



ESG WHITE PAPER

Requirements for Preventing Evasive Threats

Incorporating Deep Learning, Comprehensive Coverage, and Intelligent Management into Network Security with Palo Alto Networks

By John Grady, ESG Senior Analyst

March 2022

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

Contents

Executive Summary	3
Attackers Continue to Exploit Gaps in Traditional Cybersecurity Approaches	3
Evasive Threats Have Become the Norm.....	3
The Use of Cobalt Strike and Red Team Tools Are on the Rise.....	4
Phishing Tactics Move Beyond Email.....	4
Legacy Tools Cannot Meet These Challenges.....	4
Three Ways to Improve Protection Against Evasive Threats.....	5
Palo Alto Networks Provides In-line, ML-Based Protection Against Evasive Threats.....	6
The Bigger Truth	8

Executive Summary

Attackers continue to update their tactics to remain ahead of enterprise defenses and use evasive techniques to avoid detection by traditional cybersecurity tools. Pre-built attack tools, stealthy communications and exfiltration avenues, and advanced phishing techniques are all used to compromise and exploit target organizations. While out-of-band and signature-based detection approaches remain critical in preventing known threats, a new approach is required to protect organizations from these attacks using evasive techniques. As a result, machine learning and advanced analytics have become a critical component of threat prevention tools. Yet, just as importantly, these mechanisms must be applied in line to prevent threats before they can impact even the first potential victim.

Palo Alto Networks is addressing these issues through the addition of in-line deep learning to its network security platform. Specifically, enhancements to its Advanced Threat Prevention, Advanced URL Filtering, and DNS Security services help prevent unknown command and control traffic, block attacks from tools such as Cobalt Strike, detect attacks that evade traditional URL databases and web crawlers, and ensure attackers cannot use DNS as an avenue of attack.

Machine learning and advanced analytics have become a critical component of threat prevention tools but must be applied in line to prevent threats before they can impact even the first potential victim.

Attackers Continue to Exploit Gaps in Traditional Cybersecurity Approaches

For as much emphasis as most organizations put on cybersecurity, attackers keep evolving their tactics to remain one step ahead of defenses and high-profile breaches continue to make headlines. So, it is unsurprising that 64% of ESG research respondents indicate network security has become more difficult over the last two years.¹

Evasive Threats Have Become the Norm

While there are a variety of factors making network security more difficult, the threat landscape is the most commonly cited challenge. Specifically, 41% of organizations say that an increase in malware volume, sophistication, and targeted attacks is a critical issue.² While unfocused attack campaigns and less sophisticated malware can certainly impact an organization if not accurately identified and blocked, more targeted attacks have become increasingly common.

36% of cybersecurity and IT professionals say their company has experienced ransomware attacks at least monthly, and another 27% saying they have experienced at least one attack over the past 12 months.

This should not be surprising, as cybercrime has evolved into an organized, well-funded, multi-billion dollar enterprise, as exemplified by the ransomware epidemic of the last few years. These attacks have affected organizations of all types, with ESG finding that 36% of cybersecurity and IT professionals say their company has experienced ransomware attacks at least monthly, and another 27% saying they have experienced at least one attack over the past 12 months.³

¹ Source: ESG Research Report, [Transitioning Network Security Controls to the Cloud](#), August 2020.

² Ibid.

³ Source: ESG Research Report, [2022 Technology Spending Intentions Survey](#), November 2021.

The Use of Cobalt Strike and Red Team Tools Are on the Rise

Yet, while some threat actors are indeed more sophisticated than their peers, the availability of tools to help less-skilled attackers scale their efforts has become a significant issue. Loaders and crypters have been widely available for years to help attackers automate the process of gaining remote access and stealthily deliver malware to target organizations. More recently, attackers have turned to the use of Cobalt Strike, a legitimate penetration testing tool. Palo Alto Networks' threat research organization, Unit 42, found a 73% increase in Cobalt Strike malware samples in 2021 compared to 2020, based on malicious files evaluated by its WildFire analysis engine.⁴ Cobalt Strike provides attackers a range of pre-built capabilities to help them more efficiently perform reconnaissance, deliver malicious code, and gain persistence in the environment. In particular, the tool enables attackers to perform fileless attacks using PowerShell for remote code execution. Because these attacks use legitimate system tools in the environment, they can be very difficult to detect.

Further, once attackers gain a foothold in the environment, it has become easier for them to exfiltrate data without detection. At a minimum, attackers will often use encrypted channels to move data from inside the environment to an external repository. This may be a self-hosted server instance for which the attacker has set up encryption or SaaS services that use encryption by default such as Google Drive or Microsoft OneDrive.

Additionally, Cobalt Strike includes covert command and control (C2) capabilities over web (HTTP) encrypted channels (SSL), the domain network system protocol (DNS), or the server message block protocol (SMB). DNS tunneling in particular is difficult to detect because of the high volume of requests typically seen in an organization, coupled with the fact that many organizations do not properly inspect their DNS traffic. Palo Alto Networks' Unit 42 research has found that more than 85% of malware now uses DNS to establish command and control communications.⁵ By obfuscating their actions behind a massive number of legitimate DNS queries, attacker C2 and data exfiltration traffic can remain undetected.

Phishing Tactics Move Beyond Email

Finally, phishing tactics continue to evolve and in many cases have moved beyond the capabilities of email-based security controls. While these attacks may still be delivered via email, they are increasingly propagated via social media or even text messages. Attackers increasingly focus on avoiding detection through web evaluations, rather than crafting realistic-looking emails. They may use new URLs that traditional offline web-crawlers have never seen and quickly cycle through these links over the course of an attack to avoid detection. Additionally, attackers continue to exploit compromised websites that are categorized as good by URL filtering solutions or even include CAPTCHA challenges to confuse web security tools. Similar to Cobalt Strike, these evasions are available in ready-made phishing kits, helping elevate otherwise low-level hackers from nuisance to legitimate threat.

Legacy Tools Cannot Meet These Challenges

There are clearly many considerations organizations weigh when evaluating cybersecurity products. However, the ability to detect and prevent threats is ranked as by far the most important (see Figure 1).⁶ The use of signatures remains important for detecting known, common, and untargeted threats. In fact, most network security tools do a good job at stopping these types of attacks, which is borne out in efficacy tests and comparisons. Yet, where there is less clarity into efficacy is where organizations are often having the most difficulty—advanced, evasive threats.

The use of legitimate software and protocols, near-perfect replications of legitimate websites and application branding, fileless attacks, and cross-vector campaigns makes it incredibly difficult for traditional security tools to detect these

⁴ Source: Palo Alto Networks, [Stop Zero-Day Threat in Zero Time with Nebula](#), February 2022.

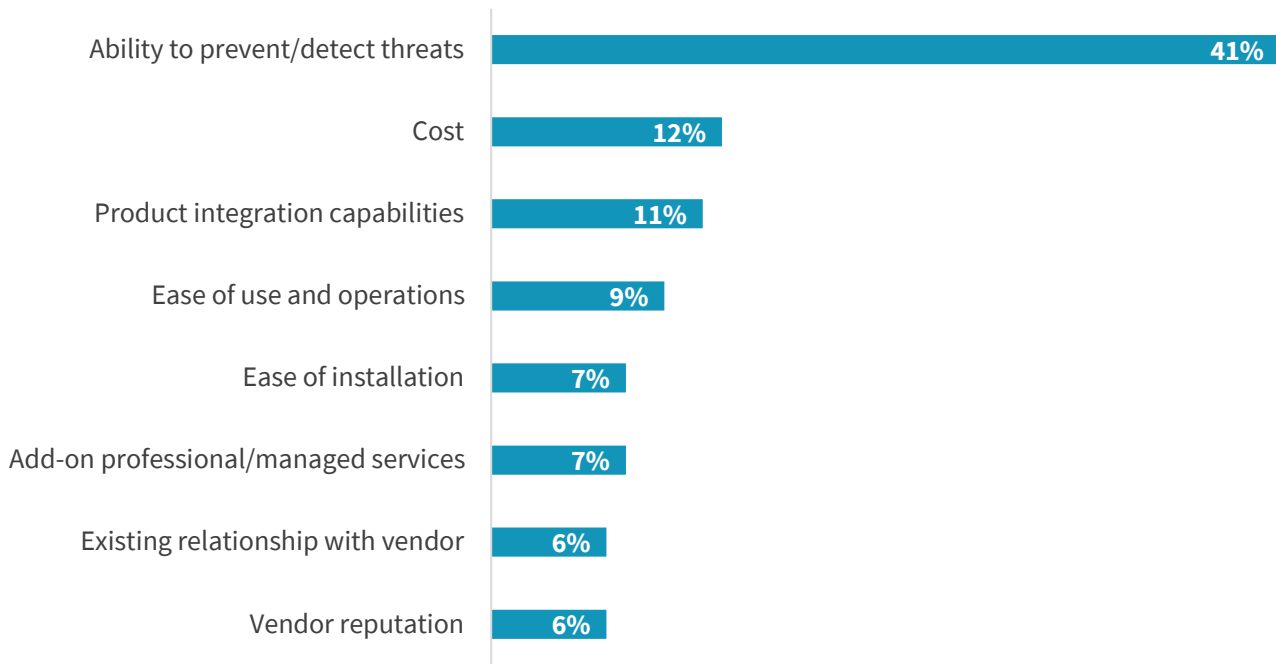
⁵ Source: Palo Alto Networks, [Stop Attackers from Using DNS Against You](#), July 2020.

⁶ Source: ESG Survey Results, [Enterprise-class Cybersecurity Vendor Sentiment](#), March 2020.

modern attacks. Typically, more advanced attacks are identified out-of-band, and signatures are created after the fact to protect organizations from any subsequent attacks. However, this method requires an initial victim and is often circumvented by attackers making small changes in their code or procedures to evade the signature. As a result, many organizations are unprepared to protect themselves in real time against these increasingly evasive attacks.

Figure 1. Top Considerations When Purchasing Cybersecurity Tools

Which of the following product considerations are most important to your organization when purchasing cybersecurity technologies? (Percent of respondents, N=247, percent ranked #1 displayed)



Source: ESG, a division of TechTarget, Inc.

Additionally, the skills shortage continues to be a key issue for many organizations. Responding to incidents after the fact is less than ideal regardless of the circumstance. But organizations struggling with staffing are starting with a disadvantage. Additionally, this directly affects an organization’s ability to efficiently manage a variety of different tools to protect against different attack types. Crafting, maintaining, and updating policies across multiple tools becomes increasingly difficult in this model. The increase of connected IoT devices and attractiveness as a target for attackers only make this issue more critical.

Three Ways to Improve Protection Against Evasive Threats

With threat protection being a key purchase criterion, but evasive attacks making detection much more difficult, what should security teams be looking for when evaluating security tools? While the specific attributes required may vary from one organization to another, there are three key areas that should be prioritized. Specifically, these are:

1. **Utilize advanced machine learning capabilities.** As noted, signature-based and out-of-band detection approaches can no longer keep pace with today’s diverse and dynamic threat environment. As investments around machine learning (ML) and artificial intelligence (AI) have grown and the effectiveness of these models has improved, it logically follows that this should be a significant area of focus for many security teams moving forward. Specifically,

38% of IT and cybersecurity professionals say their organization will purchase, deploy and operate more threat detection tools based upon artificial intelligence/machine learning over the next 12-18 months in order to improve threat detection and response.⁷ Yet not all machine learning provides the same level of effectiveness or efficiency. These models rely on both high-quality and high-quantity data, as well as the ability to be applied in-line to actively block evasive attacks before they can compromise organizational assets.

2. **Ensure coverage across key evasive attack vectors.** Many attacks, even those that are delivered via email, utilize the web in some form. With the rise in remote work and the amount of time knowledge workers spend online, it makes sense that this is an attractive entry point for attackers. The ability to obfuscate their actions by exploiting the sheer scale of the internet as well as commonly used internet protocols only makes attackers that much more likely to focus their efforts here. This makes real-time visibility into web traffic and content critical for any modern web security tool. Further, identifying and preventing attacker communications across channels used for stealth including HTTPS, DNS, and others should be table stakes and allows organizations to prevent an incident from becoming a breach by ensuring data exfiltration can be detected.
3. **Incorporate and automate intelligent management across security tools.** Even if they include advanced machine learning and broad coverage across evasive vectors, security tools will not help organizations be as effective as possible without efficient management. Next-generation firewalls (NGFW) are notorious for requiring extensive rules lists that administrators are afraid to update due to the risk of disrupting the business by blocking access to critical resources. As additional threat prevention capabilities are layered onto these platforms, policy management only becomes more cumbersome. While analytics are imperative to threat detection, tools that apply these capabilities in a management context can help teams ensure that unintentional policy errors do not occur, rules that are no longer relevant are removed, and potential configuration or performance issues are identified before they pose an unanticipated problem. This is especially relevant with regard to IoT devices. Security teams struggle maintaining visibility across the number and types of IoT devices on the network, as well as dynamically applying policy when they do connect. By automating discovery and policy creation via machine learning analytics, teams can ensure the proper controls are in place, preventing attackers from exploiting unknown or unsecured devices.

Palo Alto Networks Provides In-line, Deep Learning-based Protection Against Evasive Threats

Palo Alto Networks has continued to evolve its machine learning capabilities with the introduction of in-line deep learning. Deep learning is a subset of traditional machine learning that uses multi-layer artificial neural networks to move beyond the structured data analysis of machine learning and analyze data more in the way a human would. Whereas machine learning requires data scientists to tell the system what to look for, deep learning does not require feature sets to be defined. Further, while machine learning can plateau in effectiveness once data inputs reach a certain point, deep learning (while requiring a large amount of data to begin with) continues to become more effective as data is added. For these reasons, deep learning is particularly useful from a security perspective in finding new threats and malware variants as compared to machine learning.

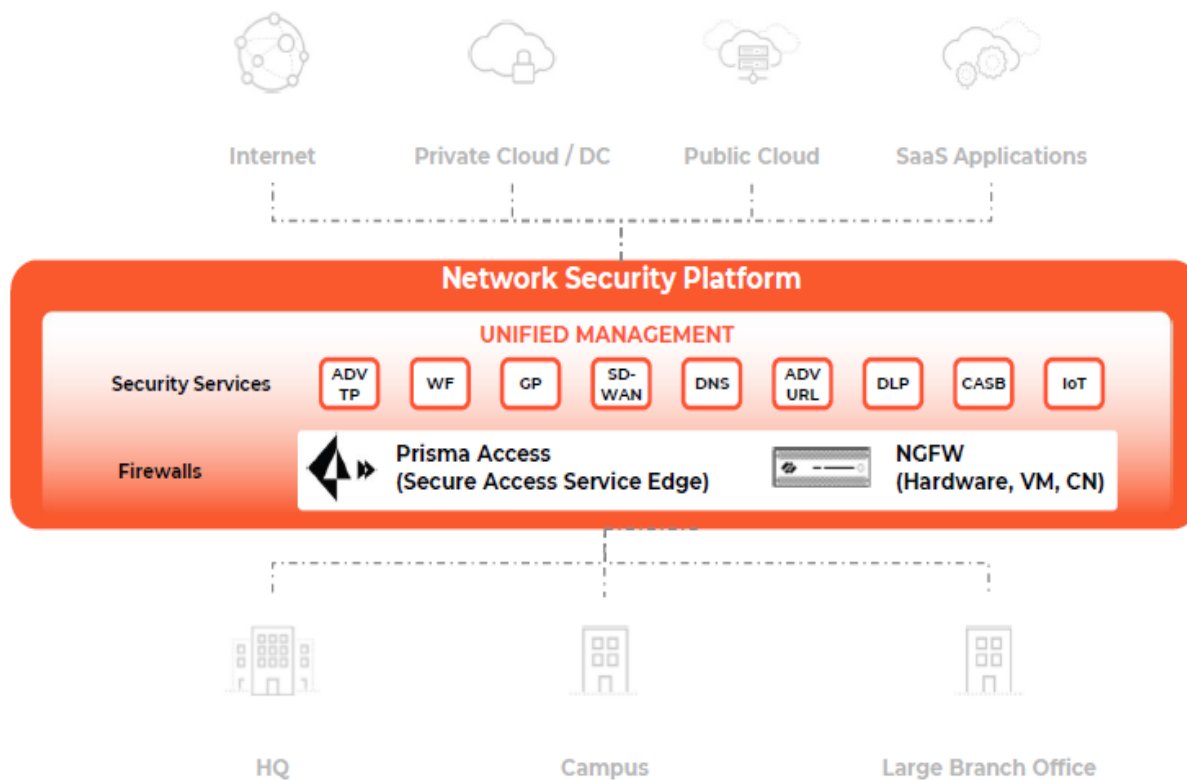
Palo Alto Networks has made deep learning available through enhancements to its Advanced Threat Prevention, Advanced URL Filtering, DNS Security, and IoT Security subscriptions, as well as a new AI Ops capability (see Figure 2). Customers can use these subscriptions in a cloud-delivered model through Prisma Access, through existing hardware and virtual firewalls, as well as two new hardware firewalls, the PA-3400 series and PA-5400 series. By leveraging inline deep learning, Palo Alto Networks can identify unknown command and control traffic, block attacks from tools such as Cobalt Strike, detect attacks

⁷ Source: ESG Survey Results, [The Impact of XDR in the Modern SOC](#), February 2021.

that evade traditional URL databases and web crawlers, and ensure attackers cannot use DNS as an avenue of attack. Some of the specific enhancements to the platform include:

- **Advanced Threat Prevention.** The deep learning capabilities Palo Alto Networks has added to its network security platform are particularly core to its threat prevention capabilities. Its existing intrusion prevention capabilities protect against known malware and command and control traffic. Advanced Threat Prevention takes the wealth of telemetry collected across Palo Alto Networks' global deployments and analyzes it via an in-line, cloud-based deep learning model. The benefit to customers is protection against unknown malware and command and control traffic, encrypted SSL and HTTPS traffic, and unknown-TCP and -UDP applications. This includes evasive command and control traffic from hack tools like Cobalt Strike.
- **Advanced URL and DNS Security.** The Advanced URL Filtering subscription adds additional protections above and beyond what offline web-crawling and URL databases provide by performing real-time, in-line scanning. The subscription analyzes web content being rendered through both static and dynamic analysis, deep recursive analysis, and JavaScript deobfuscation, among other methods. This deeper analysis helps identify advanced phishing techniques that would otherwise bypass traditional web and email security controls. Additionally, DNS Security leverages inline deep learning to detect sophisticated threats that use DNS traffic to cause harm. In addition to blocking known malicious domains, DNS Security conducts deep inspection of DNS traffic to detect dynamic DNS-based threats such as DNS tunneling, compromised DNS Zones, and the use of strategically aged domains—identifying and preventing them in real time. These types of techniques are often used to steal data, launch malware and ransomware, or conduct social engineering attacks.
- **AIOps for NGFW and IoT Security.** To improve firewall health and management, Palo Alto Networks has introduced AIOps for NGFWs. This subscription helps organizations improve their security posture by providing best practice recommendations from Palo Alto Networks subject matter experts. Additionally, AIOps for NGFW helps teams prevent business disruptions by maintaining optimal firewall health and performance through ML-powered predictions. From an IoT perspective, Palo Alto Networks has added ML capabilities to help customers optimize protection and management of their connected device security. The IoT Security subscription provides visibility and discovery for IoT devices; protection against known and unknown threats; prescriptive, least-privilege policy recommendations to support zero trust strategies; and simplified deployment through flexible traffic capture with ERSPAN. This last enhancement is particularly noteworthy, as it enables teams to collect all traffic from one switch port, eliminating the need to deploy multiple sensors across each network segment.

Figure 2. Palo Alto Networks' Network Security Platform



Source: Palo Alto Networks

The Bigger Truth

Cybersecurity has been a cat-and-mouse game for years. Attackers change their tactics, security vendors move to update defenses, rinse, repeat. Unfortunately, cyber-criminals are motivated, funded, and have access to many of the same tools and technologies security teams use to protect themselves, continuously putting organizations on the defensive.

AI/ML can be overused in security marketing—but it has generated interest for good reason. The promise of incorporating these analytics engines into cybersecurity tools is not only to truly close the gap with attackers, but to potentially keep it closed for more than a fleeting instant. The importance of deep learning is enabling these protections to occur in real time and grow in effectiveness as more data is collected. Palo Alto Networks is leveraging the wealth of threat data it sees on a daily basis to power these models and deliver advanced protections against evasive threats. As these types of attacks continue to grow in prevalence, any organization investigating alternatives to signature-based and out-of-band detection approaches should explore Palo Alto Networks.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188