



Transforming Network Data into Cyber Intelligence for State and Local Agencies

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.

Attacks on state and local governments are rising in frequency. According to cybersecurity firm Recorded Future, in 2019 alone there were 140 ransomware attacks—an average of 3 per day—targeting public, state and local government and healthcare providers. This is up 65% from the previous year.

Yet state and local agency cybersecurity efforts have not kept up. While 60% of government agency respondents describe the maturity level of their organization's cybersecurity program as mature, only 38% of state and local respondents say their agencies have achieved that level of maturity in their cybersecurity initiatives.¹

The stakes are high. According to IBM's [Cost of a Data Breach 2020](#), the average cost of a breach is \$3.86 million. 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 90% of security experts are not satisfied with the speed and capabilities they have in detecting incidents.² 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 agency (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

Riverbed® NetProfiler Advanced Security Module is Riverbed's NDR. It is an add-on module to Riverbed NetProfiler, and captures and stores all flow data, all the time, so the data you need is always available for analysis.

¹ <https://www.ponemon.org>

² RSA, Threat Detection Effectiveness Survey 2016

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

- **Security analytics:** examines network traffic and compares 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
- **Blacklisted communications:** alerts you when your system communicates with known malware, viruses, spyware, etc., so you can investigate and take action
- **Incident forensics:** provides full historical details so you get the complete scope of the attack while allowing you to drill into the packets for even more details
- **Threat hunting:** leverage full forensic records to investigate post-compromise

Threat Intelligence for Situational Awareness

Threat intelligence is evidence-based information that identifies emerging threats and helps you mitigate your agency's exposure to them. NetProfiler Advanced Security Module shows you where threats may exist in your environment so you can swiftly act on them. It provides two types of threat intelligence, which are updated regularly:

- **Blacklists** detail known malicious or suspicious entities that should not be allowed access to your network. The NetProfiler Advanced 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 blacklist as you run across them in your security landscape.

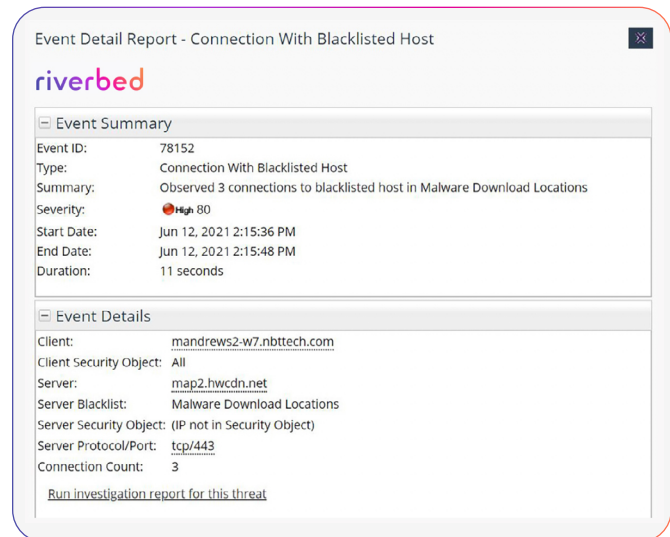


Figure 1. An example of an event detail report showing a connection to a blacklisted host with supporting info and links to investigative reports for the threat.

- **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 Electroneum 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. 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.

Security Analytics

NetProfiler Advanced Security Module ensures that threats don't slip through the cracks. It learns and understands changing patterns of behavior in your network. 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, those state and local agencies that act as MSP for other smaller agencies, there can be many new connections that are suspicious, and should be check out. This is an easy way for threats to get in unnoticed.)
- **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

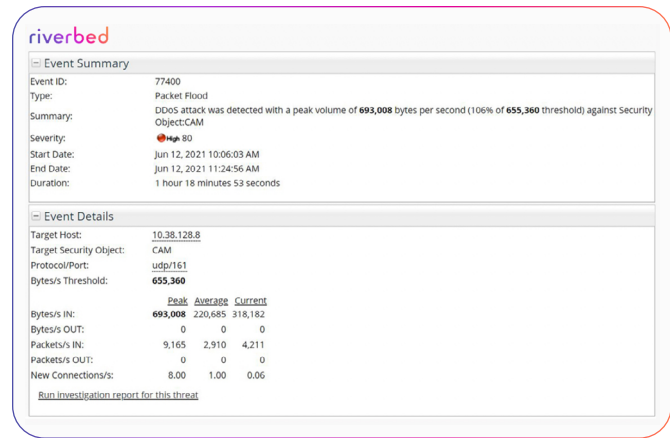


Figure 3. An example of a DDoS alert

- **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.

NetProfiler's 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 agency—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 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 Consultants 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 security insights and organizational value. They will include a review of your network architecture, desired security policy, and requirements.

Riverbed Performance Consultants 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 purchase.

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 citizen data.

To learn more about Riverbed NetProfiler Advanced Security Module, [click here](#).

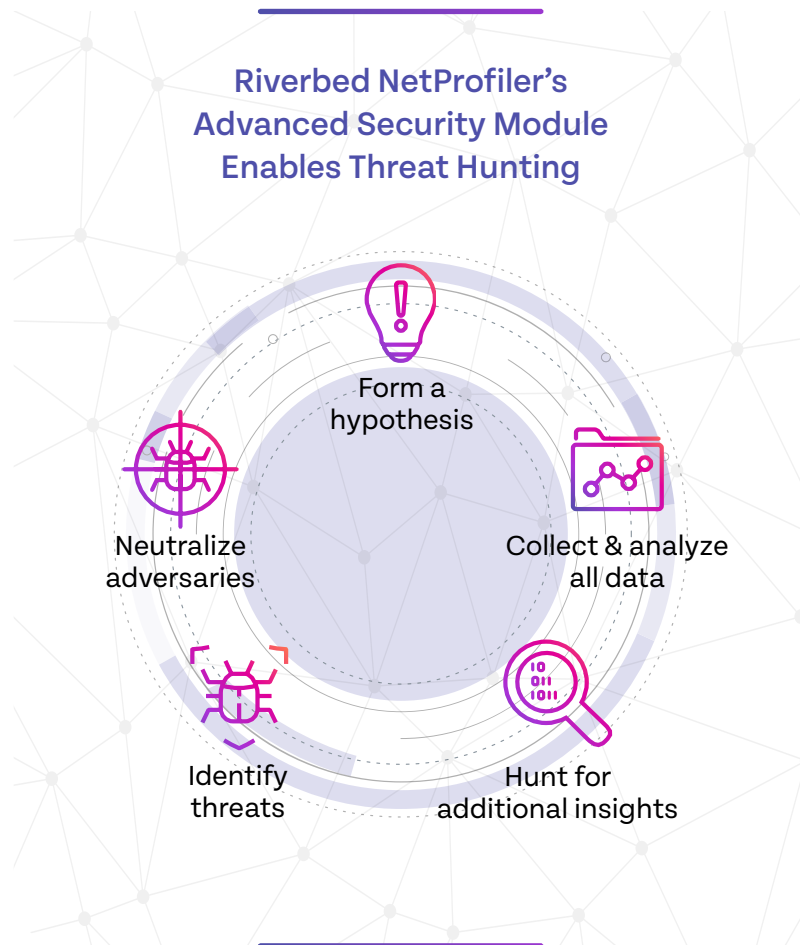


Figure 4. The Threat Hunting Process



Riverbed – Empower the Experience

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 that users get the flawless digital experience they expect across the entire digital ecosystem. Riverbed offers two industry-leading solution areas – Alluvio by Riverbed, an innovative and differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app over any network to users, whether mobile, remote, or on-prem. Together with our thousands of partners, and market-leading customers across the world, we empower every click, every digital experience. Learn more at riverbed.com.