ExtraHop

WHITE PAPER

Selection Guide for Network Visibility Tools

Improve operational efficiencies, reduce costs, and adapt to changing requirements through tool rationalization

With changing requirements and pressure to make the most of their limited budgets, IT leaders have an opportunity to rationalize and modernize their network visibility toolsets. This selection guide outlines the benefits of tool consolidation and evaluation criteria for different network-based use cases, including network performance monitoring and diagnostics (NPMD), intrusion detection (IDS), network forensics, IoT discovery and monitoring, and more.

TABLE OF CONTENTS

The Case for Tool Consolidation in the Time of COVID-19

The past decade has seen robust growth in IT spending, especially for cybersecurity tools. However, as organizations have continued adding tools to their security toolsets, they have seldom removed any. Why? It's definitely easier to add new tools to meet new requirements than it is to retire old ones. The resultant tool sprawl has left many organizations feeling a little bloated, and that is why 68 percent of respondents in the 2020 SANS Network Visibility and Threat Detection report have indicated a desire to reduce the number of tools in use. The proliferation of tools also raises operational concerns and opens potential gaps if the solutions are not properly integrated into security architectures and risk reduction strategies. The right catalyst for IT leaders to ask hard questions about a tool's utility and seek out better solutions has been lacking—until now.

With record unemployment and uncertainty about the timeline for the COVID-19 pandemic, companies are looking for ways to pare back spending. The current economic climate creates an opportunity to make the business case for re-architecting your toolset for greater efficiency and overall effectiveness.

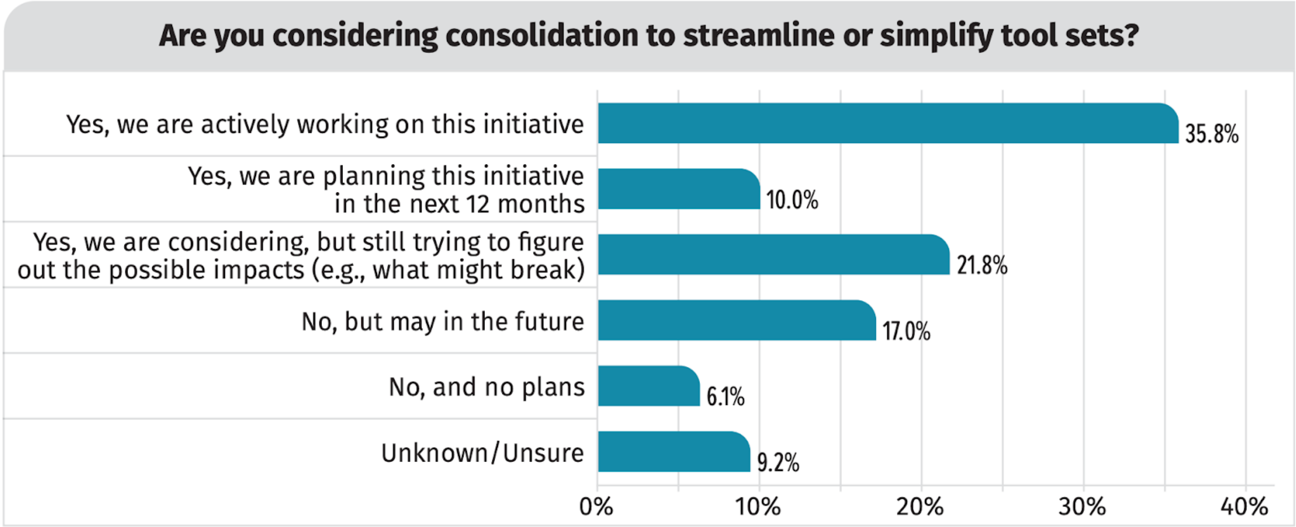


Figure 1. *Most companies use network visibility and threat detection tools from more than 10 vendors, with nearly one-fifth utilizing more than 20 tools, according to a 2020 SANS survey. Read the report: 2020 SANS Network Visibility and Threat Detection Survey*

Building a Business Justification

Use the following points when creating a business justification for your tool consolidation initiative. This process will help you and your organization understand how you can save money by consolidating tools while improving your processes (be more efficient), and your ability to support new requirements (be more effective).

1. Understand Your Current and Future Requirements

Consult with your teams to understand if their current toolsets are adequate to support your new and upcoming initiatives. Focus on outcomes, not features, and use the tool selection criteria later in this guide as a starting point. Remember, this is not about replicating the exact same feature set of a tool that should be retired—it's about how best to achieve the outcome in the most efficient manner. In addition, instead of purchasing new discrete tools for new use cases, look for solutions that can cover a broader set of existing and new use cases. See the section below for example functional criteria for categories such as IDS, network forensics, NPMD, and others.

2. Share Visibility Among Different Teams to Save Money and Reduce Friction

Tool sprawl is both a cause and effect of silos that separate data and teams, resulting in a lack of communication and slower response to issues. For example, both Security and Network Operations teams rely on network and systems data, but see it through different lenses. Siloed teams working with siloed tools degrade the efficiency, morale, and security of any enterprise IT department. Consolidating your toolset around platforms that both teams can effectively use to solve issues will not only help save CapEx and OpEx costs, it will provide teams with the shared visibility that is required for true collaboration.

3. Calculate the Benefit of Rationalization

When working through financial calculus for your organization, weigh the costs and benefits of your current toolset against a new rationalized toolset. Consider the following:

- *How many teams actively use your current set of tools?* The value of any particular tool to your organization is determined by how many people actually utilize the tool. For example, many organizations have expensive network packet capture solutions for security or network teams that are only used by a select few engineers when there is an incident. Certainly, access to network packets for root cause analysis is a legitimate use case, but if it can be accomplished by a solution that is accessible to a variety of teams, then the value to your organization will be greater.

- *Is there overlap in your current toolset?:* If your team is using a particular tool for a single function, that function might already be covered by another tool in your arsenal, creating an opportunity for you to retire that tool. It may also be the case that there is a solution that can handle the use case better and more effieciently, allowing you to decomission the use of several tools in favor of one that will bring greater effiecieny to team practices. At times it can be that a particular engineer has just always used this tool and doesn't want to change. In those cases it's important to encourage retraining along with retooling.

- *What is the benefit to your organization of greater visibility?* The CIS Top 20 Controls cite visibility as the number one security control. Visibility has value for your organization and can be quantified in terms of reduced risk (through faster time to detection and resolution) and improved user experience for your critical applications (through improved monitoring and troubleshooting). Both reduced risk and improved user experience are important business considerations, but can be difficult to quantify. To put a dollar amount on risk reduction, check if your cyber insurance provider offers discounts for implementing improved security controls or tooling. To measure user experience improvement, determine the portion of your business that depends on application delivery and calculate the impact of downtime or latency on revenue.

- *What are the CapEx and OpEx costs?* Capital expenditures are easier to measure as they include hardware and software license costs. Ask your teams when your existing solutions will require a hardware refresh. If the appliances supporting your current platform will reach end-of-life within the next couple years, that strengthens the case for consolidation. Operational costs are less obvious. To calculate OpEx, you will need to understand how many full-time engineers (FTEs) are required to maintain the platform. and how much rack space the solution occupies (with the cooling and power costs that entails).

Did You Know?

Organizations that have achieved NetSecOps convergence see significantly higher rates of operational success, according to EMA Research in their 2020 Network Management Megatrends report.

Functional Criteria by Category

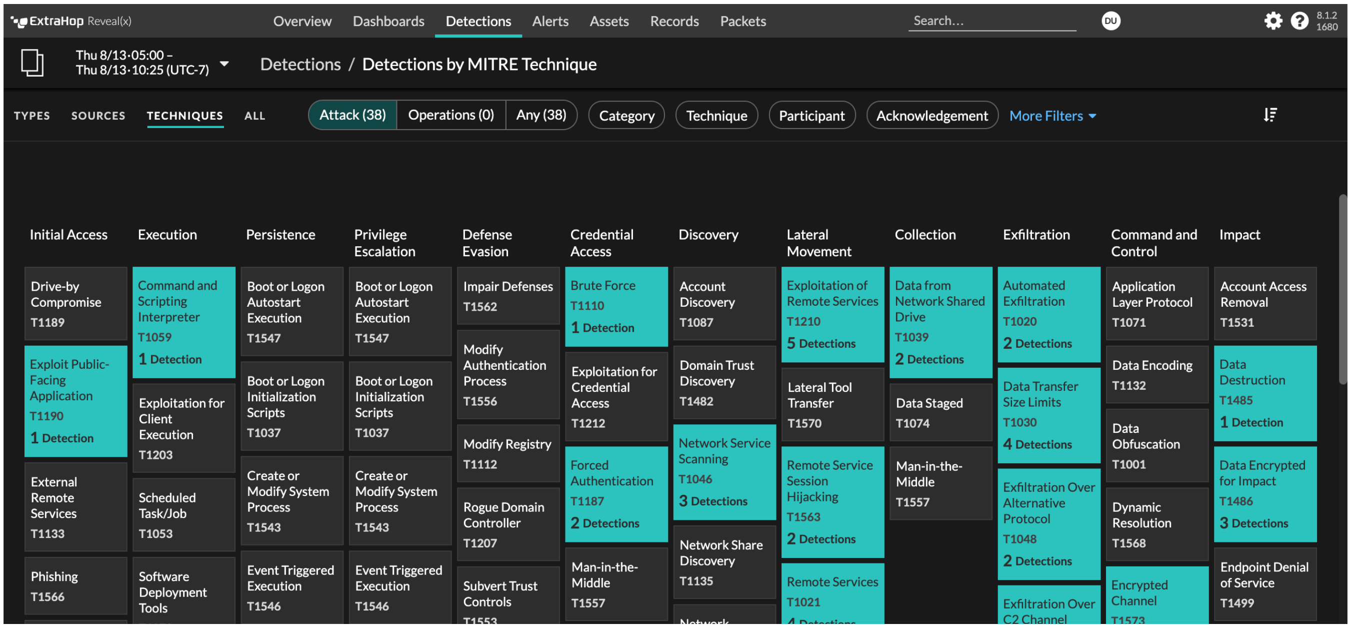
Over time, IT and Security organizations acquire a number of tools to fulfill specific functions. When looking to rationalize your toolset, consider the functional requirements of each tool—what capabilities your teams actually rely on. Your goal is to discover tools that can responsibly incorporate the functional requirements of multiple categories.

Intrusion Detection System (IDS)

An IDS helps the Security team detect attacks on the network and is typically deployed for north-south (ingress-egress) traffic at the perimeter. IDS is well-known technology with open-source efforts contributing rules and signatures (Snort, Suricata, and Zeek are examples) to detect known threats. If your organization has threat researchers, they may also develop custom signatures or rules for the IDS to detect new threats identified through industry threat intelligence sharing or successful penetration tests. Next-generation firewalls (NGFWs) incorporate IDS functionality, but many organizations do not turn it on because it can cause the performance of the appliance to degrade by up to 70 percent.

Example functional criteria for IDS:

- □ Detects known attacks at the network perimeter
- □ Supports open-source rules and signatures
- □ Integrates with SIEM for event correlation
- □ Allows for the creation of custom signatures for unique tactics, techniques and procedures (TTPs)
- □ Provides detection coverage for network-based techniques in the MITRE ATT&CK framework
- □ Support for AWS/Azure/GCP environments



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise T1189	Command and Scripting Interpreter T1059 1 Detection	Boot or Logon Autostart Execution T1547	Boot or Logon Autostart Execution T1547	Impair Defenses T1562	Brute Force T1110 1 Detection	Account Discovery T1087	Exploitation of Remote Services T1210 5 Detections	Data from Network Shared Drive T1039 2 Detections	Automated Exfiltration T1020 2 Detections	Application Layer Protocol T1071	Account Access Removal T1531
Exploit Public-Facing Application T1190 1 Detection	Exploitation for Client Execution T1203	Boot or Logon Initialization Scripts T1037	Boot or Logon Initialization Scripts T1037	Modify Authentication Process T1556	Exploitation for Credential Access T1212	Domain Trust Discovery T1482	Lateral Tool Transfer T1570	Data Staged T1074	Data Transfer Size Limits T1030 4 Detections	Data Encoding T1132	Data Destruction T1485 1 Detection
External Remote Services T1133	Scheduled Task/Job T1053	Create or Modify System Process T1543	Create or Modify System Process T1543	Modify Registry T1112	Forced Authentication T1187 2 Detections	Network Service Scanning T1046 3 Detections	Remote Service Session Hijacking T1563 2 Detections	Man-in-the-Middle T1557	Exfiltration Over Alternative Protocol T1048 2 Detections	Data Obfuscation T1001	Data Encrypted for Impact T1486 3 Detections
Phishing T1566	Software Deployment Tools	Event Triggered Execution T1546	Event Triggered Execution T1546	Rogue Domain Controller T1207	Man-in-the-Middle T1557	Network Share Discovery T1135	Remote Services T1021 4 Detections		Exfiltration Over C2 Channel	Dynamic Resolution T1568	Endpoint Denial of Service T1499
				Subvert Trust Controls T1553		Network				Encrypted Channel T1573	

Figure 2. Many organizations use the MITRE ATT&CK framework as a way of ensuring their ability to detect tactics and techniques across the lifecycle of an attack.

IoT Discovery and Monitoring

In response to the growing number of unmanaged Internet of Things (IoT) devices—smart TVs, VoIP phones, IP cameras, printers, access points, and others—a number of vendors have emerged to provide IoT discovery and monitoring solutions. These passive, network-based products automatically discover and identify IoT devices based on self-advertised data or by matching their communications with a fingerprint. This provides Security teams with visibility into potential vectors of attack that an attacker can exploit.

Purchasing a standalone IoT discovery and monitoring product contributes to tool sprawl, especially if you already have device discovery and inventory in place that is unable to account for IoT devices. Instead, budget owners should consider how other tools can incorporate the functional requirements for IoT discovery and monitoring.

Example functional criteria for IoT discovery and monitoring:

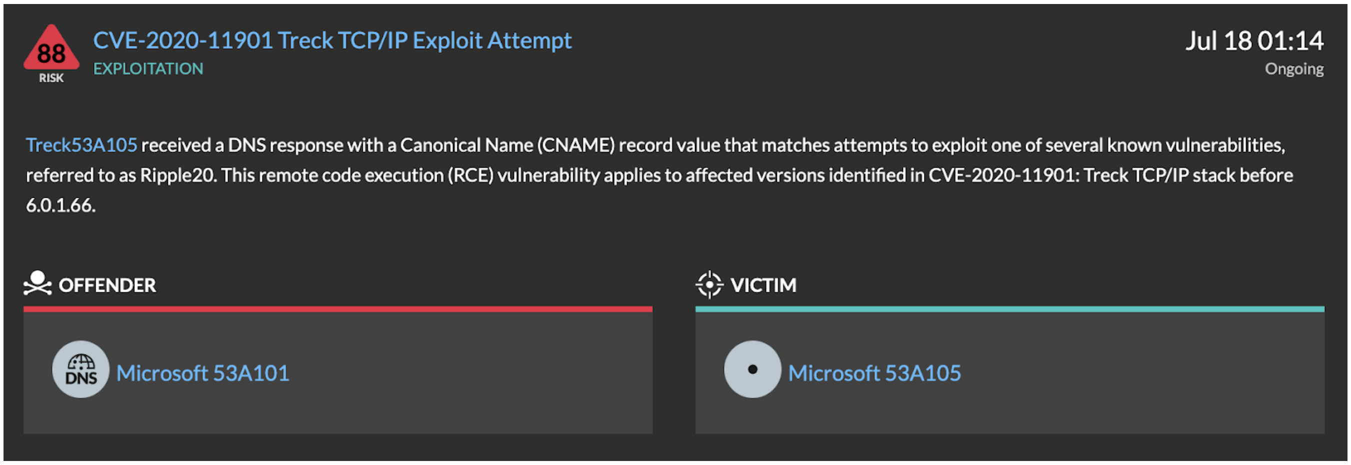
□ Identify device details such as manufacturer and model

□ Deploy passively (no active polling or agents)

□ Detect malicious behavior such as data exfiltration

□ Integrate with a configuration management database (CMDB)

□ Integrate with SIEM or SOAR to provide device context during investigations



88 RISK

CVE-2020-11901 Treck TCP/IP Exploit Attempt

EXPLOITATION

Jul 18 01:14

Ongoing

Treck53A105 received a DNS response with a Canonical Name (CNAME) record value that matches attempts to exploit one of several known vulnerabilities, referred to as Ripple20. This remote code execution (RCE) vulnerability applies to affected versions identified in CVE-2020-11901: Treck TCP/IP stack before 6.0.1.66.

OFFENDER

Microsoft 53A101

VICTIM

Microsoft 53A105

Figure 3. The Ripple20 set of vulnerabilities announced in June 2020 affect hundreds of millions of embedded systems and represent a security risk that will likely last for many years. ExtraHop Reveal(x) automatically and passively discovers devices using the vulnerable Treck software and detects some of the most critical Ripple20 exploit attempts.

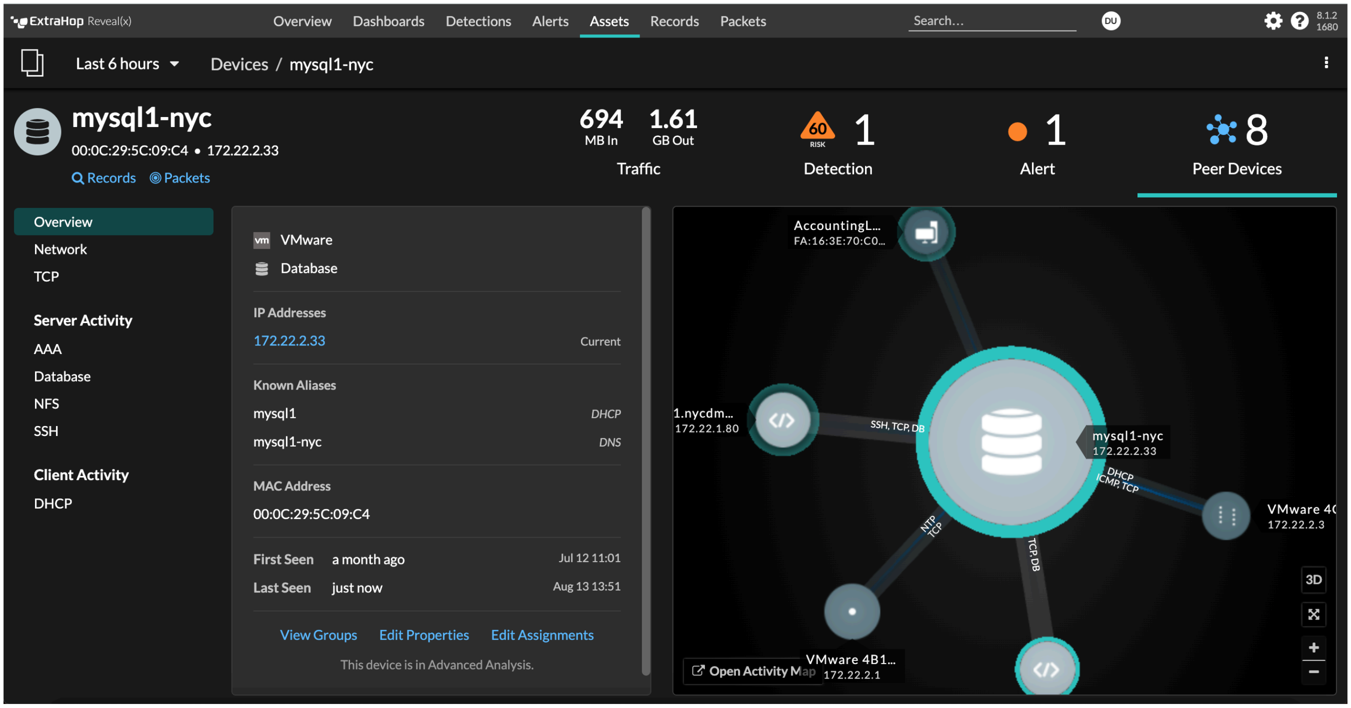
Network Detection and Response

NDR deploys passively on the network to detect threats. The focus of NDR is on the use of machine learning to detect malicious behavior at various stages of the attack lifecycle (command and control, reconnaissance, exploitation, lateral movement, data staging, etc.). In addition, NDR provides Security teams with investigative capabilities when responding to incidents or identifying risk in the environment.

NDR provides key advantages over IDS including: 1) coverage for attack behavior in east-west (lateral) traffic within the perimeter, 2) use of machine learning in addition to rules and signatures, and 3) record and packet investigation to facilitate incident response and threat hunting. Commercial NDR solutions also require far fewer staff resources to maintain than open-source IDS.

Example functional criteria for NDR:

- □ Detect both known and unknown attacks
- □ Support threat hunting through ad hoc search and query
- □ Support identification of cyber hygiene risk
- □ Integrate with SIEM for event correlation
- □ Integrate with EDR, NGFW, ticketing systems, and SOAR for orchestrated response
- □ Allow for the creation of custom rules for unique TTPs
- □ Provide detection coverage for network-based techniques in the MITRE ATT&CK framework
- □ Has advanced capability to decrypt packets
- □ Support for AWS/Azure/GCP environments
- □ Passive monitoring of north-south and east-west traffic
- □ Provide insights for IT, Security, Application, and Cloud teams



mysql1-nyc
00:0C:29:5C:09:C4 • 172.22.2.33

694 MB In
1.61 GB Out
60 RISK 1 Detection
1 Alert
8 Peer Devices

VMware
Database

IP Addresses
172.22.2.33 Current

Known Aliases
mysql1 DHCP
mysql1-nyc DNS

MAC Address
00:0C:29:5C:09:C4

First Seen a month ago Jul 12 11:01
Last Seen just now Aug 13 13:51

This device is in Advanced Analysis.

Figure 4. NDR solutions provide SOC analysts with the information they need to quickly validate alerts and investigate incidents. ExtraHop Reveal(x) is a leading cloud-native NDR solution that provides holistic coverage for on-premises and cloud environments.

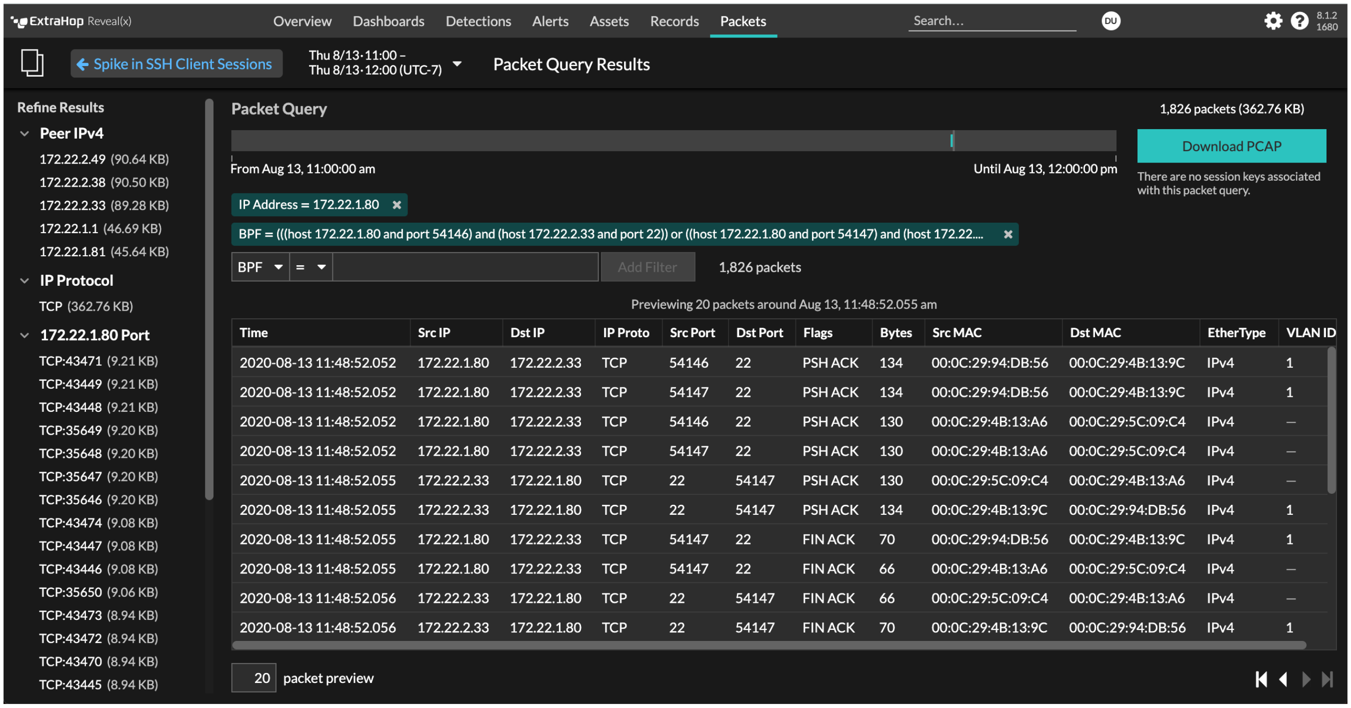
Network Forensics

Network forensics tools continuously capture packets on a network—typically for one day or up to several days, depending on the storage allocated and the traffic volume. Security teams use these solutions to gain access to authoritative packet data during investigations, allowing them to analyze attack methods (files and executables) and create threat intelligence indicators using network artifacts. They also use this packet data for root cause analysis, tying an incident back to the original compromise. Some organizations must retain captured packets for a certain period of time in order to comply with organizational or industry requirements.

Traditional network forensics tools are waning in usage due to the high level of expertise required to use them, growing network traffic volumes, and the increasing amount of encrypted internal traffic.

Example functional criteria for network forensics:

- □ Store packets for analysis for a period of time (depending on your needs)
- □ Index packets to make them searchable
- □ System should execute complex queries in a timely fashion
- □ Ability to decrypt packets
- □ Support for AWS/Azure/GCP environments



Thu 8/13·11:00 –
Thu 8/13·12:00 (UTC-7)

Packet Query Results

Refine Results

Peer IPv4
172.22.2.49 (90.64 KB)
172.22.2.38 (90.50 KB)
172.22.2.33 (89.28 KB)
172.22.1.1 (46.69 KB)
172.22.1.81 (45.64 KB)

IP Protocol
TCP (362.76 KB)

172.22.1.80 Port
TCP:43471 (9.21 KB)
TCP:43449 (9.21 KB)
TCP:43448 (9.21 KB)
TCP:35649 (9.20 KB)
TCP:35648 (9.20 KB)
TCP:35647 (9.20 KB)
TCP:35646 (9.20 KB)
TCP:43474 (9.08 KB)
TCP:43447 (9.08 KB)
TCP:43446 (9.08 KB)
TCP:35650 (9.06 KB)
TCP:43473 (8.94 KB)
TCP:43472 (8.94 KB)
TCP:43470 (8.94 KB)
TCP:43445 (8.94 KB)

Packet Query

1,826 packets (362.76 KB)

From Aug 13, 11:00:00 am
Until Aug 13, 12:00:00 pm

There are no session keys associated with this packet query.

IP Address = 172.22.1.80 ✖

BPF = (((host 172.22.1.80 and port 54146) and (host 172.22.2.33 and port 22)) or ((host 172.22.1.80 and port 54147) and (host 172.22.... ✖

BPF =

1,826 packets

Previewing 20 packets around Aug 13, 11:48:52.055 am

Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags	Bytes	Src MAC	Dst MAC	EtherType	VLAN ID
2020-08-13 11:48:52.052	172.22.1.80	172.22.2.33	TCP	54146	22	PSH ACK	134	00:0C:29:94:DB:56	00:0C:29:4B:13:9C	IPv4	1
2020-08-13 11:48:52.052	172.22.1.80	172.22.2.33	TCP	54147	22	PSH ACK	134	00:0C:29:94:DB:56	00:0C:29:4B:13:9C	IPv4	1
2020-08-13 11:48:52.052	172.22.1.80	172.22.2.33	TCP	54146	22	PSH ACK	130	00:0C:29:4B:13:A6	00:0C:29:5C:09:C4	IPv4	–
2020-08-13 11:48:52.052	172.22.1.80	172.22.2.33	TCP	54147	22	PSH ACK	130	00:0C:29:4B:13:A6	00:0C:29:5C:09:C4	IPv4	–
2020-08-13 11:48:52.055	172.22.2.33	172.22.1.80	TCP	22	54147	PSH ACK	130	00:0C:29:5C:09:C4	00:0C:29:4B:13:A6	IPv4	–
2020-08-13 11:48:52.055	172.22.2.33	172.22.1.80	TCP	22	54147	PSH ACK	134	00:0C:29:4B:13:9C	00:0C:29:94:DB:56	IPv4	1
2020-08-13 11:48:52.055	172.22.1.80	172.22.2.33	TCP	54147	22	FIN ACK	70	00:0C:29:94:DB:56	00:0C:29:4B:13:9C	IPv4	1
2020-08-13 11:48:52.055	172.22.1.80	172.22.2.33	TCP	54147	22	FIN ACK	66	00:0C:29:4B:13:A6	00:0C:29:5C:09:C4	IPv4	–
2020-08-13 11:48:52.056	172.22.2.33	172.22.1.80	TCP	22	54147	FIN ACK	66	00:0C:29:5C:09:C4	00:0C:29:4B:13:A6	IPv4	–
2020-08-13 11:48:52.056	172.22.2.33	172.22.1.80	TCP	22	54147	FIN ACK	70	00:0C:29:4B:13:9C	00:0C:29:94:DB:56	IPv4	1

20 packet preview

Figure 5. Network packets are authoritative data during investigations and can help analyst teams quickly determine root cause. Reveal(x) enables rapid drill-downs into forensic packet details.

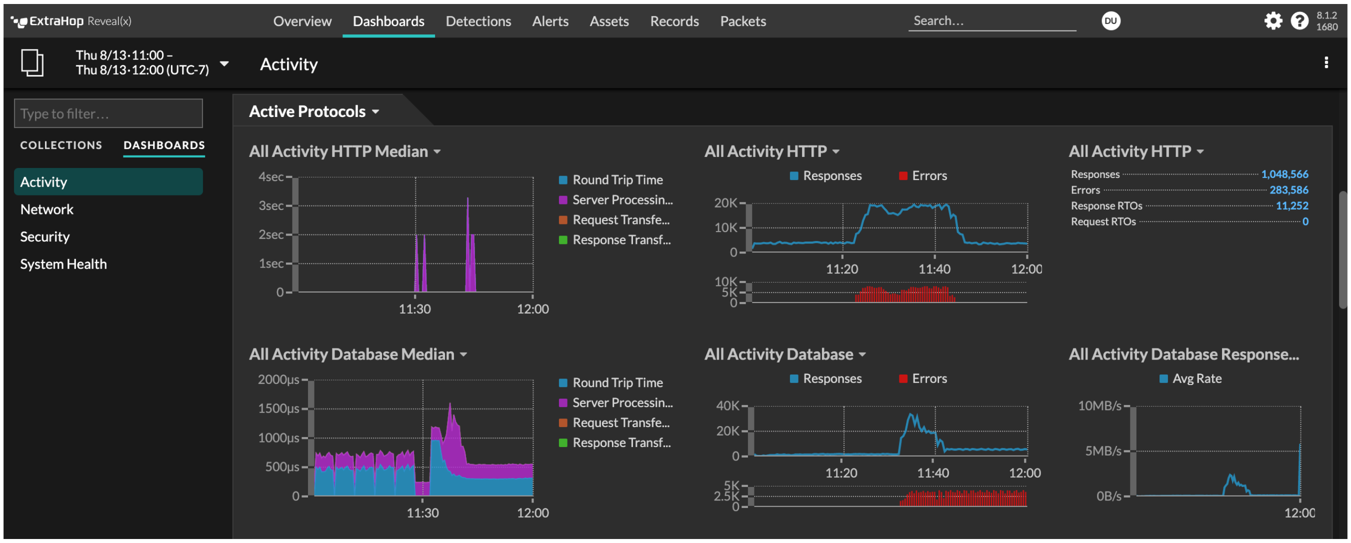
Network Performance Monitoring and Diagnostics (NPMD)

"It's the network" is a common refrain in IT, one that emphasizes the importance of the network in delivering applications. NPMD tools enable network engineers to identify and troubleshoot network performance problems that affect user experience. Even if the problem is not with the network infrastructure, NPMD tools can help IT teams identify where the bottleneck is in the application delivery chain.

NPMD tools deploy passively, analyzing a copy of the network traffic from a port mirror or network tap. Growing traffic volumes and increasing encryption on the network can pose a challenge to legacy NPMD deployments.

Example functional criteria for NPMD:

- □ Show how bandwidth is used by applications and users
- □ Identify network issues caused by infrastructure or misconfigurations
- □ Provide IT teams with performance insights for dependencies (DNS, authentication, databases)
- □ Ability to decrypt packets
- □ Support for AWS/Azure/GCP environments



Responses	1,048,566
Errors	283,586
Response RTOs	11,252
Request RTOs	0

Figure 6. Network operations teams need to be able to correlate activity across tiers to determine the root cause of slow application and network performance. Reveal(x) automatically correlates L2-L7 metrics across web, database, DNS, LDAP, storage, and more.

Adding Cloud to Your Calculation

Unless you are a business that was born within the last five years, it's likely that you still have critical data and applications that run on-premises, and have tooling to manage the security and performance of those assets. As you expand your cloud deployments, the question becomes how to expand your IT and Security teams' visibility before, during, and after cloud migration?

One option is to acquire a distinct set of tooling for your cloud workloads. This could be either the native tooling from a cloud service provider (such as AWS Guard Duty or Azure Advanced Threat Protection) or a cloud-focused service from a third-party. However, this siloed approach will exacerbate tool bloat in your organization and require your teams to manually correlate what they're seeing in on-premises and cloud environments (and won't help as you transition to the cloud). The other option is to re-architect your visibility to cover your hybrid environment, spanning your on-premises workloads as well as your workloads running in AWS, Azure, and GCP.

To reflect the reality of a hybrid environment, we've added "Support for AWS/Azure/GCP environments" to the functional requirements listed above.

Conclusion

Given that no one knows how the COVID-19 pandemic will play out, it is prudent to expect an economic downturn due to high unemployment and dampened consumer spending. This will put pressure on IT and cybersecurity budgets, even though companies need those functions more than ever to survive through accelerated digital transformation efforts.

IT leaders can optimize their budgets and support new requirements by rationalizing their existing IT and cybersecurity toolsets, especially when consolidating on platforms that address multiple use cases and can be shared among multiple teams. Many enterprise IT organizations have seen success replacing multiple legacy platforms with ExtraHop Reveal(x). We have active, passionate reference customers that can provide references of tool rationalization. To find out more about how Reveal(x) can provide value to multiple teams in your organization, please contact your local sales representative.

ABOUT EXTRAHOP
ExtraHop is the first place IT turns for insights that transform and secure the digital enterprise. By applying real-time analytics and machine learning to all digital interactions on the network, ExtraHop delivers definitive insights and instant answers that help IT improve security, performance, and the digital experience.

ExtraHop Networks, Inc.
520 Pike Street, Suite 1600
Seattle, WA 98101 USA

http://www.extrahop.com/
info@extrahop.com
T 877-333-9872
F 206-274-6393