riverbed

Solution Brief

Transform Network Data into Cyber Intelligence

Without a doubt, the volume and frequency of cyberattacks have increased in the wake of the COVID-19 pandemic. Cybercriminals are taking advantage of the increase in endpoints and security lapses due to remote work to step up the number of attacks. Phishing attacks are up 667% and other types of attacks are surging as well.[1]

Yet our detection and response efforts have not kept up. According to a recent survey, 53% of attacks successfully infiltrate without detection, and alerts are generated for only 9% of attacks.[2]

Given the lack of detection and prevention, it's not surprising that 90% of security experts are not satisfied with the speed and capabilities they have in detecting incidents.[3] Clearly, a different approach is required—one that detects threats already in the network.

Incident Detection and Response

Riverbed® SteelCentral™ NetProfiler Advanced Security Module transforms network data into cyber intelligence providing essential visibility and forensics for broad incident detection and response in today's hyper-connected digital world.

Using full-fidelity network flow analysis, Riverbed's Advanced Security Module delivers the crucial insights and empirical evidence you need to detect and investigate threats that bypass typical perimeter measures as well as those that originate inside the network.

The value of flow data is well recognized for network use cases, but less so for security. Riverbed offers a wide range of detection capabilities, including:

- **Data exfiltration**: detects when large volumes of data are staged or move out of your network unexpectedly
- **DDoS detection**: quickly identifies a wide range of DDoS attacks and automatically triggers response or black hole routes
- **Blacklisted communications**: alerts you when your system communicates with known malware, viruses, spyware, etc. so you can investigate and take action
- **Security analytics**: examines network traffic to identify threats that generate unusual traffic flows, such as unexpected new services, hosts, or connections
- **Incident forensics**: provides full historical details so you get the complete scope of the attack; drill into the packets for even more details

[1] Baracuda Networks, 2020
[2] FireeyeMandiant, Security Effectiveness 2020
[3] RSA, Threat Detection Effectiveness Survey 2016

Situational Threat Intelligence

Cyber threat intelligence is evidence-based information that identifies emerging threats and helps you mitigate your organization's exposure to them. Riverbed's Advanced Security Module shows you where threats may exist in your environment so you can swiftly respond. It provides two types of threat intelligence, which are automatically updated frequently:

- **Blacklists** detail known malicious or suspicious entities that should not be allowed access to your network. The NetProfiler Security Module correlates blacklisted items to your environment and alerts on positive matches so you can stop the communication. Event detail is available for further research on the threat. At any time, you can add new threats to your backlist as you run across them in your security landscape.

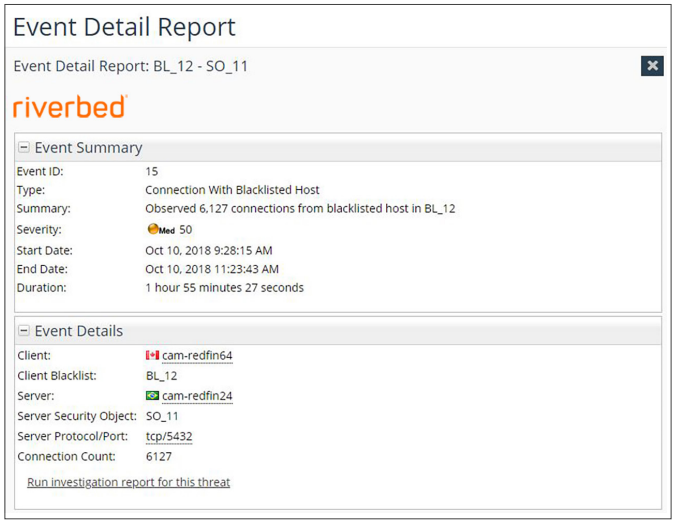

Figure 1

An example of an event detail report showing a connection to a blacklisted host with supporting info and links to investigative reports for the threat.

- **Threat feeds** are analyst-generated information about potential threats that may or may not mean your network has been compromised. Threat feeds can include topics like Shodan activity and cryptocurrency mining that could be legitimate traffic, but might also hide malicious activity. The alert provides you with resources to learn more and the links to investigate the potential vulnerability in your environment.

Figure 2

An example of a threat feed. You can read more about it, or explore your environment for signs Electronum on ports 3333, 5555, or 7777 in the past 1 hour, 1 day, or 1 week.

DDoS Detection and Mitigation

DDoS detection no longer needs to be a dedicated solution, so you need fewer vendors in the NOC/SOC. The Advanced Security Module identifies DDoS attacks fast—in just seconds—and acts immediately and surgically. Redirect traffic to an A10 TPS DDoS scrubber, Verisign cloud scrubbing center, or announce a black hole route so DDoS traffic is dropped while the rest of your network continues to operate normally.

Security Analytics

Worried that threats are slipping through the cracks? Riverbed learns and understands the changing patterns of behavior in your network to combat both insider and external threats. It provides dynamic visibility into the applications and traffic flowing throughout your network.

Out of the box, the security analytics classifies threats into these broad categories:

- **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

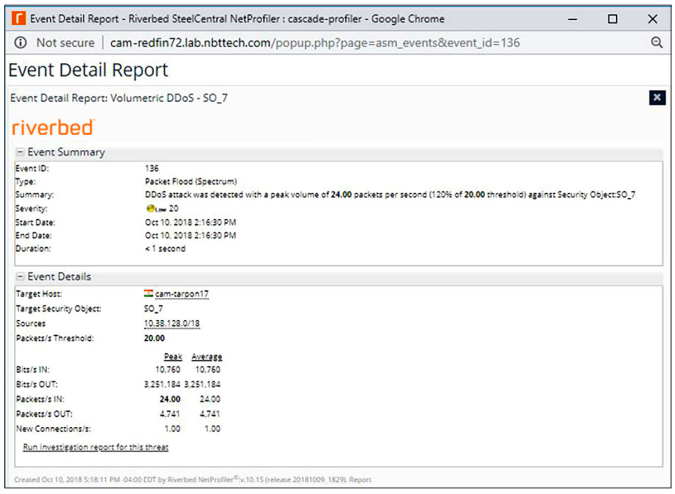

Figure 3
An example of a DDoS alert.

Threat Hunting

Cyber threat hunting starts with the premise that bad actors have already breached your perimeter defenses and are operating inside your network. An analyst starts with a hypothesis about how an attacker might have breached your defenses, and then proactively and iteratively tries to find the evidence to support the hypothesis—the systems compromised and the data accessed, etc. Along the way, the results of the investigation typically cause the analyst to pivot in other more fruitful directions.

Full fidelity flow data is critical for detecting and disrupting active attack activities. It provides both the breadth and depth of visibility you need to gain insight across the entire enterprise—the insight needed for cyber threat hunting.

In addition, the Advanced Security Module provides rich security analytics and threat hunting workflows that improve your ability to uncover hidden and entrenched threats. They let you search the network for evidence and footholds and then pivot on promising leads to ultimately determine how the intruder is controlling compromised assets.

Value Delivered

The Advanced Security Module provides full visibility into the activities of threat actors with real-time and forensic capabilities to ensure even the most evasive attacker has no place to hide.

- **Proactive incident detection and response**. Analyze data from a range of sources across the enterprise, connecting the dots between various events to detect threats or security incidents in real time.
- **Reduce incident losses**. By detecting advanced persistent threats earlier, you limit the damage and the costs due to potential regulatory fines, bad publicity, and the resulting loss of customers that inevitably comes along with a major breach.
- **Improve security forensics**. Provides insights into where an attack originated from, how a compromise happened, what resources were compromised, what data was lost, along with a timeline for the incident.
- **Reduce attack surfaces**. By supplementing your security defense posture with learned lessons, you shore up weaknesses and architectural shortcomings to ensure that similar incidents don't happen in the future.

Professional Services

Your purchase of the Advanced Security Module includes configuration and deployment professional services that will be delivered by Riverbed Professional Services. These professional services are designed to help ensure that the initial configuration of the Advanced Security Module is based on Riverbed's best practices and will deliver the security insights and business value described in this brochure.

These services will include a review of your network architecture, desired security policy, and requirements. Riverbed Professional Services will perform the applicable data analysis and configuration of your Advanced Security Module remotely in conjunction with your designated subject matter experts. They will help you get maximum value out of your solution through expert configuration based on best practice compliance.

Learn More

To learn more about Riverbed's solution for threat detection and response, go to our website here.

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. The platform addresses performance and visibility holistically with best-in-class WAN optimization, 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 riverbed.com.

riverbed