SecureIQlab®

Command & Control Prevention: SecureIQLab CyberRisk Comparative Security Vendor Report

TEST PERIOD: JULY 2022—DECEMBER 2022

PUBLISHED: 6 SEPTEMBER 2023

COMMISSIONED BY: PALO ALTO NETWORKS

www.secureiqlab.com

Report Contents:

1. Executive Summary

SecureIQLab tested the ability of nine popular cybersecurity solutions to protect against command-and-control attacks. Testing was executed from Q3 through Q4 of 2022. Six of these solutions were Next-Generation Firewall (NGFW), on-prem & virtual appliance. These include solutions from Checkpoint, Cisco, Fortinet, and Palo Alto Networks. The remaining three solutions tested were Security Service Edge (SSE) based cloud solutions from Cisco, Palo Alto Networks, and Zscaler. All products were tested to block the command-and-control capabilities of the Cobalt Strike attack suite. The test methodology measured the block rate of the tested NGFW & SSE solutions against Cobalt Strike in multiple attack scenarios.

From the results of these tests, SecureIQLab concludes Palo Alto Network's machine learning approach against Cobalt Strike Adversary Emulation Suite provides superior protection in both NGFW and SSE solution categories with competitive threat mitigation efficiency.

Table 1 shows the *Overall Block Rate* for the Next-Generation Firewall (NGFW) & Security Service Edge (SSE) solutions tested:

Cobalt Strike Command-and-Control	**Vendors and Products**								
	Cisco		**Checkpoint**	**Palo Alto Networks**			**Fortinet**		**Zscaler**
	Umbrella SIG Essentials **SSE** Solution	Firepower 4110 **NGFW** Solution	SG5100 **NGFW** Solution	Prisma Access Enterprise **SSE** Solution	PA-460 **NGFW** Solution	PA-VM-Flex **NGFW** Solution	FG-301E **NGFW** Solution	FG-VM04V **NGFW** Solution	ZIA Transformation Bundle **SSE** solution
Overall Block Rate	**16.7%**	**13.3%**	**18.9%**	**99.2%**	**99.1%**	**99.1%**	**20.%**	**20.0%**	**15.7%**

Table 1: Overall Block Rate Results.

2. Introduction

Command-and-control[1] ("C2") attacks include implants that report back to the attacker's server. The attacker's server, in turn, issues commands to a compromised machine. A compromised machine will carry out the commands from the attacker's server and may install additional software. This can be leveraged into the complete control of the compromised machine and pivoting to attack other hosts in the environment. Figure 1 illustrates where command-and-control attacks fit within the Lockheed Martin's Cyber Kill Chain.

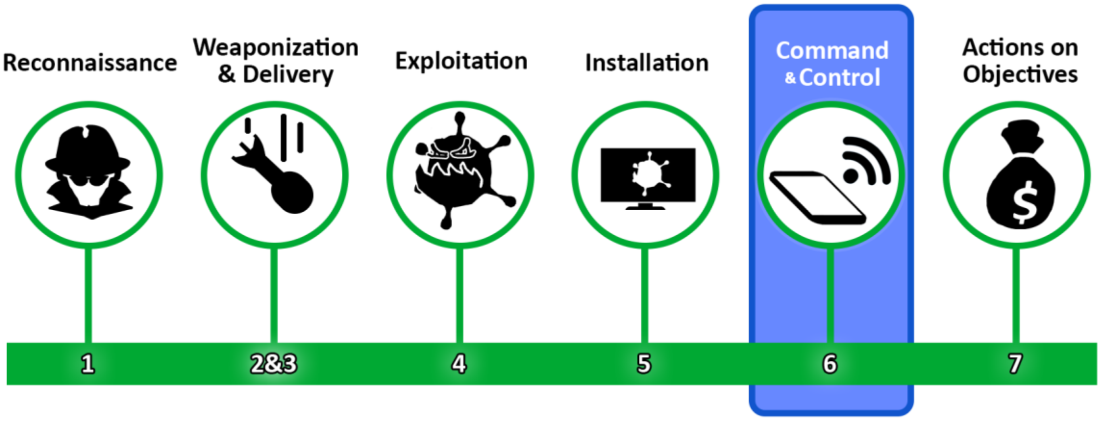


Figure 1: Position of Command and Control in the Lockheed Martin Cyber Kill Chain®.

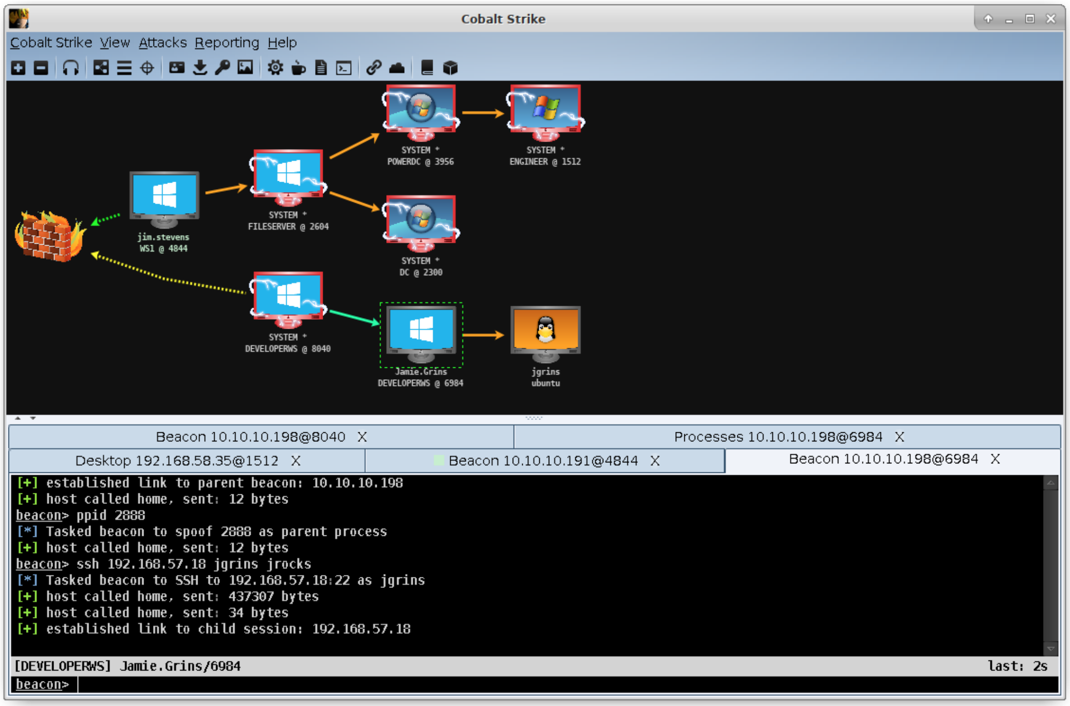
Cobalt Strike is a commercial command-and-control attack suite now owned by Fortra (formerly HelpSystems). According to the Fortra website, Raphael Mudge created the Cobalt Strike command-and-control framework in 2012 to assist red teams in testing enterprise defense postures against post-exploitation activity.

The Cobalt Strike GUI makes it very easy to use by even unsophisticated hackers. Access to this commercial tool has historically been highly restricted; however, cracked versions have recently become available. As a result, Cobalt Strike has become a favorite post-exploitation framework for threat actors[2] and a force that security providers must reckon with.

Attackers using Cobalt Strike can change many settings using malleable C2 profiles. In the wild, there has been a proliferation of publicly available malleable C2 profiles that can be used to evade detection by security products. Researchers have also created and shared tools to generate new randomized Cobalt Strike profiles easily.

[1] https://attack.mitre.org/tactics/TA0011/

[2] https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf.



```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18

[DEVELOPERWS] Jamie.Grins/6984                                      last: 2s
beacon>
```

Figure 2: Official Screenshot of Cobalt Strike GUI from https://www.cobaltstrike.com/screenshots/.

This test did not cover all of Cobalt Strike's capabilities. Instead, it was limited to testing NGFW and SSE solutions' ability to block Cobalt Strike's network callback functions using HTTP and HTTPS. Figure 2 highlights the intuitive nature of Cobalt Strike's interface.

To provide detection of command-and-control network activity between a "team server" and "beacon" (the Cobalt Strike attack server and the implant, respectively), network security products typically utilize traditional IPS signatures to match against specific static strings and patterns unique to Cobalt Strike. However, these signatures can be easily evaded with malleable profiles that can create endless combinations of the content that may have been used as Cobalt Strike "fingerprints" in creating static IPS signatures. To combat this, in addition to traditional IPS signatures, Palo Alto Networks has launched its Advanced Threat Prevention service that detects and blocks these modifications to typical command-and-control traffic in real-time. This command-and-control prevention SecureIQLab CyberRisk report is derived from the test results of both the Next-generation firewall (NGFW) & Security Service Edge (SSE) command-and-control commissioned comparative tests conducted by SecureIQLab.

Palo Alto Networks commissioned these tests to measure the value of their Advanced Threat Prevention capability compared to other leading security NGFW and SSE solutions in protecting customers against Cobalt Strike command-and-control network activity. This report is intended to indicate protection not only against Cobalt Strike's basic/standard command-and-control network activity but also to evaluate the relative resiliency of the protection provided by each product when modifications are made to evade detection.

This report is not intended as a how-to manual for hacking these products. Therefore, we omit or redact specific details of attacks.

3. Test Environment

Cobalt Strike versions 4.7.2 (SSE test) and 4.6.1 (NGFW test) were used in these tests with Debian 5.16.18-1 & 5.15.15-2kali1 (2022-01-31) kernel versions used as the platform to host Cobalt Strike's team server. On the attack side, the Cobalt Strike team server was hosted on the public internet.

The following solutions and firmware/software versions were tested:

Security Service Edge (SSE) Solutions:

Prisma Access Enterprise:	Prisma Access 3.2
Cisco Umbrella SIG Essentials:	Umbrella SIG Essentials
Zscaler ZIA Transformation Bundle:	ZIA 6.2

Next-Generation Firewall (NGFW) Solutions:

Checkpoint:	SG5100 vR81.10 HF T66 (Hardware)
Cisco:	Firepower 4110 v7.2.0 (Build 82); VDB 357 (Hardware)
Fortinet:	FG-301E v7.2.1build1254(Feature) (Hardware)
	FortiGate VM04V v7.2.1build1254(Feature) (Virtual)
Palo Alto Networks:	PA-460 v10.2.2 (Hardware)
	PA-VM-Flex v10.2.2-h1 (Virtual)

Prior to testing, all products' firmware were updated, and dynamic security content updates were configured/allowed to happen. Content that updated automatically, for example IPS signatures, continued to be updated during the test.

High-security policies suitable for deployment in a typical enterprise environment were created for all available and applicable security functionality (e.g., DNS Security, Antivirus/Sandboxing, URL Filtering, Application Control, IPS/Vulnerability Protection, SSL/decryption). Because there were subtle differences in the product settings, URL Filtering and Application Control policies were matched up as closely as possible across all products.

Publicly available best-practice documentation and admin guides for each product were referred to confirm that all products were at least minimally configured to best-practice specifications for all security features/modules ("best-practice or better"). For instance, on some vendor policy configurations, the default policy was modified to ensure consistency in the evaluation of all the vendors per the test methodology. Because product performance is generally highly configuration-dependent, results might differ if different settings had been used for any of the products tested. True positive testing was then performed to confirm the functionality of all configured security policies.

False positive testing was also performed as needed to conservatively tune the policies to what would be appropriate/acceptable for a typical enterprise. For example, the ability to browse to and render general popular websites (e.g., Amazon, Bing, CNN, MSNBC, and Wikipedia) was tested. Additionally, false positive testing included websites closely mirroring those used in various Cobalt Strike profiles through the product as configured.

4. Cobalt Strike Scenarios Tested & Validation Procedure

The overall command-and-control test procedure included five main categories of attack scenarios executed using the Cobalt Strike attack framework. Each of the five categories examines a major aspect of a product's capabilities in a specific real-world scenario. HTTP over TCP port 80 was used for command-and-control communication unless otherwise noted. For each profile tested, a stageless implant/beacon was generated and delivered to the "victims" for execution out-of-band prior to testing. In other words, only the product's capability to intervene and protect against Cobalt Strike callback network activity was tested, not the ability to block the initial delivery of the beacon itself; exploitation and delivery of the beacon are assumed to have already taken place.

The types of attacks evaluated were:

1. **Basic Attack Scenario:** This test was performed to evaluate the product's basic protection against the most commonly available public attack profiles attempting data exfiltration and malware delivery via HTTP. The basic attack scenario included three subcategories: Normal, Crimeware, and APT. Each scenario had a multitude of profiles that were evaluated as a part of the Cobalt Strike attack framework.

2. **Random Attack Scenario:** This test was performed to evaluate the protection when Cobalt Strike is leveraged to generate "randomized" attack scenarios using tools that are part of the Cobalt Strike arsenal of researchers and the public. This randomization increases the probability that the traditional threat defenses of security solutions might be rendered ineffective against data exfiltration and malware delivery.

3. **Custom Attack Scenario:** This was the first of the confirmation tests, which used a smaller profile set. This test was performed using purposely chosen and modified attacks from the Basic and Random attack scenarios. The modifications were made to attacks that were previously blocked to confirm whether the modifications would be sufficient to bypass the defenses. Modifications were made on the different variables that supported customization.

4. **Non-Standard ports-based Attack Scenario:** The purpose of this testing was to confirm if the security solutions would continue to provide protection when attacks use HTTP over a non-standard port.

5. **HTTPS Attack Scenario:** The purpose of this testing was to confirm if the products under test provided the same level of protection when attacks are delivered via HTTPS rather than HTTP.

The test scenarios did not have equal sample sizes. The Custom Attack Scenario, Nonstandard Ports-based Attack Scenario, HTTPS Ports-based Attack Scenario were verification exercises. Thus, they did not require many profiles. As a result, most profiles were run in the Basic Attack and Random Attack Scenarios.

It is possible to block some of these command-and-control attacks on the Domain Name System (DNS) and Uniform Resource Locator (URL) level. However, threat actors can seed these domains/URLs for a long time to make them appear legitimate, and thus the entire attack might bypass these protections. Thus, for this test, these capabilities were disabled should they be responsible for a block. That is, to simulate seeding, in some cases the products under tests' DNS and/or URL protections were disabled (e.g., newly observed domain category was set to monitor rather than block). In graphs, where a vendor's two products had the same results, results are presented by vendor rather than by product.

Products under test earned blocking credit in two ways: First, by stopping the Cobalt Strike attack at the communication stage, and second, by blocking the attack at the exfiltration and download stage.

The communication stage is when the compromised machine checks in with the Cobalt Strike Team Server and command-and-control is established. Blocking credit at the communication stage was earned by preventing the command-and-control link from being established.

The exfiltration and download stage are when the compromised machine sends out data or downloads malware, as directed in the communication stage. Blocking credit at the exfiltration and download stage was earned by blocking the exfiltration of system data (output of command output, e.g., 'whoami /all'), blocking output of one or more screenshots, and preventing the download of malware. At least one stage of the malicious traffic needed to be blocked to earn blocking credit at the exfiltration and download stage.

Some graphs differentiate between blocking credit at the communication stage and blocking credit at the exfiltration and download stages. Where blocking credit is not differentiated, blocking credit was given for blocking at either stage.

5. Overall Block Rate

The *Overall Block Rate* is intended to give a general overview of the capability of products under test to withstand, absorb, and mitigate variations in Cobalt Strike profiles generated via different tools and third-party maintained profiles. It includes the results from all the variations of attacks conducted. The *Overall Block Rate* is an unweighted calculation. Equation 1 demonstrates the calculation of the *Overall Block Rate* by dividing the total number of attacks blocked by all the attacks launched and multiplying by 100%.

$$\begin{array}{c} Overall \\ Block\ Rate \end{array} = \left(\frac{blocked\ attacks}{total\ attacks} \right) \times 100\%$$

Equation 1: Formula for Computation of Overall Block Rate.

The higher the *Overall Block Rate*, the better the product's ability to withstand attacks. In both the tests, the product's responses to an average 477 attacks were evaluated.

Cobalt Strike Command-and-Control	**Vendors and Products**								
	Cisco		**Checkpoint**	**Palo Alto Networks**			**Fortinet**		**Zscaler**
	Umbrella SIG Essentials **SSE** Solution	Firepower 4110 **NGFW** Solution	SG5100 **NGFW** Solution	Prisma Access Enterprise **SSE** Solution	PA-460 **NGFW** Solution	PA-VM-Flex **NGFW** Solution	FG-301E **NGFW** Solution	FG-VM04V **NGFW** Solution	ZIA Transformation Bundle **SSE** solution
Overall Block Rate	**16.7%**	**13.3%**	**18.9%**	**99.2%**	**99.1%**	**99.1%**	**20.0%**	**20.0%**	**15.7%**
Communication stage	15.5%	11.2%	17.0%	95.8%	97.8%	97.4%	16.6%	16.6%	7.63%
Additional Exfiltration and download stage	1.2%	2.2%	1.9%	3.4%	1.3%	1.7%	3.4%	3.4%	8.0%

Table 2: Table of Overall Block Rate Results by Block Stage.

The *Overall Block Rate* is only a general overview because not all attacks are equal: The composition of the various Cobalt Strike attacks targeting a given network may vary from the composition of the profiles in this test. Table 2 provides greater details into the *Overall Block Rate* by stage. While Figure 3 below provides a graphical representation of this data.

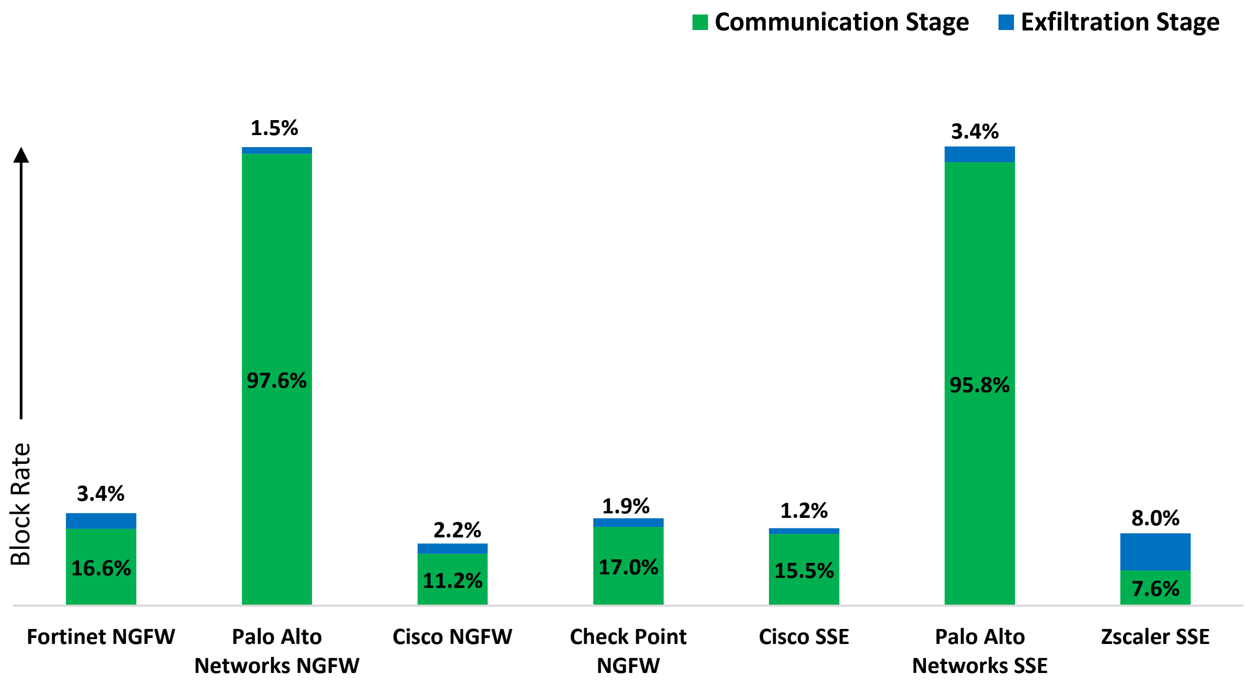


Figure 3: Overall Block Rate Results by Block Stage.

6. Attack Scenario Analysis

This section provides a breakdown of results by category. As such, it provides a more detailed analysis of the tested product's performance than the *Overall Block Rate*.

The summary of key results below shows how the five security vendors fared during our validation across five main categories of attack scenarios using the Cobalt Strike attack framework. This validation was performed alongside false positive validation during the entire test period. In all cases, results are reported using the unweighted percentages of attacks blocked. Example calculation for percentage of attacks blocked shown below in Equation 2.

$$\begin{matrix} \textit{Percentage of} \\ \textit{attacks blocked} \end{matrix} = \left(\frac{\textit{blocked attacks}}{\textit{total attacks}} \right) \times 100\%$$

Equation 2: Formula for Computation of Percentage of Attacks Blocked.

Attack scenarios are broken down into five categories: The *Basic Attack Scenario*, the *Random Attack Scenario*, the *Custom Attack Scenario*, the *Non-standard Ports Attack Scenario*, and the *HTTPS-based Attack Scenario*. Each is discussed in greater detail in the following sections. Table 3 below contains the test results for the five categories for each vendor and Figure 4 illustrates this data graphically.

Cobalt Strike Command-and-Control	Vendors and Products								
	Cisco		Checkpoint	Palo Alto Networks			Fortinet		Zscaler
	Umbrella SIG Essentials **SSE** Solution	Firepower 4110 **NGFW** Solution	SG5100 **NGFW** Solution	Prisma Access Enterprise **SSE** Solution	PA-460 **NGFW** Solution	PA-VM-Flex **NGFW** Solution	FG-301E **NGFW** Solution	FG-VM04V **NGFW** Solution	ZIA Transformation Bundle **SSE** solution
Basic Attack Scenario	16.9%	26.0%	47.3%	100.0%	99.7%	99.7%	36.7%	36.7%	44.1%
Random Attack Scenario	12.9%	2.0%	3.0%	100.0%	99.0%	99.0%	10.0%	10.0%	2.9%
Custom Attack Scenario	33.3%	14.3%	28.6%	66.7%	85.7%	85.7%	14.3%	14.3%	41.7%
Non-Standard Ports Attack Scenario	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	16.7%	16.7%	75.0%
HTTPS-based Attack Scenario	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 3: Overview Block Rate by Attack Scenario Category.

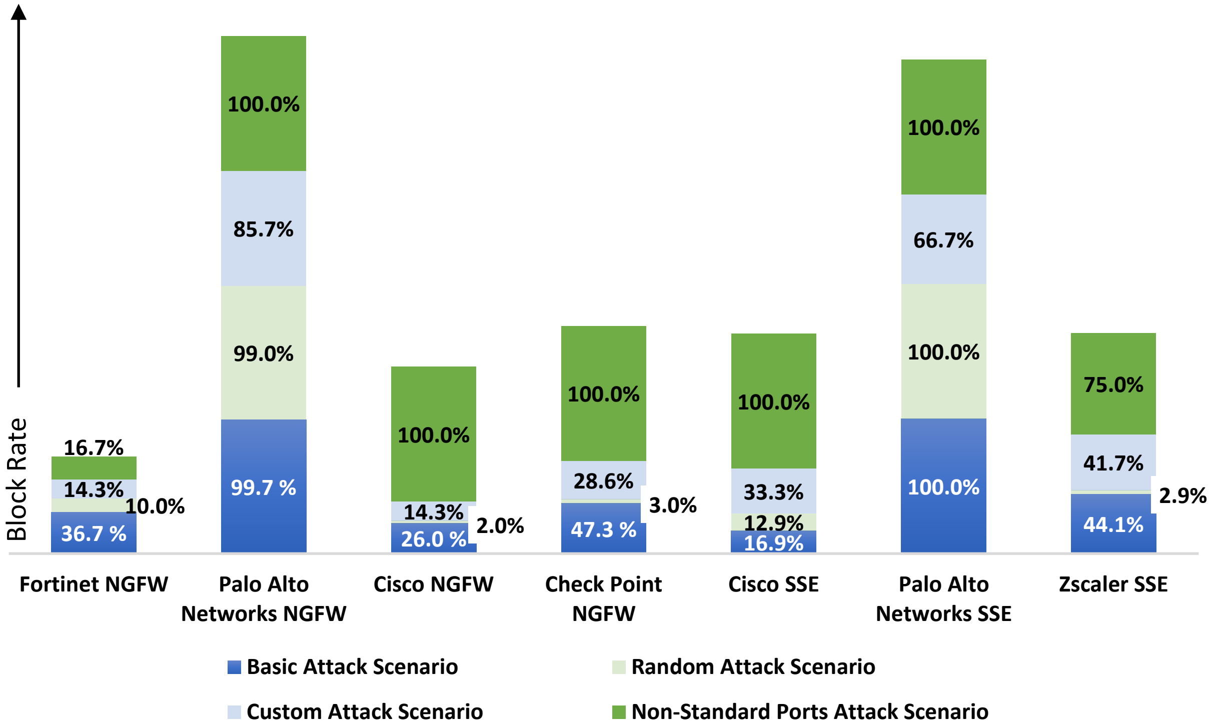


Figure 4: Overview Block Rate by Attack Scenario Category

7. Threat Mitigation Efficiency Comparative Analysis

The *Threat Mitigation Efficiency Score* is intended to measure the ability of the product to identify and respond to the threat campaigns that were delivered as a part of the Cobalt Strike testing. The appropriate response and mitigation capabilities of the different solutions were measured to understand how the products under test help improve the overall risk posture and the security efficacy of the organization. It was measured by factoring in the ease of tuning the solution against Cobalt Strike attacks, the solution's attack response intuitiveness from a policy and security configuration perspective, the comprehensiveness of the data and the enhanced reporting capabilities, and the ease of using data it generates to provide an effective threat detection & response. Threat mitigation efficiency was determined for five different categories: Simplicity of attack mitigation tuning specific to Cobalt Strike-based threats, speed to tune and respond which makes it easier to detect and respond to command-and-control based threats, intelligence-driven attack response, customizable analytics dashboard, and enhanced mitigation-centric reporting. During analysis, each of these products were rated high (10 points), medium (6 Points) or a low (3 points) score accordingly.

- **Attack Mitigation Tuning Efficacy:** Ability to tune the firewall effectively against known and on-going attacks from the Cobalt Strike framework was one of the key metrics that was factored into the overall threat mitigation metric. Business requirements should be in alignment with the environment being used. Scoring for this category was performed as follows:
  - **High (10 points):** Solution has multiple ready-to-use canned, pre-set configuration policies, response-based signatures, or tuning based on certain key indicators present. Solutions should be able to address different business requirements in line with the attacks resulting from Cobalt Strike with automated deployment models with zero-to-very minimal professional intervention.
  - **Medium (6 points):** Solution has some ready-to-use canned, pre-set configuration policies, response-based signatures, or tuning based on certain key indicators. Solutions should be able to address different business requirements in line with the attacks resulting from Cobalt Strike with semi-automated deployment models with medium professional intervention.
  - **Low (3 Points):** Solution does not have ready-to-use, canned, pre-set response policies, response-based signatures, or tuning based on certain key indicators. Solutions are extremely manual in nature to address different business requirements in line with the attacks resulting from Cobalt Strike with manual deployment models with maximum professional intervention.
- **Speed to Tune and Respond:** This goes directly to the time taken to identify, detect and respond to threats from Cobalt Strike framework. Scoring was based on the solutions capability around the following three criteria:
    - Time-to-detect and alert on attacks.
    - Time to notify and have a response and mitigation (or a recommendation) in place.
    - The quality of mitigation and post-attack mitigation reliability.
  - **High (10 points):** Solution can showcase all the 3 highlighted metrics above end-to-end.
  - **Medium (6 Points):** Solution can showcase at least 2 of highlighted metrics above end-to-end.
  - **Low (3 Points):** Solution can showcase at least 1 of the highlighted metrics above end-to-end.

- **Intelligence-Driven Attack Response:** This applies directly to the core of the solutions response strategy with minimal intervention and simplified workflows. Scoring was based on the solutions capability around the following:
    - **High (10 points):** Consolidated high-level summary (single pane of glass) of the threat workflow, and view of a set of command and control-based attack campaigns/profile/threats that are easily categorized (intuitively) to take bulk-actions around effective response or mitigation plan. Ability to take a proactive response-centric approach is integral to the intelligence-driven model.
    - **Medium (6 Points):** Distributed view of attack campaigns/profile/threats that are easily categorized (intuitively) with some level of bulk operational capabilities around the effective response or mitigation plan with basic intelligence built-in around proactive response.
    - **Low (3 Points):** No categorization of attack campaigns/profile/threats (intuitively) with no or missing bulk operation capabilities around the effective response or mitigation plan.
- **Customizable Analytics Dashboard**: This evaluates how customizable the product's dashboard is and whether it allows the customer to choose and represent both the data and incident of interest visually. The threat analytics dashboard should also give the investigators the customization capabilities on-demand and the ability to integrate the data via multiple operational streams.
    - **High (10 points):** There is a highly customizable widget-driven dashboard that allows the customer to choose both the data presented and how that data is represented visually (e.g., pie chart, xy plot, bar graph, and so forth). This also provides enhanced API functionality to integrate with third party Power BI or other third-party data visualization platforms.
    - **Medium (6 Points):** The product provides some level of API out of the box to integrate with third party data visualization platforms such as Power BI. The product had a widget-driven dashboard that allows customers to choose the data but does not allow the customer to choose how the data is represented visually.
    - **Low (3 Points):** Only the default dashboard was available with no API integration.
- **Enhanced Mitigation-centric Reporting**: This enables the solutions to require a proactive mitigation approach to the Cobalt Strike-based attacks that answers critical questions like: Which threat actors are most likely to cause an impact in my organization, possible motivation and goals, attack surface, and C2 prevention capabilities with actionable countermeasures that be deployed to improve my organization's cyber defense capabilities.
    - **High (10 points):** Solution can showcase Cobalt Strike threat notification with context, attack source and timelines with deep dive into each attribute and artifact of the attack. Present product configuration/vulnerabilities on a unified dashboard with the ability to recommend and advise response/mitigation actions to be taken. Having the ability to identify, alert with search capabilities and give the ability to remediate suboptimal product configurations and conditions.
    - **Medium (6 Points):** Cobalt Strike threat notification with information such as minimum of IP, hostname, geolocation, time, threat disposition with some basic information around why an attack was classified as a threat. Attacks may be searched and filtered via date and other fields with some level of graphical representation, advisory and recommendations.
    - **Low (3 Points):** Cobalt Strike basic threat notification with the ability to search and filter attacks and threats via date and other fields. Minimal graphical representation that is specific to those

attacks with no advisory and recommendations. No alert capabilities on suboptimal product configuration or conditions or to act.

$$\begin{matrix}\textit{Threat Mitigation}\\ \textit{Efficiency Score}\end{matrix} = \frac{\left(\begin{matrix}\textit{Attack Mitigation}\\ \textit{Tuning Efficacy}\end{matrix} + \begin{matrix}\textit{Speed to Tune}\\ \textit{and Respond}\end{matrix} + \begin{matrix}\textit{Attack}\\ \textit{Response}\\ \textit{Intelligence}\end{matrix} + \begin{matrix}\textit{Customizable}\\ \textit{Analytics}\\ \textit{Dashboard}\end{matrix} + \begin{matrix}\textit{Enhanced}\\ \textit{Mitigation-}\\ \textit{Centric}\\ \textit{Reporting}\end{matrix}\right) \times 100\%}{50}$$

Equation 3. Threat Mitigation Efficiency Score Calculation

As shown by Equation 3, the *Threat Mitigation Efficiency Score* was calculated by adding the points awarded for each subcategory, then dividing this number by the maximum potential points (50) and multiplying that number by 100%.

Cobalt Strike command-and-Control	Vendors and Products								
	Cisco		Checkpoint	Palo Alto Networks			Fortinet		Zscaler
	Umbrella SIG Essentials **SSE** Solution	Firepower 4110 **NGFW** Solution	SG5100 **NGFW** Solution	Prisma Access Enterprise **SSE** Solution	PA-460 **NGFW** Solution	PA-VM-Flex **NGFW** Solution	FG-301E **NGFW** Solution	FG-VM04V **NGFW** Solution	ZIA Transformation Bundle **SSE** solution
Attack Mitigation Tuning Efficacy	Low	Low	Medium	High	High	High	High	High	Medium
Speed to Tune and Respond	Medium	Medium	Medium	High	Medium	Medium	Medium	Medium	Medium
Intelligence-Driven Attack Response	Medium	Medium	Medium	High	Medium	Medium	Medium	Medium	Medium
Customizable Analytics Dashboard	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Enhanced Mitigation-Centric Reporting	Medium	Medium	High	High	High	High	Medium	Medium	High

Table 4: Threat Mitigation Efficiency Results.

As the above Table 4 shows, all participating vendors had some level of medium-to-high threat mitigation efficiency capabilities. The overall *Threat Mitigation Efficiency Scores* were at 68% for Fortinet's two offerings, the FG301E and the FG-VM04V alongside Zscaler ZIA Transformation Bundle and Check Point SG5100. Cisco Firepower 4110 and Umbrella SIG Essentials were close behind at 54% efficiency, while the Palo Alto Networks Prisma Access Enterprise Solution was at the head of the pack with an efficiency rating of 92% while the other 2 Palo Alto Networks PA-460 and PA-VM-Flex series receiving a 76% *Threat Mitigation Efficiency Score*.

8. CyberRisk Comparative: Overall Block Rate vs Threat Mitigation Efficiency

Figure 5 puts everything together. It is a visual comparison of how the *Overall Block Rate* relates to the *Threat Mitigation Efficiency Score*. The graph splits the products into 3 categories. This split is shown by curved blue ripples.

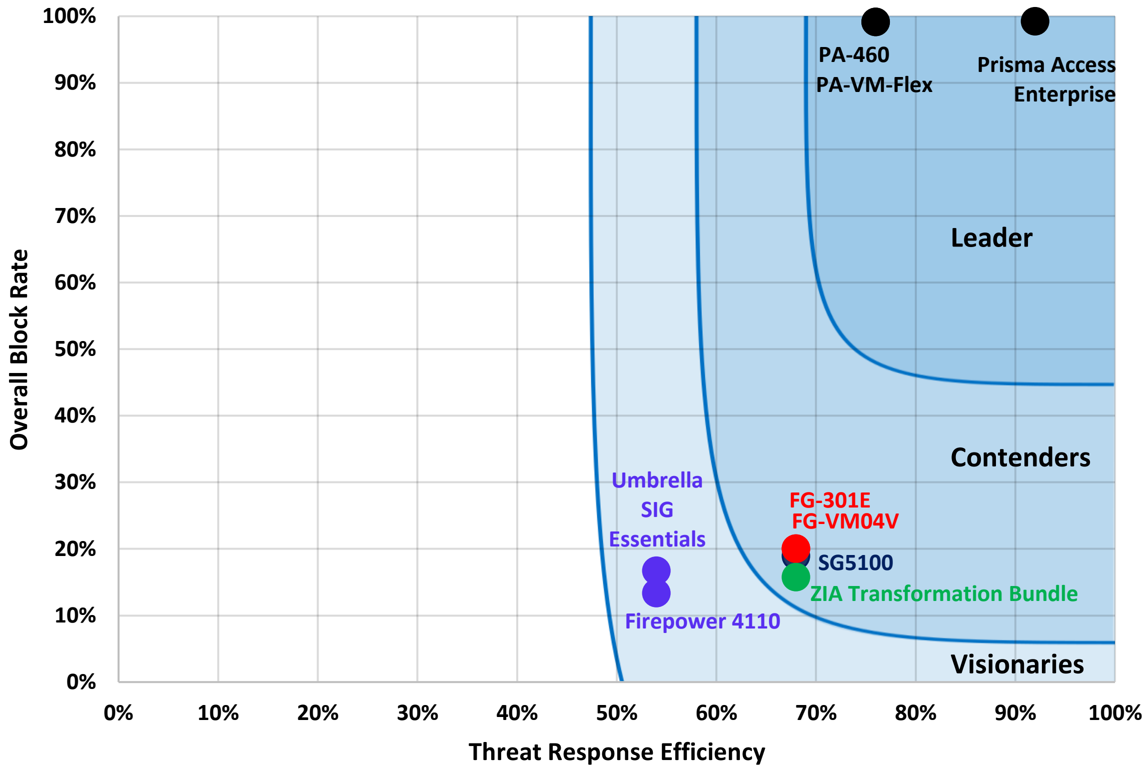


Figure 5: Overall Block Rate versus Threat Mitigation Efficiency Score Ripple

The three categories for *Overall Block Rate* versus *Threat Mitigation Efficiency Score* Ripple are derived from the results of the *Overall Block Rate* and the *Threat Mitigation Efficiency Scores*. These three categories are:

Leaders: These NGFW or SSE products demonstrate equal to or greater than average *Overall Block Rate* and *Threat Mitigation Efficiency Score.*

- Palo Alto Networks Prisma Access Enterprise
- Palo Alto Networks PA-460 and PA-VM-Flex

Contenders: These NGFW or SSE products demonstrate an *Overall Block Rate* and *Threat Mitigation Efficiency Score* that are less than average and greater than the average *Overall Block Rate* minus one standard deviation and average *Threat Mitigation Efficiency Score* minus one standard deviation.

- Fortinet FG-301E and FG-VM04V
- Check Point SG5100
- Zscaler ZIA Transformation Bundle

Visionaries: These NGFW or SSE products demonstrate an *Overall Block Rate* and *Threat Mitigation Efficiency* Score that are less than the average *Overall Block Rate* minus one standard deviation and average *Threat Mitigation Efficiency Score* minus one standard deviation and greater than the average *Overall Block Rate* minus two standard deviations and average *Threat Mitigation Efficiency Score* minus two standard deviations.

- Cisco Umbrella SIG Essentials and Firepower 4110

The above graph shows how Palo Alto Network's *Overall Block Rate* and *Threat Mitigation Efficiency* Score rises above the pack.

9. Conclusion

In the Cobalt Strike attack suite tests we performed, the Palo Alto Networks Next Generation Firewall as well as SSE solutions were top performers or tied for top performance in block rate while also providing highest threat mitigation efficiency.

Reviewing the results of the tests in sequence, the Palo Alto Networks SSE we tested performed better than the SSE competition in the Basic Attack Scenario. The Palo Alto Networks SSE managed to block 99.2% of attacks, while the next best performance was Cisco's SSE at 16.7%. In the Random Attack Scenario, Palo Alto Networks' SSE blocked 100.0% of attacks. The next best performance was from Cisco's SSE, this time at 12.9% blocked.

Turning to the confirmation tests, in the Custom Attack Scenario, the Palo Alto Networks SSE blocked 66.7% of attacks. The next best performance was from the Zscaler's SSE, which blocked 41.7% of attacks. The SSE of Palo Alto Networks and Cisco blocked 100% of attacks in the Non-standard ports Attack Scenario while Zscaler achieved 75%. The SSE of Palo Alto Networks and Zscaler continued to block HTTPS-based attacks that were previously tested using HTTP, while Cisco did not. The results indicate that Cisco's SSE doesn't have full SSL decryption ability.

Going through the results of the tests in sequence, starting with the on-premises products to the cloud-centric solutions, the Palo Alto Networks firewalls we tested performed better than the competition in the Basic Attack Scenario. The Palo Alto Networks firewalls managed to block 99.4% of attacks, while the next best performance was Checkpoint's firewall at 37.2%. In the Random Attack Scenario, Palo Alto Networks' firewalls blocked 99.0% of attacks. The next best performance was from Fortinet's firewalls, this time at 10.0% blocked.

Turning to the confirmation tests, in the Custom Attack Scenario the Palo Alto Networks firewalls each blocked 85.7% of attacks. The next best performance was from the Checkpoint firewall, which blocked 28.6% of attacks. The firewalls of Palo Alto Networks, Cisco, and Checkpoint all blocked 100% of attacks in the Nonstandard Ports Attack Scenario. All firewalls continued to block HTTPS-based attacks that were previously tested using HTTP. In the Hostname Change Scenario, only the Palo Alto Networks firewalls blocked attacks.

Finally, there was less variance in *Threat Mitigation Efficiency Score*, an indication that differentiation via interface is not as broad as the differentiation via *Overall Block Rate*.

Overall, Palo Alto Networks performed well against the Cobalt Strike attack profiles tested. Palo Alto Networks Prisma Access Enterprise was the *Overall Block Rate* vs. *Threat Mitigation Efficiency Score* Leader. Compared with the other products tested, Palo Alto Network's Advanced Threat Prevention capability outperformed the competition by a significant margin in most of the Cobalt Strike tests we executed. The large difference in performance in *Overall Block Rate* was what propelled the Palo Alto Networks Prisma Access Enterprise into leader status.

10. Appendix

Product Staging

The following documentation was referred to during product configuration:

Zscaler

- https://help.zscaler.com/zia/recommended-ips-control-policy
- https://help.zscaler.com/zia/recommended-malware-protection-policy
- https://help.zscaler.com/zia/recommended-advanced-threat-protection-policy
- https://help.zscaler.com/zia/recommended-sandbox-policy
- https://help.zscaler.com/zia/recommended-url-cloud-app-control-policy
- https://help.zscaler.com/zia/recommended-file-type-control-policy

Cisco

- https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/umbrella-design-guide.pdf

On page 81, in the above linked document, Cisco recommends disabling intelligent proxy if you have Web Policy enabled.

- https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720.html
- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72.html
- https://secure.cisco.com/secure-firewall/v7.2/docs

Palo Alto Networks

- https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/create-prisma-access-policy/best-practices
- https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices

Checkpoint

- https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111303&partition=Basic&product=All
- https://sc1.checkpoint.com/documents/Best_Practices/IPS_Best_Practices/CP_R80.10_IPS_Best_Practices/html_frameset.htm
- https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112249
- https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202
- https://sc1.checkpoint.com/documents/Best_Practices/CP_R80.20_Best_Practices_for_Threat_Prevention/Content/Topics/Introduction.htm
- https://sc1.checkpoint.com/documents/R81.10/SmartConsole_OLH/EN/Topics-OLH/Home-Page.htm?tocpath=_____1
- https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Welcome.htm
- https://downloads.checkpoint.com/dc/download.htm?ID=103845

Fortinet

- https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/954635/getting-started
- https://docs.fortinet.com/document/fortigate/7.2.0/best-practices/587898/getting-started
- https://docs.fortinet.com/document/fortigate/6.4.0/best-practices/587898/best-practices

11. About SecureIQLab

SecureIQLab is a cybersecurity testing lab that was founded in 2019. SecureIQLab works with enterprises, governments, and security vendors to bridge the applied intelligence gap that exists between market and technology research. SecureIQLab also provides services to operationalize security and the metrics to help organizations improve their return on security investments.

SecureIQLab, LLC.
9600 Great Hills Trail, Suite 150W
Austin, TX 78759 USA

+1.512.575.3457
www.secureiqlab.com
info@secureiqlab.com

12. Copyright and Disclaimer

THIS REPORT IS PROVIDED "AS IS," "AS AVAILABLE" AND "WITH ALL FAULTS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, SECUREIQLAB EXPRESSLY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING: (a) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (b) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF THE REPORT, OR THAT USE OF THE REPORT WILL BE ERROR-FREE, UNINTERRUPTED, FREE FROM OTHER FAILURES OR WILL MEET YOUR REQUIREMENTS. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING SENTENCE, YOU ACKNOWLEDGE AND AGREE THAT THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT DEPEND UPON VARIOUS FACTORS, INCLUDING FACTORS OUTSIDE OF SECUREIQLAB'S CONTROL, SUCH AS: (1) THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF INFORMATION AND MATERIALS PROVIDED BY OTHER PARTIES THAT ARE RELIED UPON BY SECUREIQLAB IN PERFORMING PREPARING THE REPORT; AND (2) THE UNDERLYING ASSUMPTIONS MADE BY SECUREIQLAB IN PREPARING THE REPORT REMAINING TRUE AND ACCURATE. YOU ARE SOLELY RESPONSIBLE FOR INDEPENDENTLY ASSESSING THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT BEFORE TAKING OR OMITTING ANY ACTION BASED UPON THE REPORT. IN NO EVENT WILL SECUREIQLAB BE LIABLE FOR ANY LOST PROFITS OR COST OF COVER, OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES ARISING FROM OR RELATING TO ANY TYPE OR MANNER OF COMMERCIAL, BUSINESS OR FINANCIAL LOSS, EVEN IF SECUREIQLAB HAD ACTUAL OR CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE.

For more information about SecureIQLab and the testing methodologies, please visit our website.

SecureIQLab (September 2023)