riverbed

SOLUTION BRIEF

Transforms 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]

In fact, 86% of organizations had at least one user connect to a phishing site and 70% had users that were served malicious browser ads.[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]

IBM's Cost of a Data Breach 2021 also validates this. The average time to identify and contain a breach is 280 days: 207 days to identify a breach and 73 day to contain it.

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

Network Detection and Response

Network Detection and Response (NDR) solutions transform network visibility into security intelligence, providing essential analytics and forensics for broad threat detection, investigation and mitigation. By capturing and storing all network packet and flow data in real- or near real-time across your enterprise (both north/south as well as east-west traffic) and leveraging analytics to identify suspicious traffic, it delivers the crucial insights to detect and investigate advanced threats that bypass typical preventative measures, as well as those that originate inside the network.

Unprecedented Visibility

Alluvio NetProfiler Advanced Security Module is network detection and response (NDR). It is an add-on module to Alluvio NetProfiler, leading network traffic monitoring. They both leverage NetProfiler's ability to capture and store all flow data all the time so the data you need is always available for analysis.

1 Cisco, 2021 Cyber Security Threat Trends
2 FireeyeMandiant, Security Effectiveness 2020

NetProfiler Advanced Security Module offers a wide range of detection capabilities, including:

- **Security analytics:** examines network traffic and compared it to historical baseline to identify threats that generate unusual traffic patterns, such as zero-day events, unexpected new services, hosts, or connections
- **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 mitigations or black hole routes
- **Incident forensics:** provides full historical details so you get the complete scope of the attack; drill into the packets for even more details
- **Threat hunting:** Leverage full forensic records to investigate post-compromise

DDoS Detection and Mitigation

DDoS detection no longer needs to be a dedicated solution, so you need fewer vendors in the NOC/SOC. NetProfiler Advanced Security Module accurately identifies all types of DDoS attacks fast—in just 10 to 30 seconds—and acts immediately and surgically. Redirect traffic to an A10 TPS DDoS scrubber or other mitigations so DDoS traffic is dropped while the rest of your network continues to operate normally.

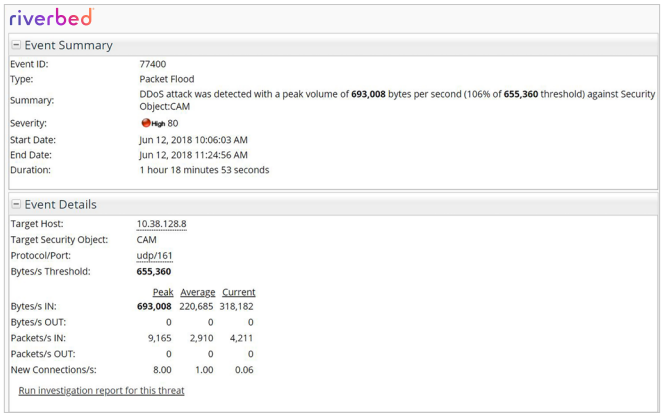

Figure 1: An example of a DDoS alert.

Security Analytics

Worried that threats are slipping through the cracks? NetProfiler Advanced Security Module 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.

Right out of the box, the security analytics classifies 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

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 and packet data are 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. One-click access to packet data also supplements your flow data.

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 that ultimately determine how the intruder is controlling compromised assets.

Professional Services

Your purchase of the NetProfiler Advanced Security Module includes configuration and deployment professional services that Riverbed Professional Services (RPS) will deliver. These services are designed to ensure that the initial configuration of the NetProfiler Advanced Security Module is based on Riverbed's best practices and deliver the security insights and business value described in this brochure. They will include a review of your network architecture, desired security policy, and requirements. RPS will perform the applicable data analysis and configuration of your NetProfiler Advanced Security Module remotely in conjunction with your designated subject matter experts and help ensure you get maximum value out of your NetProfiler Advanced Security Module purchase through expert configuration based on best practice compliance.

Value Delivered

The NetProfiler Advanced Security Module provides full visibility into the activities of threat actors with real-time and forensic capabilities to ensure even the most evasive attackers have no place to hide. As a result, you can reduce your risks, lower your financial exposure, and protect your customer data.

To learn more about Alluvio NetProfiler Advanced Security Module, click here.

riverbed

About Riverbed

Riverbed is the only company with the collective richness of telemetry from network to app to end user, that illuminates and then accelerates every interaction, so organizations can deliver a seamless digital experience and drive enterprise performance. Riverbed offers two industry-leading portfolios: Alluvio by Riverbed, a differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless, secure digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of partners, and market-leading customers globally – including 95% of the FORTUNE 100 –, we empower every click, every digital experience. Riverbed. Empower the Experience. Learn more at riverbed.com.