The Network at the Core of Detection and Response

Katie Teitler
Senior Analyst, TAG Cyber

Enterprises' attack surfaces are ever-expanding, and cyber criminals are taking advantage of the known unknowns to compromise and exploit well-meaning but often under-resourced security programs. With that said, there is no better place than the network to understand the security posture of an organization.

Introduction

An old saying goes, "an ounce of prevention is worth a pound of cure." And over the last decade, enterprises spent significant effort and budget on tools to prevent cyber security compromise. However, even with the plethora of preventative tools on the market, attacks continue to evade defenses. The reality is that with enterprises' growing attack surfaces, fueled by digital expansion and transformation, it's nearly impossible to keep well-resourced attackers—who have the time and patience to execute an attack—from leveraging any one of the thousands of vulnerabilities in an enterprise's technology stack. As such, in more recent years, we've seen an explosion in detection and response (*DR) technologies: EDR (endpoint), MDR (managed), XDR (extended), ADR (application), and of course, NDR (network).

Network detection and response (NDR), which considers the network the "ground truth" of an organization's attack surface, leverages network data to find and highlight suspicious behavior, then allows for automated response capabilities.

As part of NDR capabilities, network traffic analysis is one of the most foundational elements for executing proper security control. Now more than ever, the network is the central component of business operations. But today, the network isn't just the on-premises, bare mental data center of yesteryear. Modern enterprises use a combination of cloud and virtual environments, containers, and internal data centers. Internet of Things (IoT) devices are becoming commonplace. And operational technology (OT) is converged with and managed on IT-based systems. If that weren't enough, third-party connected systems must all be monitored as closely (if not more when you consider the shared and ephemeral nature of some of these new network spaces).

With all the change in IT, the one thing companies can rely on is the network: what entities are present, which ones are communicating, how, what patterns and behaviors do they exhibit? If the network is the "ground truth," then arguably IT and security teams need better visibility into traffic and behavior patterns—at all layers.

As such, we at TAG Cyber, along with our partner, Awake Security, set out to understand how CISOs and their teams view their network (a.k.a. the network attack surface) and management thereof. Through personal email outreach to select CISOs, coupled with a social media survey to the security and

networking community, we gained the perspectives of active practitioners at both large and small enterprises, across industries in the U.S.

To that end, each solicited expert was asked to provide their best assessment of the following questions.

Which definition best describes your network?

1. It's everything communicating on our internal, on-prem data center
2. It includes the on-prem data center plus everything in the cloud
3. Something else _____

What is your main concern about your network?

1. Lack of visibility at layers 2-7
2. The increase in unmanaged devices on the network
3. The scope of our partner and supplier ecosystem introduces unbounded threats
4. The amount of telemetry we collect is overwhelming
5. We lack internal resources to triage and remediate threats
6. Other _____

Network hosting

Fifty-seven percent of respondents said that their network is a hybrid of the on-premises data center plus cloud. (The assertion is that "cloud" consists of private, public, and multi-cloud environments.) This result is not surprising; despite the clear benefits of cloud usage and the built-in security accompanied by the major cloud providers' offerings, many organizations continue to maintain legacy infrastructure. The reasons—whether control concerns, budget pressures, resource constraints, or other issues—are out of scope for this focused study.

The remaining 43% of respondents said their network infrastructure is comprised of "something else"; the supplied answers were, as expected, a mix of full-cloud (a combination of public, private, and multi-cloud) and virtual. No respondent claimed to run a fully on-prem environment.

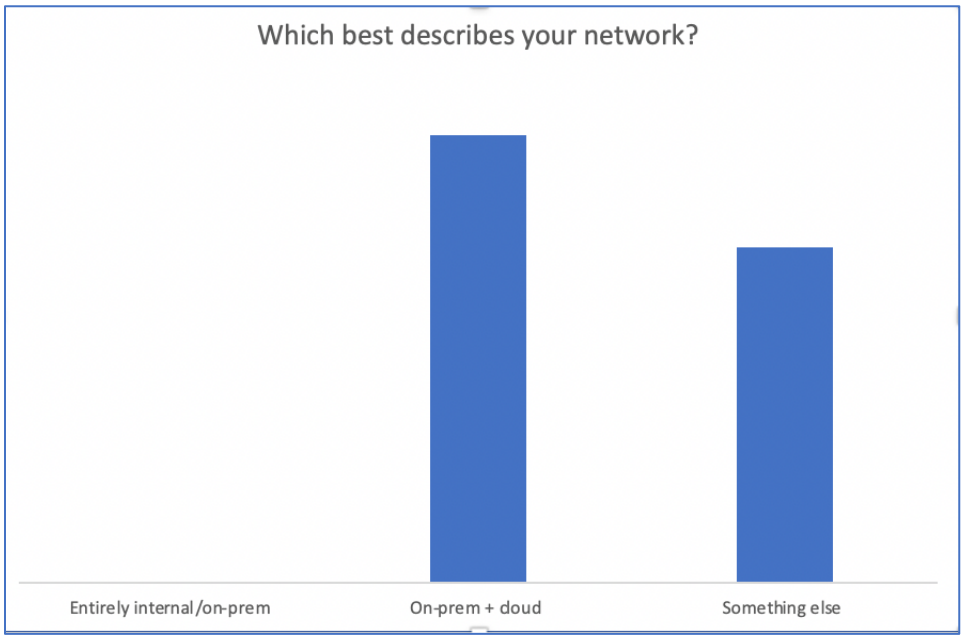

Figure 1: Security executives report the greatest use of hybrid cloud networks

It's important to note that the responses for this survey were collected in August 2020, five months after U.S. companies were suddenly forced to operate 100% remotely. This is relevant because, during this time, many companies expressed their need to rapidly move to the cloud. And while this might have been true for applications and services, core networks did not see a sudden migration (which would have been near-impossible for many companies in such a limited time period).

While the security industry has been talking about cloud migration for over a decade, the fact is that most companies operate in hybrid mode, meaning that to properly evaluate network traffic, they must deploy, manage, and maintain tools that can work ubiquitously across hybrid environments. The challenge of running disparate tools for on-premises, cloud, and virtual environments is too much for any but the largest and most well-funded security organizations to bear, from both a cost and a resource standpoint. Even at that, in our work with enterprise security teams, we have overwhelmingly found that security organizations prefer to run tools that can provide consistency and standardization across their hybrid infrastructure. The resource cost of context switching between disparate systems is burdensome, and thus incident detection and response capabilities that seamlessly extend across environments is attractive to these practitioners.

Network concerns

For the second question—what is your main concern about your network?—43% of respondents said "lack of visibility at layers 2-7," 29% said "the increase in unmanaged devices," and 21% said they were most concerned with third-party connected ecosystems. The remaining 7% of respondents were evenly split between concern over an abundance of telemetry and a lack of internal resources to triage and remediate threats.

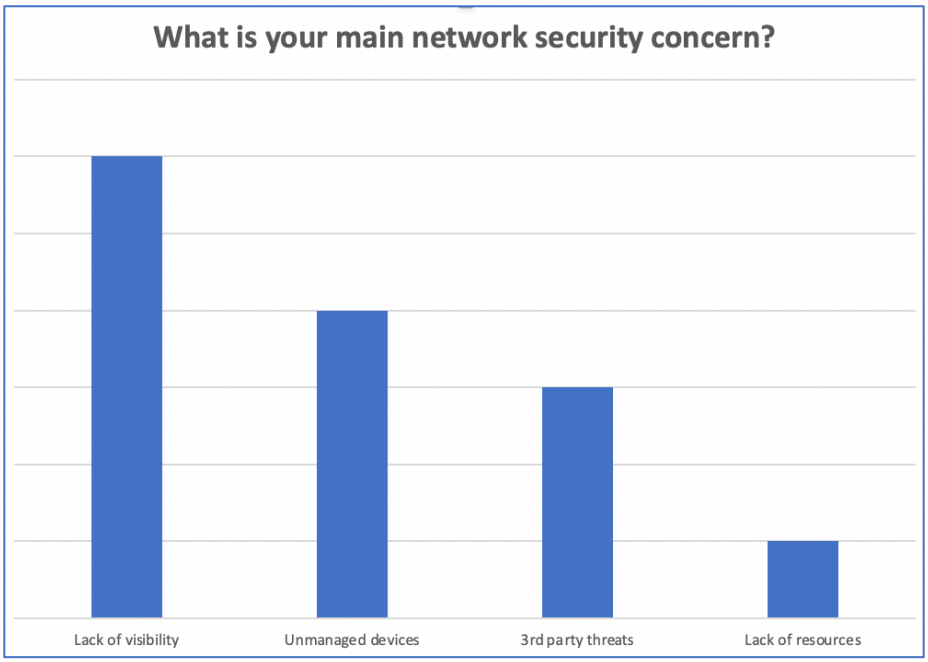

Figure 2: Security executives express concern over lack of visibility on their networks

In one respect, one could attribute the concern over unmanaged devices on the network to "lack of visibility." However you chose to interpret respondents' answers, lack of visibility across hybrid, disparate environments has been a chief concern for many years. Spotty visibility and inability to automatically correlate network data across environments have eaten up tremendous resources, often in the form of manual work by network admins, and caused a lot of management headaches, missed signals, and thus unnecessary network risk.

With the complexity of today's network environments and the abundance of data traversing them, organizations want automated tooling that can provide real-time visibility into network anomalies and intent detection based on behavioral analysis. The data outputs must also be normalized across network environments. Furthermore, today's technologies must raise the signal from the noise, allowing operators to quickly respond when a potential network threat is identified. Lastly, as machine learning capabilities improve, security teams are relying more and more on security technologies that can automate elements of triage and response, freeing up analyst time for higher-level tasks that help the business respond and recover from a cyber event swiftly, without widespread damage.