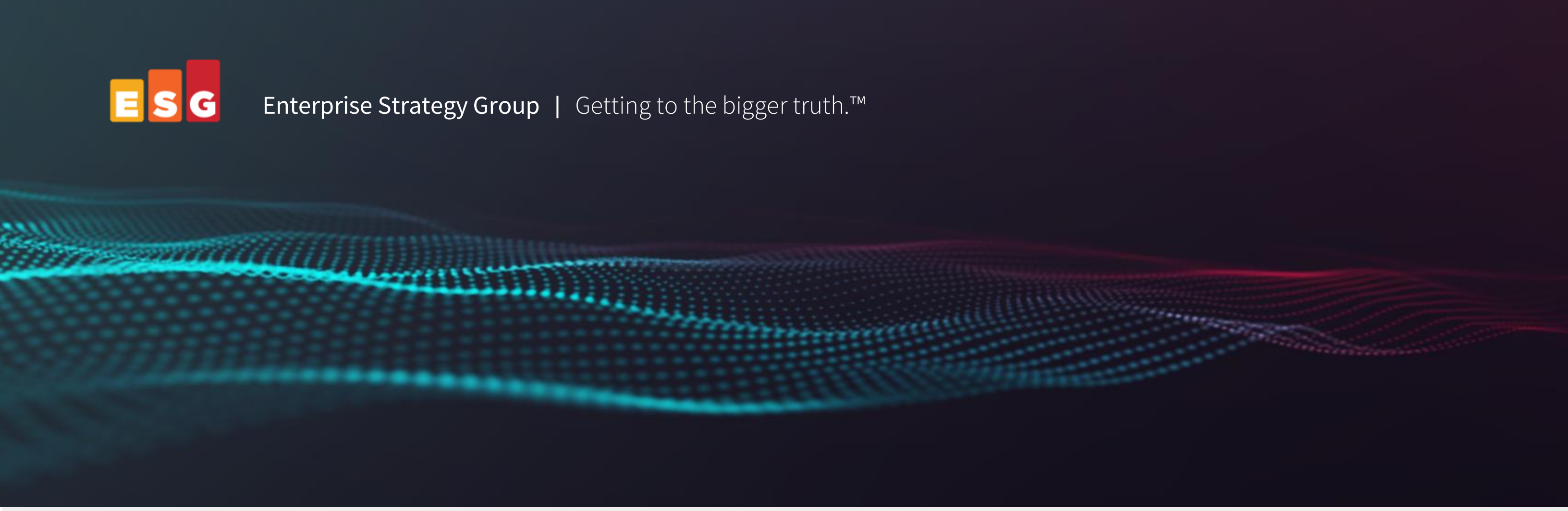


Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

Network Traffic Analysis (NTA): A Cybersecurity ‘Quick Win’

NTA Requirements and Benefits with Cisco Stealthwatch

By Jon Oltsik, Senior Principal Analyst and ESG Fellow

February 2020

This ESG White Paper was commissioned by Cisco and is distributed under license from ESG.

Contents

Executive Summary

According to research from ESG and the Information Systems Security Association (ISSA), 91% of cybersecurity professionals believe that most organizations are either extremely or somewhat vulnerable to a significant cyber-attack or data breach.[1] This level of cyber-risk demands immediate attention and action from CISOs, CIOs, and business executives. As a result, 62% of organizations plan to increase cybersecurity spending in 2020.[2]

Here's the problem: Increasing security budgets alone isn't enough. CISOs need quick and easy wins that can greatly bolster security efficacy and streamline operations without demanding massive projects and vast resources. There is a lot of work ahead. This white paper concludes:

- Security analytics and operations are in a state of disrepair. Organizations count on security analytics for threat prevention, detection, and response. Regrettably, security operations grow more difficult each year due to several external and internal factors. Indeed, organizations face an increasingly dangerous threat landscape and growing attack surface but continue to address security operations with disconnected point tools, manual informal processes, and a lack of the right staff and skills. This mismatch leads to greater cyber-risk.

- Modern NTA tools can provide a quick win. Security operations teams have long used network traffic analysis (NTA) tools like Ethereal, TCPdump, and Wireshark to investigate anomalous, suspicious, and malicious network traffic. These tools morphed into early "on the wire" NTA tools for deep packet inspection and full packet capture (PCAP). Over the past few years, more modern NTA tools surfaced in response to massive scale increases, encryption, and threat sophistication. NTA can now provide comprehensive network visibility, include analytics for threat detection, and store historical metadata for retrospective investigations. Leading NTA tools can be deployed quickly and provide immediate value to junior and experienced analysts.

- Cisco Stealthwatch provides attractive NTA functionality. As part of an ESG research project, cybersecurity professionals were asked to identify the most important attributes of NTA technologies. The list of cited capabilities includes advanced analytics, integration with threat intelligence, and strong monitoring/network visibility.[3] Cisco Stealthwatch aligns well with this list of top attributes. ESG also spoke with several Stealthwatch customers who confirmed its value as a "quick win" technology. This should make Stealthwatch an attractive option for CISOs looking for immediate and measurable help.

The State of Security Analytics and Operations

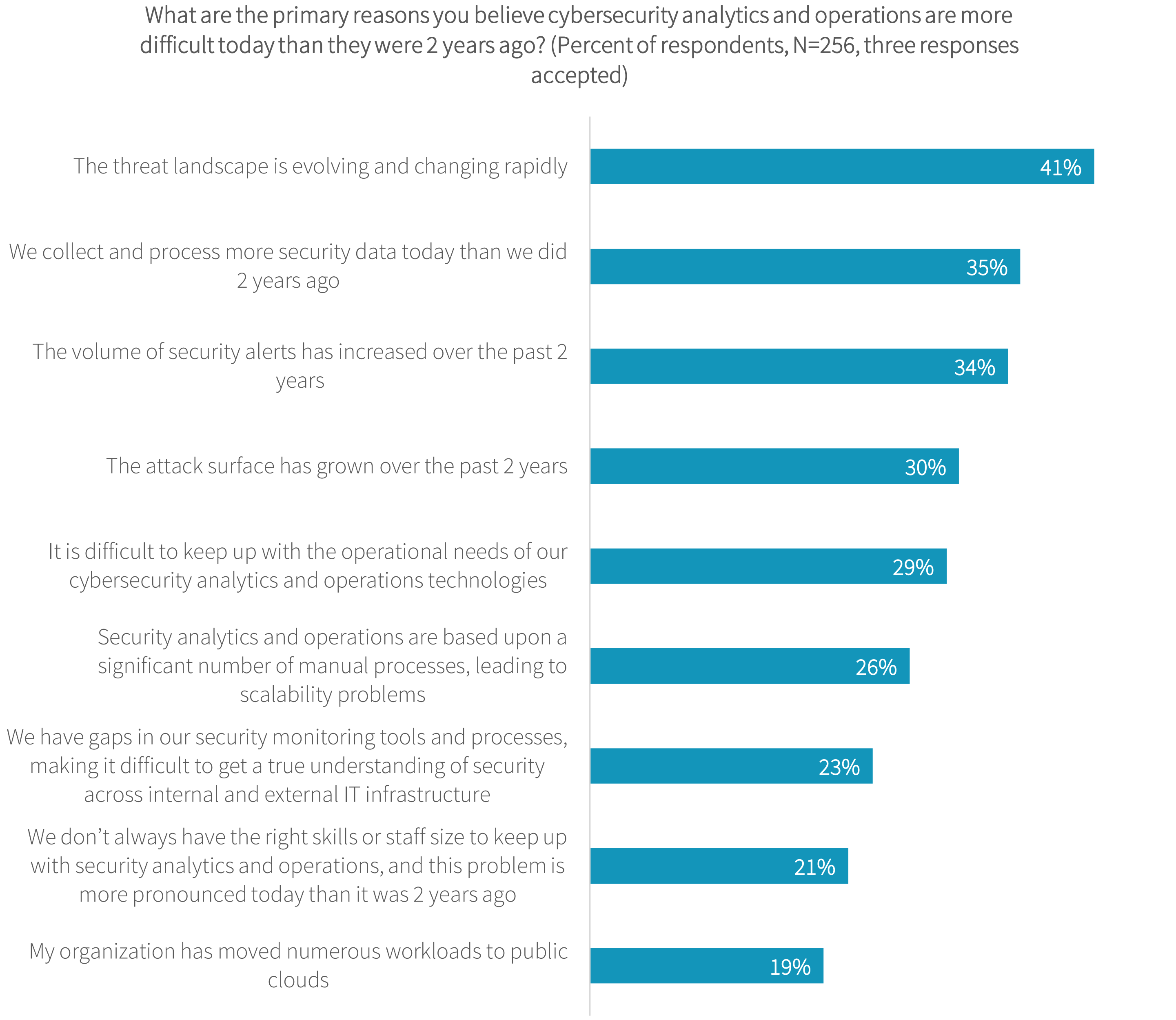
Cybersecurity continues to get harder for organizations in the face of an increasing number of attack vectors and adversary sophistication, and this complexity extends to the area of security analytics and operations. In fact, nearly two-thirds (63%) of respondents claim that security analytics and operations are more difficult for their organization today than they were two years ago.[4] In this regard, security analytics is defined as the collection, processing, and analysis of large and growing amounts of streaming and historical security telemetry like network metadata, cyber threat intelligence, and DNS logs.

Of those respondents who believe security analytics and operations are more difficult than they were two years ago, 41% believe this is the case due to the evolving and changing threat landscape, 35% say they collect and process more security data today than they did two years ago, 34% claim that the volume of security alerts has increased over the past two years,

[1] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2018*, May 2019.
[2] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[3] Source: ESG Brief, *Key Attributes of a Network Traffic Analysis Solution*, September 2019.
[4] Source: ESG Research Report, *The rise of cloud-based security analytics and operations technologies*, December 2019.

and 30% point to a growing attack surface (see Figure 1).[5] CISOs must scale security operations to address the threat landscape and growing attack surface, while adopting modern security and data management technologies to help them tackle growing data and alert volumes.

Figure 1. Reasons Why Security Analytics and Operations Are Increasingly Difficult



Source: Enterprise Strategy Group

Clearly, organizations face a series of internal and external cybersecurity challenges. Internally, security teams must address a massive security data pipeline, keep up with growing volumes of security alerts, and streamline security operations. Externally, organizations need a strategic plan for the swelling attack surface and dangerous threat landscape.

[5] ibid.

The research also indicates that organizations can't simply hire their way out of these issues—nearly three-quarters (74%) of cybersecurity professionals agree that the global cybersecurity skills shortage has had an impact on security operations at the organizations they worked at over the past few years.[6] Furthermore, 70% of organizations reported in a separate survey that it is extremely or somewhat difficult to recruit and hire additional staff for security analytics and operations.[7]

Somehow, CISOs must improve security efficacy, streamline operations, and bolster employee productivity while relying on the existing staff to make this happen.

Network Traffic Analysis (NTA) to the Rescue?

Modernizing security analytics and operations is a tall order. To mitigate risk and protect their organizations, CISOs need to make progress quickly. Where should they start? As the old security saying goes, "the network doesn't lie." In other words, organizations may find it beneficial to start by improving their understanding of network behavior.

According to ESG research, this is already happening—87% of organizations use NTA tools for threat detection and response today, and 43% say that NTA is a "first line of defense" for threat detection,[8] which aids in responding to cyber adversary tactics, techniques, and procedures (TTPs) like network enumeration, command-and-control (C2) communications, and data exfiltration. Beyond threat detection, however, many organizations rely on NTA tools for:

- Network visibility. To quote marketing guru Peter Drucker, "You can't manage what you can't measure." This saying applies equally to cybersecurity. NTA tools can help here by exposing devices on the network, tracking all network connections, and identifying network anomalies. This is especially true as organizations seek to expand visibility beyond north/south traffic to monitor east/west connections within internal networks and extend visibility to public cloud infrastructure.

87% of organizations use NTA tools for threat detection and response today, and 43% say that NTA is a "first line of defense" for detecting and responding to cyber adversary tactics, techniques, and procedures (TTPs).

- Forensic investigations. NTA tools can capture connections history, providing details about network nodes and their conversations. When SOC analysts suspect security issues, they use NTA data to trace back to "patient zero" and track all subsequent network activity. This is why 43% of cybersecurity professionals think of NTA as a first line of defense for threat detection. SOC analysts often start with NTA, and proceed by pivoting to endpoint data, threat intelligence, and security information and event management (SIEM) to further their investigations.
- Strategic planning. NTA provides a map of host communications over time. This gives security and network engineers real data that can be used as a template for zero-trust network segmentation projects. In some cases, NTA tools can integrate with network infrastructure directly for zero-trust policy enforcement. This can be effective in helping organizations reduce their attack surfaces.

Many organizations also share NTA tools between security and network operations teams. While the security team focuses on anomalous/suspicious communications patterns, network operations teams use NTA for performance management

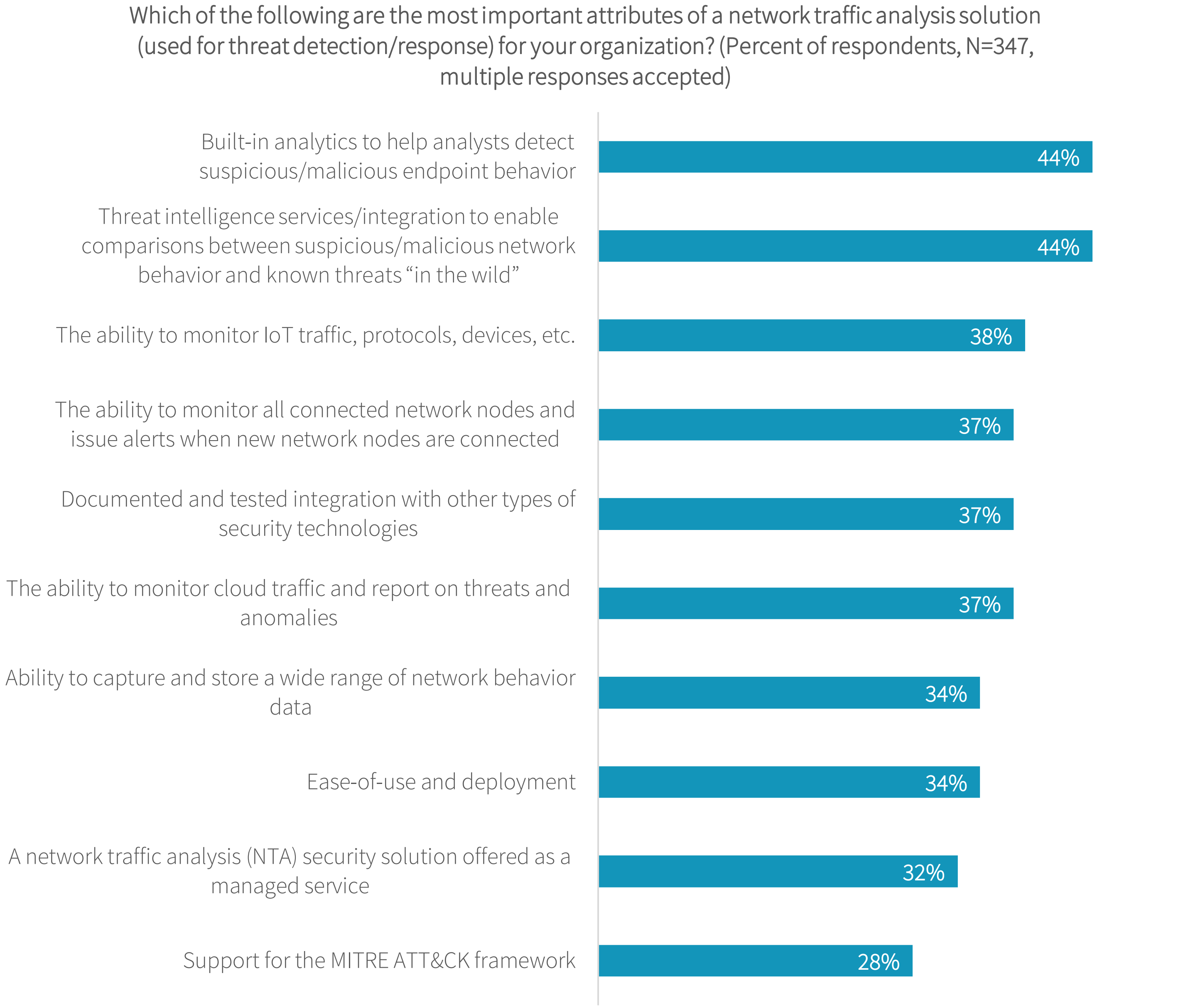
[6] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2018*, May 2019.
[7] Source: ESG Research Report, *The rise of cloud-based security analytics and operations technologies*, December 2019.
[8] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

and troubleshooting. Through this sharing model, organizations gain a technology "force multiplier" while spreading purchasing and maintenance costs across multiple budgets.

Important NTA Attributes

ESG research demonstrates that NTA is an essential tool for security analytics and operations. So, what are the most important attributes of NTA tools? As part of its research, ESG asked 347 cybersecurity professionals this question and found (see Figure 2):[9]

Figure 2. Most Important Attributes of NTA Products



Source: Enterprise Strategy Group

[9] Source: ESG Brief, *Key Attributes of a Network Traffic Analysis Solution*, September 2019.

- 44% said that one of the most important attributes of NTA tools is built-in analytics to help analysts detect suspicious/malicious endpoint behavior, which would improve and accelerate threat detection. Built-in analytics can include machine learning algorithms, heuristics, and signatures. Analysts want NTA tools to crunch the data and deliver high-fidelity alerts, helping them to streamline workloads and accelerate incident response.

- 44% said that one of the most important attributes of NTA tools is providing threat intelligence services and/or integration to enable comparisons between suspicious/malicious network behavior and known threats "in the wild." In this way, NTA tools enrich network security telemetry, making alerts more thorough and actionable.

- 38% said that one of the most important attributes of NTA tools is the ability to monitor IoT traffic, protocols, devices, etc. This requirement is especially important for industries making aggressive investments in IoT like healthcare, manufacturing, and transportation.

- 37% said that one of the most important attributes of NTA tools is the ability to monitor all connected network nodes and issue alerts when new network nodes are connected. In other words, security professionals want NTA tools to assume this traditional NAC capability and issue alerts when unsanctioned devices connect. This is especially important for monitoring and mitigating cyber-risks.

- 37% said that one of the most important attributes of NTA tools is documented and tested integration with other types of security technologies. These integrations often include malware sandboxes, EDR, SIEM, and network segmentation enforcement technologies. In this way, NTA tools can participate in a closed-loop process that includes network security development, monitoring, and enforcement.

- 37% said that one of the most important attributes of NTA tools is the ability to monitor cloud traffic and report on threats and anomalies. In other words, NTA tools must be able to tap into VPCs, cloud monitoring logs, and APIs across AWS, Azure, GCP, etc., to provide end-to-end network security visibility. This is especially useful for monitoring modern serverless applications that can't accommodate host-based security agents.

It is also worth noting that 34% of respondents believe NTA tools must offer ease-of-use and deployment. This is particularly important given the global cybersecurity skills shortage. Unfortunately, many organizations have no time for complex or customized security projects, so NTA must be designed to deliver immediate value to junior analysts and seasoned security investigators.

Cisco Stealthwatch

In October 2015, Cisco acquired Lancope and its NTA product Stealthwatch. Since that time, Cisco has enhanced product functionality and extended Stealthwatch coverage to include monitoring of traffic to, from, and between cloud-based workloads.

> **"With Stealthwatch, we've been able to turn a lot of network security noise into a handful of actionable alerts each day."**
>
> Network Security Administrator, Financial Services Firm

Cisco Stealthwatch should appeal to cybersecurity professionals as it aligns well with the most important NTA attributes cited by surveyed professionals. For example, Stealthwatch:

- Features multiple types of built-in analytics. 44% said that one of the most important attributes of NTA tools is built-in analytics to help analysts detect suspicious/malicious endpoint behavior, which would improve and accelerate threat detection. Stealthwatch aligns with this requirement by providing security analytics like behavioral modeling and multi-layered machine learning algorithms to detect hidden threats. This is likely why Stealthwatch customers give the product high marks for its ability to provide high-fidelity and actionable security alerts. Using Encrypted Traffic Analytics (ETA), Stealthwatch works with Cisco network infrastructure to extend network threat detection to encrypted connections through analysis of network security telemetry, machine learning, and threat intelligence to program classifiers to distinguish between benign and malicious network activity. It's worth emphasizing that ETA performs this function without the expense and overhead of decrypting and then re-encrypting network traffic. Since up to 80% of all web traffic is encrypted today, ETA can be extremely valuable—the Cisco customers ESG spoke with who are using ETA claim that 63% of all threat detections and 76% of critical/high-risk threats were discovered in encrypted traffic.

- Links into Cisco Talos threat intelligence. 44% said that one of the most important attributes of NTA tools is providing threat intelligence services and/or integration to enable comparisons between suspicious/malicious network behavior and known threats "in the wild." Stealthwatch marries onboard analytics with global threat intelligence from Cisco Talos, its large and global threat team composed of analysts, researchers, and engineers. For example, Stealthwatch can help organizations detect when anomalous traffic is connecting with a known C2 server in Odessa Ukraine so they can take immediate remediation actions.

- Provides traffic monitoring and visibility. 37% said that one of the most important attributes of NTA tools is the ability to monitor all connected network nodes and issue alerts when new network nodes are connected. Stealthwatch uses "dynamic entity modeling" to assign roles to entities or devices connecting to the network, and recognizes new devices joining the network. Stealthwatch also has a "host classifier" app that scans the network and assigns entities to select host groups like DNS, web, DHCP, and NTP servers. Additionally, Stealthwatch is often used for IoT security monitoring and threat detection. For example, healthcare customers monitor medical devices using Stealthwatch, while manufacturing and utilities customers use Stealthwatch network monitoring to ensure their OT environments aren't communicating with parts of the network they don't need to. Stealthwatch also integrates with Cisco Cyber Vision to protect specific types of industrial control systems (ICSs).

> **"We had very little monitoring into our network traffic. With Stealthwatch, we were able to see everything! We then used this visibility for threat detection, security investigations, network troubleshooting, and our strategy for network segmentation."**
>
> Network Manager, Higher Education

This level of monitoring and visibility can serve as a baseline for security teams for risk management and mitigation steps like pursuing network segmentation for zero trust. Stealthwatch network traffic monitoring can also be helpful to network operations teams for performance management and troubleshooting.

- Integrates with other Cisco and third-party products. 37% said that one of the most important attributes of NTA tools is documented and tested integration with other types of security technologies. Aside from Talos, Stealthwatch is integrated with several other Cisco products. For example, Stealthwatch

> **"We have a number of Cisco security products beyond Stealthwatch like ISE, AMP for Endpoints, and Umbrella. When we get Stealthwatch alerts, we pivot to CTR for further investigations. This is much more effective than the way we used to do things!"**
>
> Network Administrator, Financial Services Firm

interoperates with the Cisco Identity Service Engine (ISE) and pxGrid for network segmentation policy enforcement and incident response.

Stealthwatch Cloud can be integrated with Cisco Umbrella to add DNS telemetry like geo-location data and malicious domain information to Stealthwatch analytics. Stealthwatch also integrates with Cisco Threat Response (CTR), providing analysts a common interface across NTA, EDR, DNS, and threat intelligence data. Finally, Stealthwatch can be used with leading SIEM software to help SOC analysts align SIEM log analysis with network flow telemetry. This can help enhance and accelerate security investigations.

- Offers visibility into public cloud workloads. 37% said that one of the most important attributes of NTA tools is the ability to monitor cloud traffic and report on threats and anomalies. Stealthwatch Cloud is a SaaS solution that consumes all sources of telemetry native to Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), such as Amazon Virtual Private Cloud (VPC) flow logs, to monitor all activity in the cloud without the need for software agents. This is especially useful for hybrid cloud infrastructure that includes corporate data centers and multiple public cloud services.

Stealthwatch also features a simple, agentless deployment model based upon flow and metadata collected directly from the existing network infrastructure (i.e., switches, routers, cloud-based logs and APIs, etc.). This not only eases deployment but also turns the network into a real-time threat sensor.

> **"When we switched from a traditional 3-tiered architecture to using cloud-native technologies like AWS Lambda, we had to find an agentless security monitoring tool. With Stealthwatch, we were able to gain visibility into the VPC traffic flow logs. Now we can see Lambda functions spinning up and talking to the database and Elasticsearch clusters and lots of other things."**
>
> CTO, Health Care Firm

The Bigger Truth

Based upon the ESG research presented in this white paper, it is safe to assume that security operations grow increasingly difficult annually due to increasing scale, an expanding attack surface, and unrelenting sophisticated cyber adversaries targeting all types of organizations.

Given the increasing demands, CISOs can't expect to keep up with security workloads through tactical adjustments to their programs—especially considering the global cybersecurity skills shortage impacting most organizations.

To alter the balance, CISOs need high-impact quick wins. In other words, they need to make changes that can deliver high impact without the requirement for lots of time and resources. ESG research clearly indicates that NTA has the potential to deliver this type of quick win, but only if it provides the important product attributes described.

Cisco Stealthwatch aligns well with cybersecurity professionals' list of important NTA attributes. Furthermore, ESG interviews with several Stealthwatch customers provided good examples of organizations gaining a lot of value quickly, without undertaking major resource-intensive projects. As such, CISOs may want to contact Cisco to learn more about how Stealthwatch may be able to help them improve efficacy while streamlining security operations.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com ✉ contact@esg-global.com ☎ 508.482.0188