existing hosts begin to exhibit a change in behavior, can be used to trigger events and signal the VM system to initiate a scan.

Mitigation

Cascade supports mitigation actions using a number of different technologies. It can

- Remove a system from the network by turning off switchport(s), injecting null-routes, and via ACLs on routers, switches and firewalls
- Trigger an intrusion prevention system to quarantine a hostile system
- Prompt a network access control (NAC) systems to revoke the access of a system from the network
- Prompt a DHCP server to revoke an IP lease

Different mitigation enforcement technologies offer different courses of mitigation, including 100 percent removal from network access, quarantine, blocking of access, etc. Cascade presents the various mitigation methods as options in a mitigation plan which provides context and an understanding of the impact particular mitigation action will have, allowing for informed mitigation decisions.

Benefits of Cascade for security

By analyzing network behavior in real time, Cascade identifies changes in application, system and user behavior to provide early warning of security threats and breaches, without relying on signatures. In addition, Cascade can act as a network surveillance camera to store network traffic for extended periods of time, providing the evidence needed to efficiently detect and root out intrusions, malware, and other unauthorized activities within the IT infrastructure. In a world of ever-increasing malware, hackers, and espionage, Cascade complements traditional perimeter-based security solutions to provide complete protection:

- Eliminate network blind spots by detecting threats across the entire network, including inside of virtual machines
- Protect against advanced persistent threats, internal threats and emerging malware, without the need for signatures or blacklists
- Understand network trends to detect unauthorized activities, users, applications or hosts
- Enforce regulatory and IT governance policy and reduce time and cost of audits
- Achieve branch to core coverage by leveraging existing data sources, minimizing the need for expensive hardware deployments
- Quickly identify compromised hosts and rapidly contain the resulting infection
- Provide situational awareness into your workflow, accelerating incident response and minimizing time spent on false or immaterial alarms
- Understand what systems are in-scope and why, regardless of their physical location
- Maintain a forensic audit trail for post incident analysis

About Riverbed

Riverbed delivers performance for the globally connected enterprise. With Riverbed, enterprises can successfully and intelligently implement strategic initiatives such as virtualization, consolidation, cloud computing, and disaster recovery without fear of compromising performance. By giving enterprises the platform they need to understand, optimize and consolidate their IT, Riverbed helps enterprises to build a fast, fluid and dynamic IT architecture that aligns with the business needs of the organization. Additional information about Riverbed (NASDAQ: RVBD) is available at www.riverbed.com.



Riverbed Technology, Inc.
199 Fremont Street
San Francisco, CA 94105
Tel: (415) 247-8800
www.riverbed.com

Riverbed Technology Ltd.
One Thames Valley
Wokingham Road, Level 2
Bracknell. RG42 1NG
United Kingdom
Tel: +44 1344 31 7100

Riverbed Technology Pte. Ltd.
391A Orchard Road #22-06/10
Ngee Ann City Tower A
Singapore 238873
Tel: +65 6508-7400

Riverbed Technology K.K.
Shiba-Koen Plaza Building 9F
3-6-9, Shiba, Minato-ku
Tokyo, Japan 105-0014
Tel: +81 3 5419 1990