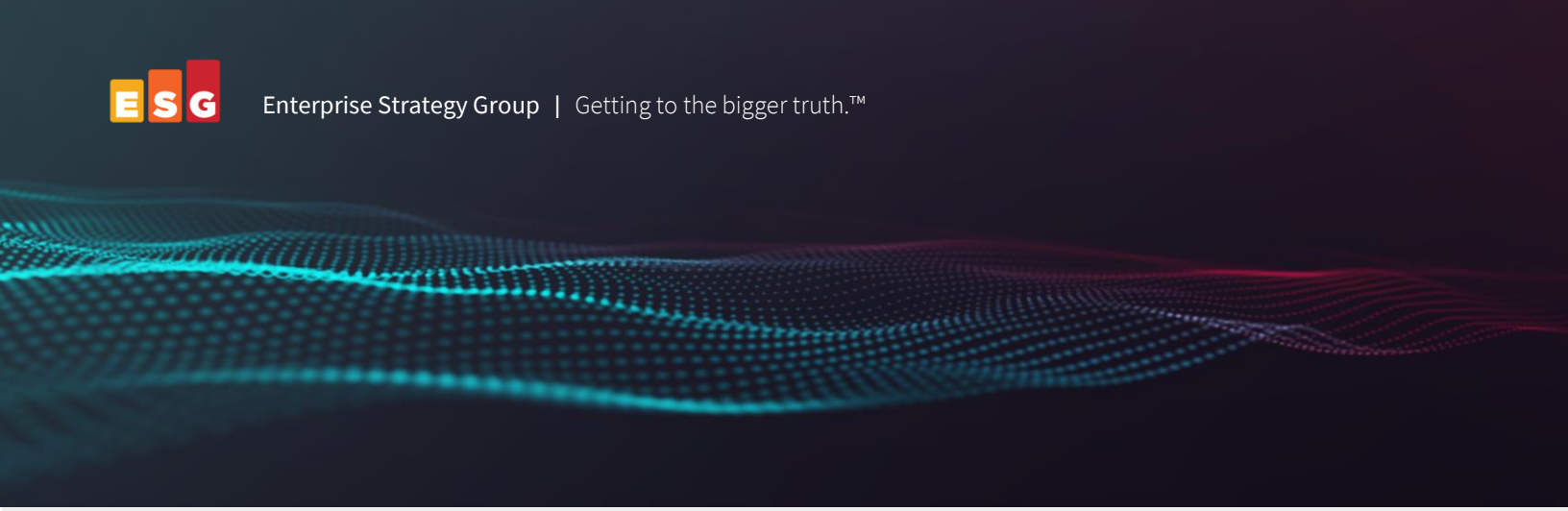


ESG WHITE PAPER

How Security Approaches Must Evolve to Address Modern Network Threats

By John Grady, ESG Analyst

June 2020

This ESG White Paper was commissioned by Palo Alto Networks and is distributed under license from ESG.

Contents

Executive Summary

Many organizations today have undertaken digital transformation initiatives. These programs have led to the increasing adoption of IoT, mobility, and cloud, resulting in an increasingly distributed IT landscape. Attackers have resources and more sophisticated methods than ever to use against organizations.

Organizations should look for network security platforms that leverage machine learning to proactively ensure real-time, consistent, distributed enforcement across the entire network and provide intelligent centralized management.

A significant part of the problem is that legacy security solutions cannot adequately address the dynamic nature of the attack landscape and enterprise environment itself. Traditional signature-based, manual, and siloed tools struggle to provide the protection, scalability, and performance necessary to meet the requirements of the modern enterprise. As a result, organizations should look for network security platforms that leverage machine learning to proactively ensure real-time, consistent, distributed enforcement across the entire network and provide intelligent centralized management.

Digital Transformation Has Dramatically Increased the Attack Surface

Digital transformation (DX) initiatives are not new yet continue to drive the evolution of even the most foundational areas of IT in order to create operational efficiencies, provide differentiated customer experiences, and develop new data-centric products and services. In large part to enable these programs, organizations increasingly turn to IoT, mobile, and cloud technologies.

Distributed IT Has Become the New Normal

The common thread across all the enabling technologies supporting digital transformation is their distributed nature. While it is well understood that many organizations are investing in IoT, mobility, and cloud services in some fashion, the nuance here is important. Specifically, ESG research has found:

- 35% of organizations reported having IoT initiatives underway. Further, another 29% are currently developing them and expect to launch in 2020, pointing towards an imminent broad, cross-industry focus on IoT.[1]
- 76% of knowledge workers are currently working from home due to the COVID-19 crisis.[2] More specifically, 70% of employees reported that they usually worked from the office before COVID, but now are only working from home, highlighting the massive scope of this transition not only for IT organizations but users themselves.[3]
- Three-quarters of organizations reported storing sensitive data in multiple public cloud platforms., a fact that holds true across software-as-a-service (SaaS) and infrastructure-/platform-as-a-service (IaaS/PaaS).[4]

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[2] Source: ESG Master Survey Results, *Technology Impact of COVID-19: IT Decision Maker (ITDM) View*, May 2020.
[3] Source: ESG Master Survey Results, *COVID-19 Technology Implications for Knowledge Workers*, May 2020.
[4] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

Siloed, Legacy Security Approaches Cannot Address These Modern Dynamics

Despite implementing these significant changes throughout the enterprise, many continue to utilize legacy approaches to secure their environments. However, as these initiatives have been more broadly deployed, significant security challenges have arisen. In fact, 85% of respondents indicated that network security is more difficult than it was 2 years ago. Threats remain the single largest reason, cited by 45% of respondents. However, network complexity due to the increasing number of devices on the network (38%), the use of both sanctioned (30%) and unsanctioned (25%) cloud applications, and an increasingly distributed workforce (24%) were also cited as causes for this difficulty.[5]

Security Efficacy Is Impacted

Cyberattacks are relentless and continue to use more sophisticated approaches. Both the volume and variants of malware are on the rise, and signature-dependent, reactive tools cannot keep up. Organizations are often forced to choose between weaker security controls that rely on not being the initial victim of a new type of threat or intrusive file scanning or modification that prevent threats at the expense of the user experience.

Further, the security tool sprawl resulting from a siloed approach leads to inconsistent visibility and enforcement, which impacts security effectiveness. This problem is multifaceted.

- Human error: The potential for human error increases as manual tasks mount. Misconfigurations and rule conflicts are more likely when devices are managed in isolation.
- Visibility: While analytics and operations tools may help to aggregate the telemetry from different types of security infrastructure across the network, this can take time and often detects issues after they occur. Additionally, when the threat intelligence supporting different tools is not synchronized, some tools may have visibility into zero-day threats while others remain blind.
- Consistency: With different tools in place, it is difficult to consistently enforce policy across different environments. For example, when users are on the network, policy is enforced by on-premises tools. But when they're off the network, a separate toolset must be configured to enforce the same policy (endpoint protection, for example), which is time-consuming and cannot be ensured by organizations.

Complexity Makes Efficient Security Management Difficult

The current tools in use help drive this complexity as well. Siloed, independently and manually managed network security tools create operational inefficiencies. It has become nearly impossible to scale the replication and implementation of firewall rules and network security policy on the myriad of devices across physical, virtual, and cloud environments. Some of the top challenges that organizations face relative to their network security tools include:[6]

- Inconsistent management across physical and cloud/virtual environments: The most common challenge, cited by 44% of respondents, was inconsistent management across different environments. This has been an issue for years but has percolated to the top of the list with the adoption of hybrid cloud and multi-cloud environments.
- Number of tools: With the security industry having historically developed a new tool to address each new platform and threat vector, it is unsurprising that 36% of respondents reported the number of different tools as a top challenge.

[5] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.
[6] ibid.

- Implementation: While security is often part of the network design and engineering process, it is not always a consideration. When security teams have to "bolt" solutions on after the fact, implementation can become difficult, which 33% of respondents cited as a top challenge.

- Scalability: As stated, the network is increasingly dynamic, with IoT and container environments requiring performance on demand to support analytics and increased utilization. Security tools not purpose-built for these environments can impact scalability, which was a challenge reported by 25% of respondents.

The Performance Penalty

Finally, legacy approaches often have adverse effects on performance and ultimately end-user experience. In fact, 42% of organizations cited performance issues negatively impacting user experience as one of the biggest challenges relative to network security tools.[7] One example of this relates to how organizations secure branch office traffic destined for cloud applications: Historically, this traffic would be routed back through the campus data center for enforcement. However, backhauling traffic that may originate in South America to the United States only to terminate in an AWS EC2 Instance in Sao Paulo adds unnecessary latency and may degrade application performance. SD-WAN solutions have emerged to solve the networking issues associated with this dilemma, but have led to a security choice: Utilize the native SD-WAN security functionality, which is often extremely limited, or deploy cloud-delivered security services to support local breakouts, which adds tools to the mix and starts the cycle over again with inefficiency and complexity.

Attributes for Today's Network Security Platform

The responsibility of today's cybersecurity team is to securely and dynamically provide the right level of access to anyone and any resource on the network, regardless of the location or time. This has become increasingly difficult for all the reasons previously discussed. To better address the dynamic nature of not only the threat landscape but the network itself, organizations require a proactive platform-based approach to network security, leveraging machine learning to provide real-time, consistent, distributed enforcement across the entire network with intelligent centralized management.

Best-of-breed Capabilities in a Consolidated Platform

Enterprise security organizations have historically focused on a best-of-breed approach over the integrated focus of their smaller counterparts. That has not changed, with 68% of respondents reporting that their organization tends to purchase best-of-breed security products. This is often measured, at least in part, by security efficacy, which remains the top purchase consideration for cybersecurity technologies by an overwhelming margin. Specifically, ESG research found that 41% of respondents ranked the ability to detect and prevent threats as their top purchase consideration.[8]

To address modern polymorphic malware, targeted phishing attacks, and advanced ransomware, security solutions must increasingly utilize artificial intelligence (AI) and machine learning (ML) to differentiate malicious content from the benign. So, it should come as no surprise that cybersecurity technologies that employ AI/ML for threat detection are most commonly named as one of the areas of cybersecurity that will see the most significant investment over the next 12-24 months, as cited by 32% of ESG research respondents.[9] However, these capabilities must be inline so as not to impact the user-experience and ensure threats are prevented in real time.

Enterprise organizations are beginning to recognize that platform-based solutions can offer best-of-breed capabilities. ESG research indicates that 80% of respondents believe their organization would consider buying a significant amount of its

[7] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.
[8] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment*, March 2020.
[9] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

security technologies from a single vendor. In fact, by reducing the number of vendors from which security technology is procured, a majority of respondents feel threat prevention and detection efficacy would be improved (58%) as well as operational efficiencies realized by security and IT teams (51%). Faster time to problem resolution (46%) and tighter integration between previously disparate security controls (39%) were also frequently cited as perceived benefits.[10] So, while highly effective security solutions remain a top requirement, organizations are beginning to realize that consolidated solutions can offer that efficacy across multiple domains, while also providing the benefits realized through a platform approach.

Flexibility Is Paramount

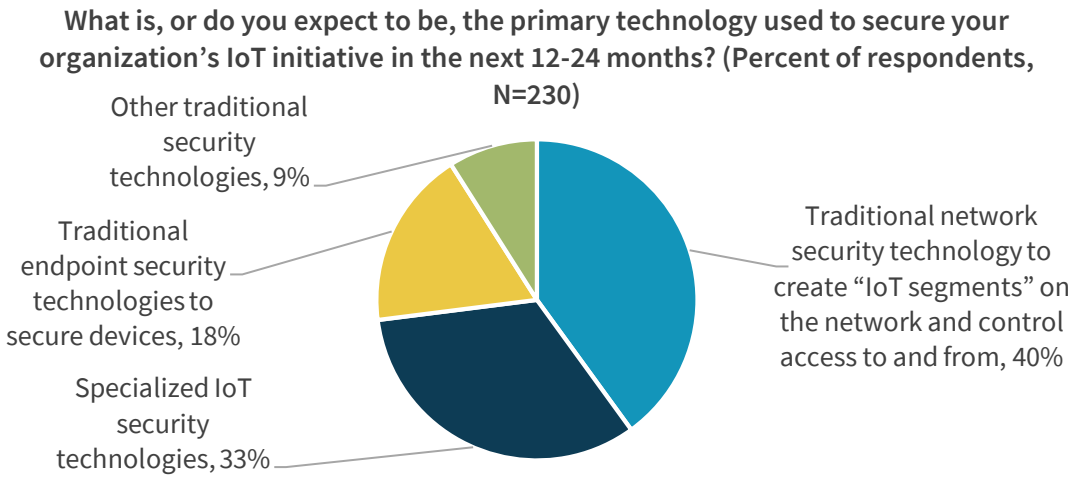
Distributed enforcement must address not just the different locations across the enterprise environment, but the different approaches that may occur within each.

WAN

IoT

While there are numerous dedicated solutions for IoT security, 40% of organizations expect to use traditional network security technologies to secure their IoT initiatives (see Figure 1).[11] Although utilizing the network makes sense considering the difficulty in using an agent-based approach for many IoT use cases, and leveraging existing investments makes sense from an efficiency perspective, IoT security is still something new to many security vendors. Segmenting this traffic from the rest of the network often makes sense to prevent compromised IoT devices from becoming the beachhead for an attack. However, this can become overwhelming as the number and type of devices increase. As such, vendors that have invested in IoT-specific capabilities to accurately categorize devices, automatically apply policy based on the type of device and predetermined rulesets, and most importantly, utilize advanced analytics and machine learning to parse through the overwhelming amount of IoT-based traffic to fingerprint unknown devices, uncover anomalies, and detect attacks are better able to secure these environments.

Figure 1. Traditional Network Security Tools Will Be Critical to IoT Security



Source: Enterprise Strategy Group

[10] ibid.

[11] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.

SD-WAN

SD-WAN has risen to the top of the networking to-do list for many organizations, but the capabilities and approaches vary. There are different SD-WAN models to address the first, middle, and last mile of transport. The first mile may terminate at a standard network or security device, or a lightweight device that connects to the cloud where the actual functionality resides. The middle mile may consist of a fully managed cloud service, or organizations themselves may deploy virtual machines to optimize routing through the public internet to avoid congestion and other issues. Similarly, the last mile may be fully managed, or organizations may choose to create their own peering through proximity to their cloud providers.

Additionally, the security capabilities vary from solution to solution. Even those SD-WAN offerings with strong, native security functionality may only provide a single consumption model (i.e., a fully cloud-delivered solution, or a heavy branch approach). Some industries may favor one approach over another; for example, retail and hospitality businesses see value in maintaining an on-premises approach at their distributed locations for compliance reasons. However, some organizations are simply not prepared to shift to a fully cloud-delivered model all at once. So, the ability to leverage the existing security infrastructure and over time adopt a cloud-centric approach is important. Regardless of which approach an organization takes, consolidated security solutions with SD-WAN functionality that provide cloud-delivered capabilities are poised to see massive adoption over the coming years.

Mobile

Especially in today's world, securing remote workers with the same consistency as when they're on premises is a top priority for nearly all organizations. But perhaps even more important, the ability to quickly ramp these capabilities up to meet a sudden spike in remote work and back down again when those workers return to the office is only possible at scale through a cloud-enabled solution. Traditional approaches relying solely on legacy VPNs utilizing on-premises appliances cannot scale up and down in this way or provide the same level of security when employees access cloud applications.

Data Center and Hybrid Multi-cloud

Physical appliances remain a key control point for data center ingress/egress for many organizations and provide the required horsepower for highly performant networks. At the same time, virtual appliances continue to see increased adoption to provide visibility into east/west traffic in software-defined data centers and enable security to keep pace with the dynamic nature of these environments.

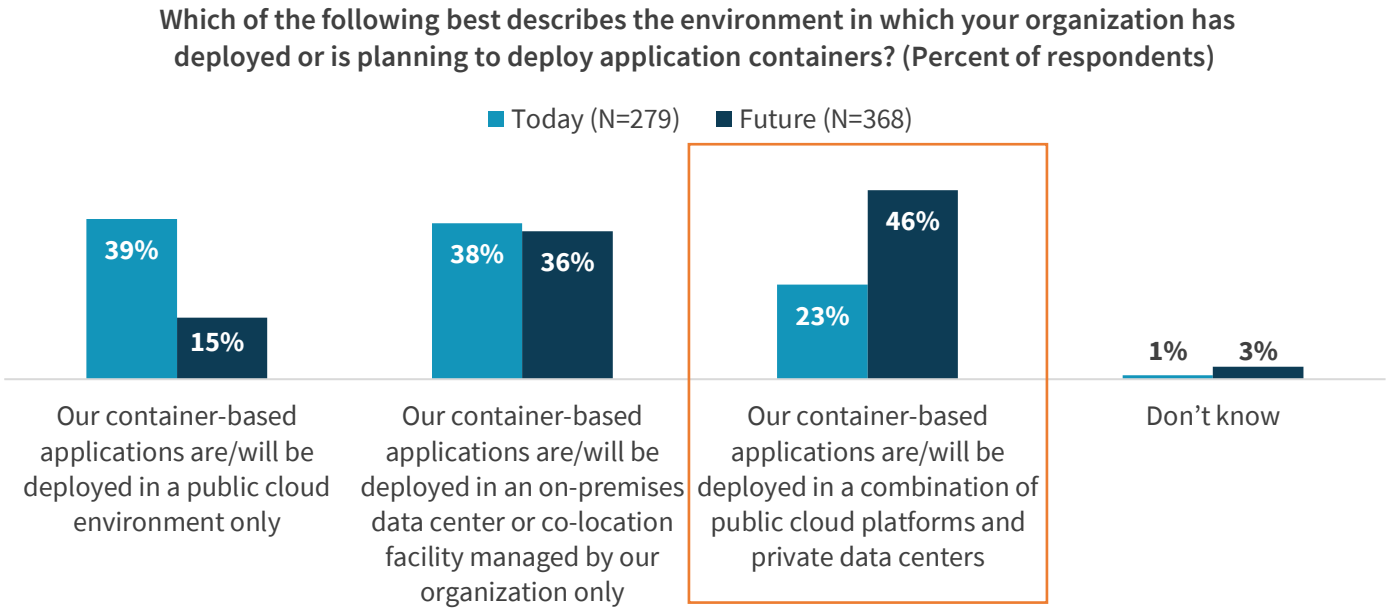
However, container adoption has added new dynamics to network security. Containers enable hybrid cloud and multi-cloud adoption, an approach in which inter-application east/west traffic in fact becomes north/south. This will become an increasing issue over time as ESG research has found that 46% of respondents expect their container-based applications to be deployed in a combination of public cloud platforms and on-premises data centers, highlighting the direction the market is taking toward hybrid-cloud (see Figure 2).[12]

While some existing solutions integrate with container orchestration tools, the visibility is often limited to the node or cluster and focused on basic port and protocol filtering. To properly address cloud-native container environments, NGFW-level visibility and enforcement must extend to inter-pod and container-to-container traffic to apply threat inspection within a cluster and improve protection within containerized data centers. Further, containers are often accessing web resources such as GitHub repositories to pull down source code. This becomes an additional driver to have visibility and control over web application traffic to ensure the container only communicates with the correct repository and that the

[12] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.

resulting traffic is not spoofed or malicious. NGFWs offering support across physical, virtual, and containerized environments help drive consistent security across increasingly hybridized data centers.

Figure 2. Hybrid Cloud Adoption Will Increase with the Use of Containers



Source: Enterprise Strategy Group

Subscriptions

A key factor to successfully delivering the flexibility to address these different use cases and parts of the environment is a subscription-based approach. This enables the efficient expansion of existing capabilities and the adoption of additional use cases over time. For network security, broad coverage is required not just across traditional next generation firewall (NGFW) functionality such as application control, IPS, and URL filtering, but also for advanced capabilities such as advanced malware detection, DNS protection, and data loss prevention (DLP). Capabilities supporting the SD-WAN and mobile use cases described should also be consumable via subscription on the core network security platform.

Further, these threat protection subscriptions should provide inline prevention utilizing multi-technique malware detection to identify and block unknown file-based threats. This functionality should be informed by machine learning capabilities to accurately detect evasion techniques and zero-day threats prior to them entering the network.

Centralized Management Across the Entire Spectrum

Providing a broad set of capabilities only solves part of the problem. A single pane of glass, centralized management console is a necessity because so many parts of the environment are addressed, but it must go further. Specifically, a proactive approach to remain ahead of attackers by identifying misconfigurations before they are exploited, recommending optimal policy constructs, and recognizing potential future performance impacts based on traffic flows are all important components in securing the modern enterprise environment. Capabilities should include:

- Automation informed by machine learning to generate and apply policies as resources are spun up to securely harness the dynamic nature of software-defined and containerized resources.
- A centralized rule base with the ability to push consistent policy across all network security devices, regardless of location or environment.

- Visibility across the entire infrastructure.
- Granular, role-based administration to address the increasing consolidation of network and security functionality and limit access to the specific management functions an individual is responsible for—not only for policy creation, but also for visualization, logging, and reporting.

The Bigger Truth

Security teams continue to be understaffed and overworked and are too often blamed for slowing down the adoption of new technologies. But the security organization can only do so much and is limited by the tools it has at its disposal. Attackers exploit the fact that enterprises are forced to move quickly and often insecurely as they implement technologies to support digital transformation initiatives. The combination of an expanded threat surface with sophisticated malware and multi-phase attack chains has made prevention harder than ever.

With all this in mind, it has become essential for network security organizations to reconsider their strategies and shift to a more proactive model. One way to enable this is through the integration of machine learning into a platform-based approach in order to improve efficacy, efficiency, and agility. The ability to detect advanced threats inline while limiting the attack surface by reducing misconfigurations and optimizing policy is essential to defend the distributed enterprise from the modern attacker.

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