IDC TECHNOLOGY SPOTLIGHT

Sponsored by: ExtraHop

Cybersecurity point products are cleverly designed. However, tools that have visibility over an enterprise's entire network surface gain and correlate insights that a slew of discrete tools cannot.

How Network Intelligence Tools Find an Adversary and Defend Against Advanced Threats

July 2021

Written by: Christopher Kissel, Research Director, Security and Trust Products, and Michelle Abraham, Research Director, Security and Trust Products

AT A GLANCE

KEY STATS

In 2020, network intelligence tools (also known as network detection and response tools) were a nearly $1 billion industry, and IDC anticipates these tools will realize an 18% compound annual growth rate from 2020 to 2024.

KEY TAKEAWAYS

The following maxim remains true: "You cannot protect what you cannot see." Organizations require tools that provide real-time visibility into public cloud environments as well as sessions in the Open Systems Interconnection (OSI) Layer 2–7 stack.

Introduction

Many enterprises and their employees proved themselves resilient to the disruption of COVID-19 in 2020 and are hoping to move to a new normal in 2021.

Nonetheless, COVID-19 put many companies in scramble mode, which had negative impacts on the security posture of even the most resilient and flexible enterprises. The impacts of advanced threats such as supply chain attacks and ransomware are affecting organizations around the world as we emerge from the pandemic. On-premises security operations centers (SOCs) had to adapt. As organizations were adapting tools and processes to accommodate the "branch office of one," the shortcomings of conventional cybersecurity approaches were exposed, and the following issues needed to be accounted for:

- Solutions often lacked visibility into the entire attack surface, and encrypted traffic obscured the view.
- COVID-19 accelerated digital transformation (DX) and mobilized a work-from-anywhere workforce.
- Even before COVID-19, the network attack surface was expanding as enterprises migrated processes to the public cloud.
- Overlap in products led to tool sprawl and conflicting agents. Roughly 73% of all organizations use one endpoint security vendor, but the other 27% use two or more vendors.
- Enterprises had to contend (and still do) with vendor lock-in.
- Point products generated alerts but did not necessarily point to a ground truth.

- Adversaries played a multidimensional game — visibility was required all the way through the Open Systems Interconnection (OSI) Layer 2–7 stack, but most often such visibility is not available.
- Understanding and mitigating against advanced threats and threat actors became more difficult as the attack surface expanded.

The complex nature of enterprise hybrid and multicloud environments has made it challenging to create generalized tools for monitoring and security. This subsequently led to the proliferation of "point solutions" — security tools that address a narrow range of threats. The broad range and rapid evolution of attacker tactics, techniques, and procedures created a perceived need for many of these point solutions, with a separate solution for each attack vector. Identity security, email security, firewalls, honeypots, endpoint agents, and more are simultaneously helping businesses solve a range of security problems and crushing security teams under administrative overhead and sheer context-switching costs. While there will never be one tool to rule them all, tool sprawl has become unsustainable, and a more broad-reaching and generalizable solution for threat detection and response is desperately needed. The common denominator across every attack campaign, and nearly every attacker behavior, is the network. No attack can succeed without communicating on the network. Tools exist for monitoring network sessions, connections, users, and protocols to find indicators of malware and the spread of malware if that is the case. IDC calls these tools network intelligence tools (also referred to as network detection and response [NDR] tools).

Network intelligence solutions have visibility over ingress/egress points in the network and in infrastructure-as-a-service (IaaS) environments. The tools embed threat intelligence, user behavioral analytics (UBA), and multiple points of telemetry to refine alerts and discover the ground truth of cybersecurity incidents to help protect against advanced threats. Other reasons to consider cloud-based network intelligence tools are as follows:

- Cybersecurity solutions are moving to software as a service (SaaS) to improve scalability and offer pricing based on actual usage instead of traditional software licenses and capacity-based tools, which are less flexible.
- Network intelligence tools may supplant overlapping and obsolescent tools, such as intrusion detection systems/ intrusion prevention systems (IDS/IPS), with the integration of features such as UBA that can add to the data points to be analyzed for threats.
- Real-time network visibility from anywhere in the world can help bridge the IT, operations, and security gap with shared data from the public cloud, multicloud, and on-premises equipment.
- Enterprises can use the MITRE ATT&CK framework, with network data as the foundation of visibility, to create a ubiquitous framework across an organization to train analysts and mitigate threats.
- Extensibility is greater with agentless solutions that are easy to scale without increasing management burden.
- Cloud-native tools monitor hybrid and multicloud footprints in their entirety to investigate and respond to threats.

The Rise of Network Intelligence Tools

New network intelligence tools are bringing detection, investigation, and response together into one tool compared with legacy tools, which only offered alerts. Network intelligence platforms ingest network data, flows, and data points to look for indicators of compromise and consolidate the alerts into incidents that can be analyzed, prioritized, and countered more precisely. This approach provides contextual awareness to SOC analysts regarding where the threat actor has been and what damage was done.

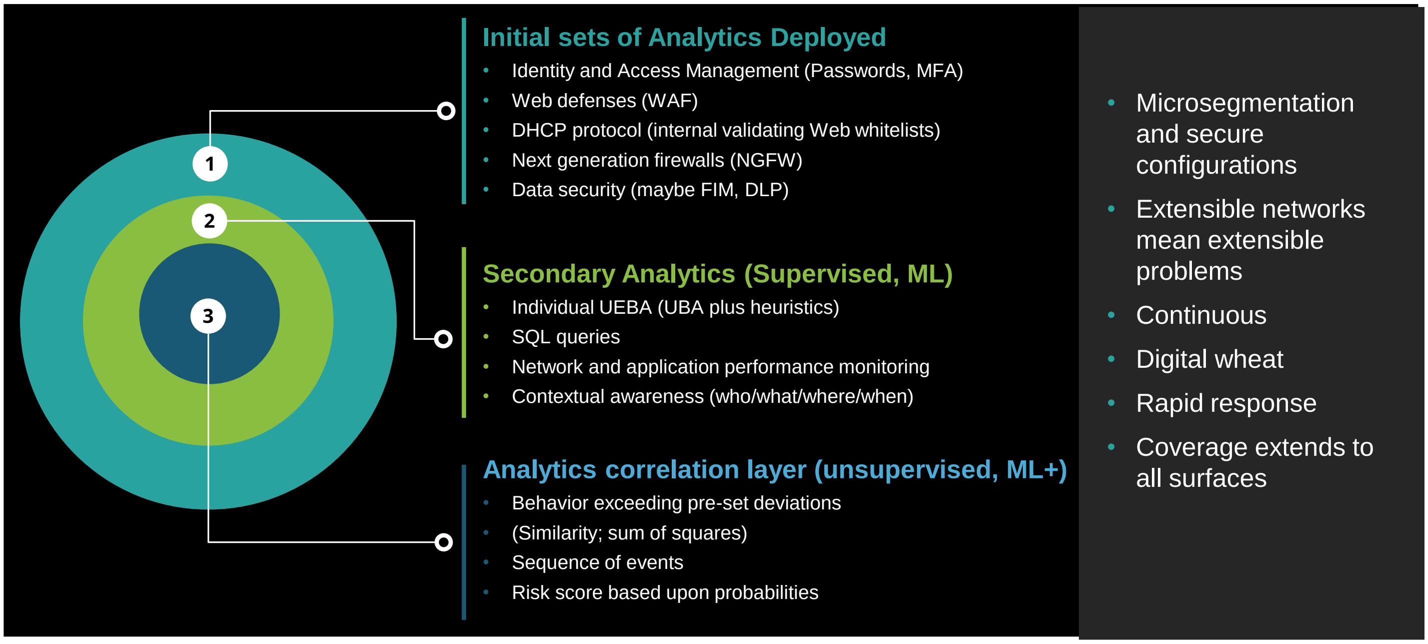
Legacy tools were also unable to detect attacks in encrypted traffic. Today, network intelligence solutions can extract metadata from packets at OSI Layers 2–7, providing deeper visibility and richer context than legacy network security tools. The metadata collected can be user-based anomalies, heuristics, network performance baselines, malware signatures, and deviations from statistical baselines.

Data from the network is broader than that of other solutions and can cover all the devices in an environment, including Internet of Things/operational technology (IoT/OT) devices incapable of running agents or regularly generating logs. Network intelligence tools are passive observers of the entire network, making the entire attack surface visible and providing security without imposing friction on the development or application teams. By running in the cloud, the systems can work across on-premises, hybrid, and multicloud environments.

Network traffic observations are a source of ground truth because threat actors are unable to modify the data or turn it off. This sets network data apart from log and endpoint data, which is vulnerable to tampering, evasion, and deletion by savvy threat actors. Behavior-based detection reduces the false positive alerts generated by signature-based intrusion detection. Benchmarks for performance can help security analysts understand if there is configuration drift.

Figure 1 shows the suggested layering of cybersecurity tools and the space where each tool operates. The first layer of defense is legacy signature-based systems monitoring ingress/egress and looking for obvious visible indicators of compromise. Microsegmentations and secure configurations are part of this layer. The second layer adds more analytics such as UBA, artificial intelligence/machine learning (AI/ML) algorithms to look at entropy and statistical anomaly, statistical baselines, and normality and abnormality. The third layer uses unsupervised learning to reduce alerts and chain events together while looking for the root cause in full packet data. Security incidents can be prioritized so analysts investigate the most important incidents first.

FIGURE 1: ***Analytics Technologies and a Single Version of Truth***



Initial sets of Analytics Deployed

- Identity and Access Management (Passwords, MFA)
- Web defenses (WAF)
- DHCP protocol (internal validating Web whitelists)
- Next generation firewalls (NGFW)
- Data security (maybe FIM, DLP)

Secondary Analytics (Supervised, ML)

- Individual UEBA (UBA plus heuristics)
- SQL queries
- Network and application performance monitoring
- Contextual awareness (who/what/where/when)

Analytics correlation layer (unsupervised, ML+)

- Behavior exceeding pre-set deviations
- (Similarity; sum of squares)
- Sequence of events
- Risk score based upon probabilities

- Microsegmentation and secure configurations
- Extensible networks mean extensible problems
- Continuous
- Digital wheat
- Rapid response
- Coverage extends to all surfaces

Source: ExtraHop, 2021

Threat detection monitoring may identify remote control of an internal host, command and control activity, internal reconnaissance of network systems and resources, brute-force password attempts, correlation of data collection and exfiltration, and encryption of network share drives. Dashboards, workflows, and drilldowns are provided to replicate the MITRE ATT&CK framework, mapping the phases of an attack to help the SOC analyst determine the attack flow. Platforms may respond automatically to threats detected with the appropriate action based on rules set in the platform.

Network intelligence solutions add telemetry from the network side for threat hunting while bringing in external threat intelligence to anticipate and not just react to attacks. These solutions complement endpoint detection and response (EDR) and security information and event management (SIEM) solutions by enriching the data with that of the network to provide a 360-degree view of an enterprise and where to act.

Cybersecurity

Cybersecurity is a discipline that encompasses everything from BiOS, secure log-ins, and configurations to threat monitoring and the repair and remediation of vulnerabilities (optimally before an adversary actively creates a breach). The problem, though, is the network is no longer tucked behind a stateful firewall; it includes IoT, batch data and, increasingly, mobile devices with 5G technology waiting in the wings.

The network comprises four elements. The client or host is a given machine or device that sends or receives data. Servers have multiple functions, but they ultimately host applications. Applications are programs designed for end users to use. The network is the sum of the events on clients, servers, and applications as well as the fabric that connects them. The one long card that network administrators and cybersecurity professionals have is that the truth is in the packets — "packets don't lie."

Finding vulnerabilities based on information coming from the network sounds easy, but it is challenging for the following reasons:

- **Despite the best intentions, cybersecurity is a reactive game.** Companies invest a lot of money and talent in tools, securing configurations, and microsegmenting the network. Unfortunately, new business use cases, clients, servers, and applications are constantly added and taken away, creating a shape-shifting attack surface that can make security monitoring difficult.
- **Unfortunately, there are ghosts in the machine.** Cybersecurity tools have two specific problems. The first problem is excessive alerting. Some tools alert too much, or spew false positives, which analysts learn to ignore. In other scenarios, poorly integrated tools lead to a situation where analysts investigate the same incident from a policy engine/firewall, an endpoint, or a SIEM system before understanding that they are looking at the same event from different perspectives. The second big challenge is that the network is constantly changing. Operating system and software upgrades can trigger alerts based on old settings. Essentially, old whitelisted behaviors and associations must be cataloged.
- **Full packets contain the whole truth** but are difficult to decipher without context.

IDC defines network intelligence and threat analytics as the combination of network performance monitoring and intelligence, deception, and forensics-based analytics. This definition encompasses more than network detection and response to include all the ways the network is used for detection.

Considering ExtraHop

ExtraHop is an NDR vendor with a special emphasis on deep L7 analysis, forensics, and investigation with 90-day lookback. The ExtraHop Reveal(x) 360 SaaS-based NDR platform performs out-of-band analysis on L2–L7 traffic to monitor all communications on the network and provide unified visibility into both north-south and east-west traffic across on-premises, cloud, and hybrid networks. Reveal(x) 360 uses cloud-based machine learning to understand baseline behavior and detect any unusual activity inside the hybrid network. Reveal(x) 360 detections are provided with context and correlation with other activity for a full view of the attack timeline and recommendations for response.

The underpinning of ExtraHop Reveal(x) 360 is the strong AI/ML-based analytics foundation with full spectrum detection and investigation capabilities to defend against advanced threats. Unsupervised machine learning creates the detection models that include the establishment of statistical baselines, network privilege escalation detection, peer group anomaly detection, and ransomware. These represent relational values. The platform monitors over 5,000 metrics and 70 different protocols. Importantly, Reveal(x) 360 has visibility over SSL/TLS 1.3 sessions with perfect forward secrecy (PFS) enabled.

Reveal(x) 360 is a cloud-native and cloud-agnostic NDR product designed for hybrid and multicloud security. Delivered as a SaaS, Reveal(x) 360 enables security teams to detect, investigate, and respond to threats anywhere — from the datacenter to the cloud to the user and device edge — in a single management pane. This unified approach eliminates the complexity of deploying and operating separate tools in each environment. It also removes the friction caused by data silos between security and IT teams that need to collaborate closely to provide a safe, reliable digital experience. For cloud deployments, Reveal(x) 360 leverages native integrations with packet mirroring features from Amazon Web Services and Google Cloud, as well as the announced Microsoft Azure vTAP, eliminating the need for agents and making the platform highly scalable and elastic.

Data ingest occurs at line rate as does metadata indexing and collection. However, Reveal(x) 360 provides more than just metadata; a cloud-hosted record store with 90-day lookback enables fully hosted and managed search for streamlined investigation of attacks such as SUNBURST, where an enterprise needs to go back in time to see if it was compromised. The platform also offers optional continuous packet capture (PCAP) for deep forensic investigation, accessible immediately, not just after the fact.

Additional features of ExtraHop Reveal(x) 360 are as follows:

- **Seamless detection over multiple environments.** Reveal(x) 360 can detect and respond to threats immediately across hybrid environments, with response actions including automated investigation and forensics gathering; blocking and quarantining via cloud-native capabilities in AWS, Azure, and GCP; and integrations with endpoint agents and firewalls in any environment.
- **Handling of sensitive data and adherence to regulatory and compliance standards.** Examples of specific data handling include HIPAA compliance and the ability to parse healthcare-specific protocols such as HL7 and DICOM for the healthcare industry and built-in compliance with PCI DSS to audit sensitive data for financial services and retail/ecommerce.
- **Application layer analysis.** Reveal(x) 360 L7 decryption and analysis make it possible to detect the types of threats that other network intelligence products will miss.

Of course, a platform is only as good as its ability to be used effectively in the SOC. The Reveal(x) 360 dashboards have been enhanced to make gains in analyst efficiency and productivity, helping with today's security skill shortage. The data is surfaced so that analysts have everything they need related to an event with one-click drilldown for packet details to determine if it should be escalated to an incident and investigated. Reveal(x) 360 is an NDR product that integrates MITRE ATT&CK into its UI to provide information about the type of attack, detection cards, and detection timeline. Additionally, ExtraHop is an NDR company that contributes expertise to the MITRE ATT&CK framework itself. Toward response, Reveal(x) 360 is widely integrated with leading EDR, SIEM, and security orchestration, automation, and response (SOAR) platforms. This means Reveal(x) 360 can be useful as either a standalone tool or a complementary tool in the SOC.

ExtraHop offers an AI/ML-based foundational approach along with full spectrum detection and response capabilities that include forensics to consolidate legacy tools such as IDS, standalone network forensics, and network performance monitoring (NPM). It can assemble data to see indicators of compromise and provide high-fidelity alerts to defend against advanced threats (including supply chain attacks). Advanced L7 analysis detects advanced threats and ensures network hygiene.

Reveal(x) 360 provides comprehensive visibility over complex hybrid and multicloud environments due to integration with native cloud service provider capabilities such as AWS Traffic Mirroring and GCP Packet Mirroring as well as the ability to investigate and respond to detections via cloud-hosted services securely accessible from anywhere. The 90-day lookback is useful for investigation and threat hunting while its SaaS pricing is customer-friendly. In addition, it is conceivable that Reveal(x) 360 can supplant tools such as IDS/IPS or SIEM for cloud environments as the platform collects insights in real time.

Challenges

Incident detection and response is the most hotly contested market in cybersecurity with many competitors. The types of analytics used by Reveal(x) 360 are the basis for other security toolsets. The shape of extended detection and response (XDR) is not yet determined. XDR may have multiple vendors or a single vendor bringing data to be analyzed. Network intelligence solutions may compete with XDR, but they may also be the analytics engine of an XDR architecture that is still evolving.

Network intelligence may not remain a standalone solution; instead, it may become a feature of the SIEM or XDR tool. SOCs may use a combination of EDR and public cloud IaaS for telemetry to be analyzed with threat intelligence.

However, whatever perspective a given cybersecurity technology uses to detect and respond to network incidents, the demonstrated value of a platform is in the mean time to detect (MTTD) and the mean time to respond (MTTR) to the adversary. Therefore, there's a lot to assess — which applications are affected, if specific users or devices are targeted, and what ingress/egress paths are available to the adversary.

From a cybersecurity standpoint, there is nothing special about the public cloud. To effectively monitor and protect assets, organizations need real-time visibility.

Conclusion

The security of networks requires comprehensive visibility of the network and a source of ground truth to combat advanced threats. Properly understanding the network is more advantageous than assembling insights from point products. From a cybersecurity standpoint, there is nothing special about the public cloud. To effectively monitor and protect assets, organizations need real-time visibility. If ExtraHop can address the challenges highlighted in this paper, IDC believes the company can be successful in the important market for network intelligence tools.

About the Analysts

***Chris Kissel,** Research Director, Security and Trust Products*

Chris Kissel is a Research Director in IDC's Security and Trust Products group, responsible for cybersecurity technology analysis, emerging trends, and market share reporting. Mr. Kissel's primary research area is Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO). The major technology groups within this practice are SIEM, device and application vulnerability management, threat analytics, and automation and orchestration platforms.

***Michelle Abraham,** Research Director, Security and Trust Products*

Michelle Abraham is a Research Director in IDC's Security and Trust Products group, responsible for the Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO) practice. Ms. Abraham's core research coverage includes the cybersecurity AIRO market, focusing on security information and event management (SIEM) platforms and device and application vulnerability management.

MESSAGE FROM THE SPONSOR

About ExtraHop

Stopping a breach requires knowing exactly what you're up against. ExtraHop Reveal(x) 360 shows you not just where intruders are going, but where they've been. Built for cloud scale and delivered as a SaaS, Reveal(x) 360 provides visibility across cloud, datacenter, and IoT—even when traffic is encrypted. Powered by cloud-based AI, Reveal(x) 360 finds advanced threats in real time, while powerful investigation and forensics capabilities allow you to respond 84% faster.

To see the capabilities of cloud-native network detection and response (NDR) for yourself, explore the ExtraHop demo at extrahop.com/demo/cloud/.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.