SecureIQLab
Independent. Rigorous. Reproducible.
Evidence you can trust.

COMMISSIONED REPORT

SECURITY SERVICE EDGE
INDEPENDENT CYBERRISK VALIDATION COMPARATIVE REPORT

Products :	Cisco Secure Access, Fortinet FortiSASE, Netskope One, Prisma Access, Zscaler Zero Trust Exchange
Test Period :	April – July, 2026
Report Classification:	Commissioned Comparative Validation
Commissioned By :	Palo Alto Networks

Table of Contents

01 Executive Summary 3

02 Tested Products and Deployment 5

2.1 Tested Products and Versions 5

2.2 Deployment and Architecture 5

03 Security Efficacy Comparative 8

3.1 Scoring Methodology 8

3.2 SSE Security Pillars 9

3.2.1 Firewall as a Service (FWaaS) 9

3.2.2 Cloud Access Security Broker (CASB) 12

3.2.3 Zero Trust Network Access (ZTNA) 15

3.2.4 Secure Web Gateway (SWG) 16

3.2.4.1 SWG Scoring 17

3.2.4.2 Complete Secure Web Gateway Score 18

3.2.4.2.1 Known Threats (Threat Intelligence Feeds) 19

3.2.4.2.2 Advanced Threats (Patient Zero) 19

3.2.4.3 Categorization Accuracy Score 21

04 Operational Efficiency 22

05 False Positives 24

06 Conclusion 25

07 Appendix, Copyright and Disclaimer 26

7.1 Appendix 26

7.2 Copyright and Disclaimer 28

01
Executive Summary

Security Service Edge (SSE) has become a critical security architecture for protecting modern hybrid workforces and cloud applications through integrated, cloud-delivered security services. This commissioned comparative validation independently assesses five SSE solutions from Palo Alto Networks, Zscaler, Netskope, Cisco, and Fortinet using SecureIQLab's standardized SSE methodology to evaluate security effectiveness, operational excellence, and enterprise readiness. All evaluated solutions were configured by SecureIQLab based on vendor-recommended best practices and publicly available product documentation. Palo Alto Networks was not provided with the test samples prior to execution.

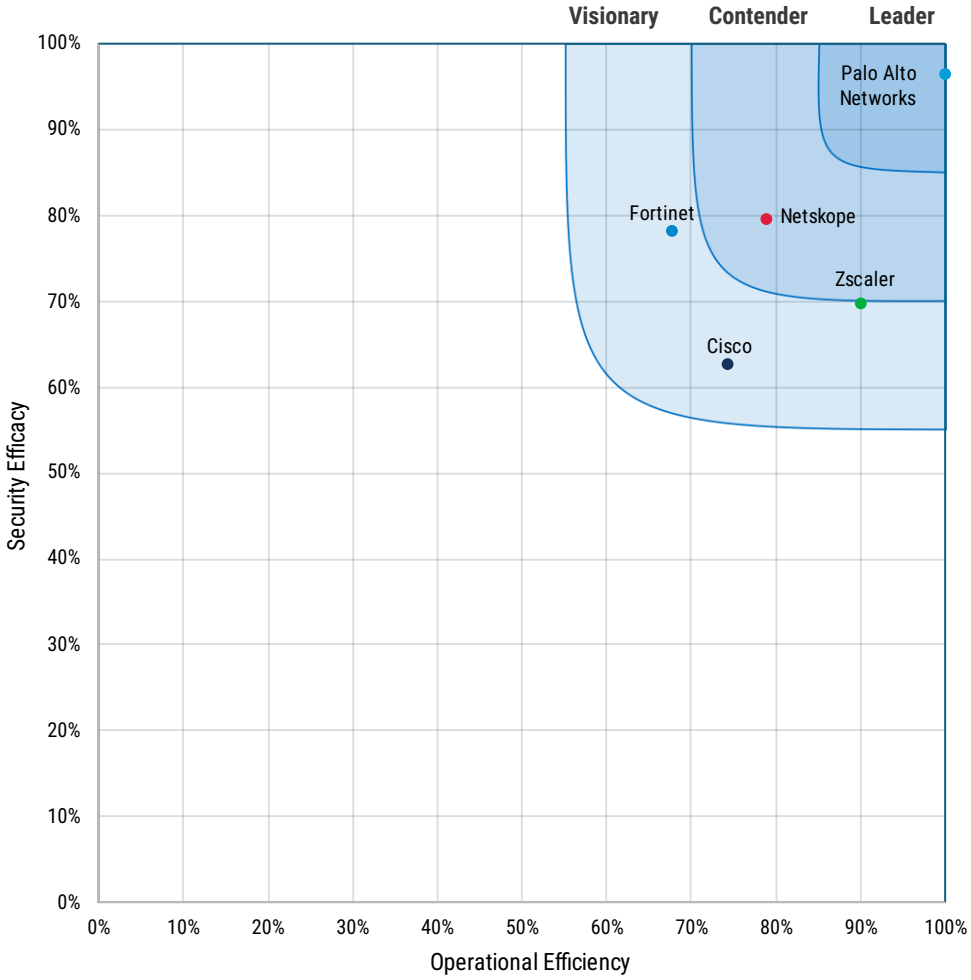

Figure 1. 2026 Security Service Edge (SSE) CyberRisk Ripple

The 2026 Security Service Edge (SSE) CyberRisk Ripple, illustrated in Figure 1, presents the relative positioning of the evaluated SSE solutions along two primary evaluation dimensions: security efficacy (Y-axis) and operational efficiency (X-axis). Solutions demonstrating higher scores across both dimensions represent stronger overall performance while maintaining operational effectiveness.

This comparative report provides an overview of the results for all tested vendors. The evaluated vendors are categorized into three rankings: (1) Leader, (2) Contender and (3) Visionary. These rankings reflect each vendor's placement within the respective zones of the 2026 Commissioned Comparative Security Service Edge (SSE) CyberRisk Ripple shown in Figure 1, which visualizes security efficacy and operational efficiency.

Palo Alto Networks is positioned as the **Leader**, Netskope as the **Contender**, and Fortinet, Cisco, and Zscaler as **Visionaries**.

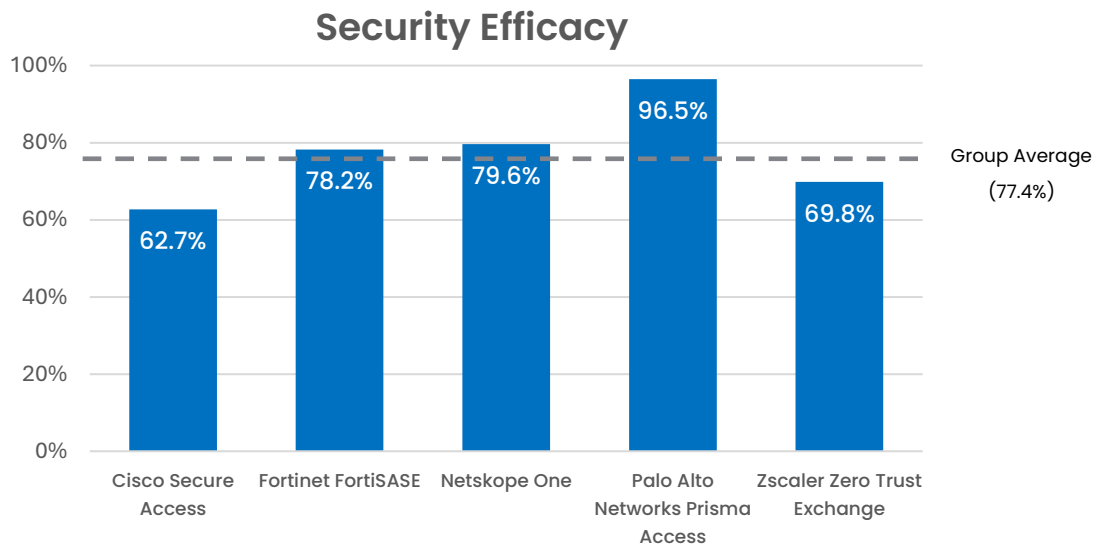

Figure 2. Overall Security Efficacy Scores for the SSE Solutions

Figures 2 and 3 present the overall Security Efficacy and Operational Efficiency results for the evaluated SSE solutions, respectively.

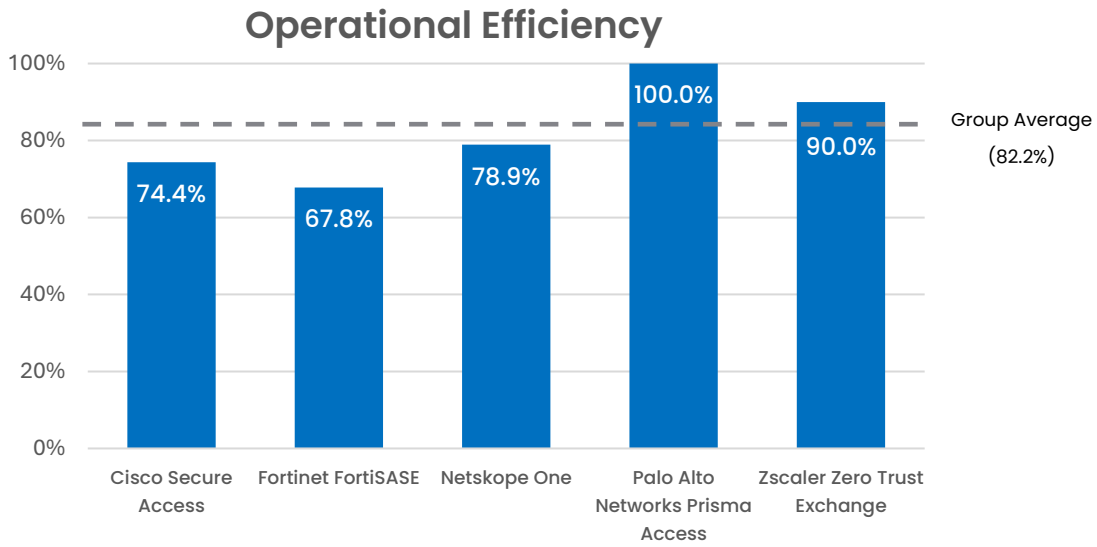

Figure 3. Overall Operational Efficiency Scores for the SSE Solutions

02
Tested Products and Deployment

2.1 Tested Products and Versions

Vendors	Product	Product Version
Palo Alto Networks	Prisma Access	6.2.0 PAN-OS Version (12.1.7)
Fortinet	FortiSASE	v7.4_v26.2.152-v2.11.18
Netskope	Netskope One	139.0.4.307
Cisco	Cisco Secure Access	Cloud Managed
Zscaler	Zscaler Zero Trust Exchange	Cloud Managed[1]

Table 1. Product Version and Licensing

2.2 Deployment and Architecture

The test environment was designed to simulate a representative enterprise deployment using a Security Service Edge (SSE) architecture. Multiple SSE solutions were evaluated under consistent network conditions to compare security efficacy, functionality, performance, operational efficiency, and user experience.

The environment included remote users, branch offices, Internet-based applications, public-cloud services, and private enterprise resources hosted in a centralized data center. Traffic from each user and branch location was routed through the SSE platform, enabling centralized security inspection and consistent policy enforcement.

Internet and cloud resources. Internet destinations included SaaS applications, GenAI platforms, public-cloud services, and external websites. Internet-bound traffic was inspected by the SSE platform before reaching its destination.

[1] Cisco Secure Access and Zscaler Zero Trust Exchange are continuously-delivered cloud services; specific build IDs are not exposed to tenants. Test window: April – July 2026

The SSE Platform served as the centralized security inspection and enforcement layer, providing:

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Zero Trust Network Access (ZTNA)
- Firewall-as-a-Service (FWaaS)

Remote Users simulated employees working from home, traveling, or connecting from unmanaged networks. These users accessed both Internet-based applications and private enterprise resources through the SSE platform. Validation focused on user authentication, application access, policy enforcement, user experience, performance, logging, and visibility.

Branch Networks. Branch offices represented distributed enterprise locations connected to the SSE platform. Each branch included user workstations and a secure network gateway. Testing evaluated branch-to-Internet connectivity, access to private applications, security inspection, policy consistency, and performance under representative enterprise traffic conditions.

Data Center and Private Applications. The data center represented enterprise-hosted applications and internal services requiring controlled access. These resources were not directly exposed to the Internet and were accessed through the SSE platform using ZTNA-based controls. Testing verified that authenticated and authorized users received appropriate access while unauthorized requests were denied according to configured security policies.

Test Traffic Flow. The evaluation followed several common enterprise communication paths:

- Remote users accessing Internet and SaaS applications through the SSE platform.
- Remote users securely accessing private enterprise applications through ZTNA.
- Branch offices communicating with Internet services through centralized SSE inspection.
- Branch offices accessing private data-center resources through policy-controlled connections.

Figure 4 illustrates the architecture diagram that represents a common enterprise scenario where users require secure access to both internal and external resources while maintaining centralized visibility and policy enforcement.

All user and branch traffic was routed through the SSE platform, providing a consistent basis for comparing security controls, policy enforcement, operational visibility, performance, and user experience across the evaluated SSE solutions.

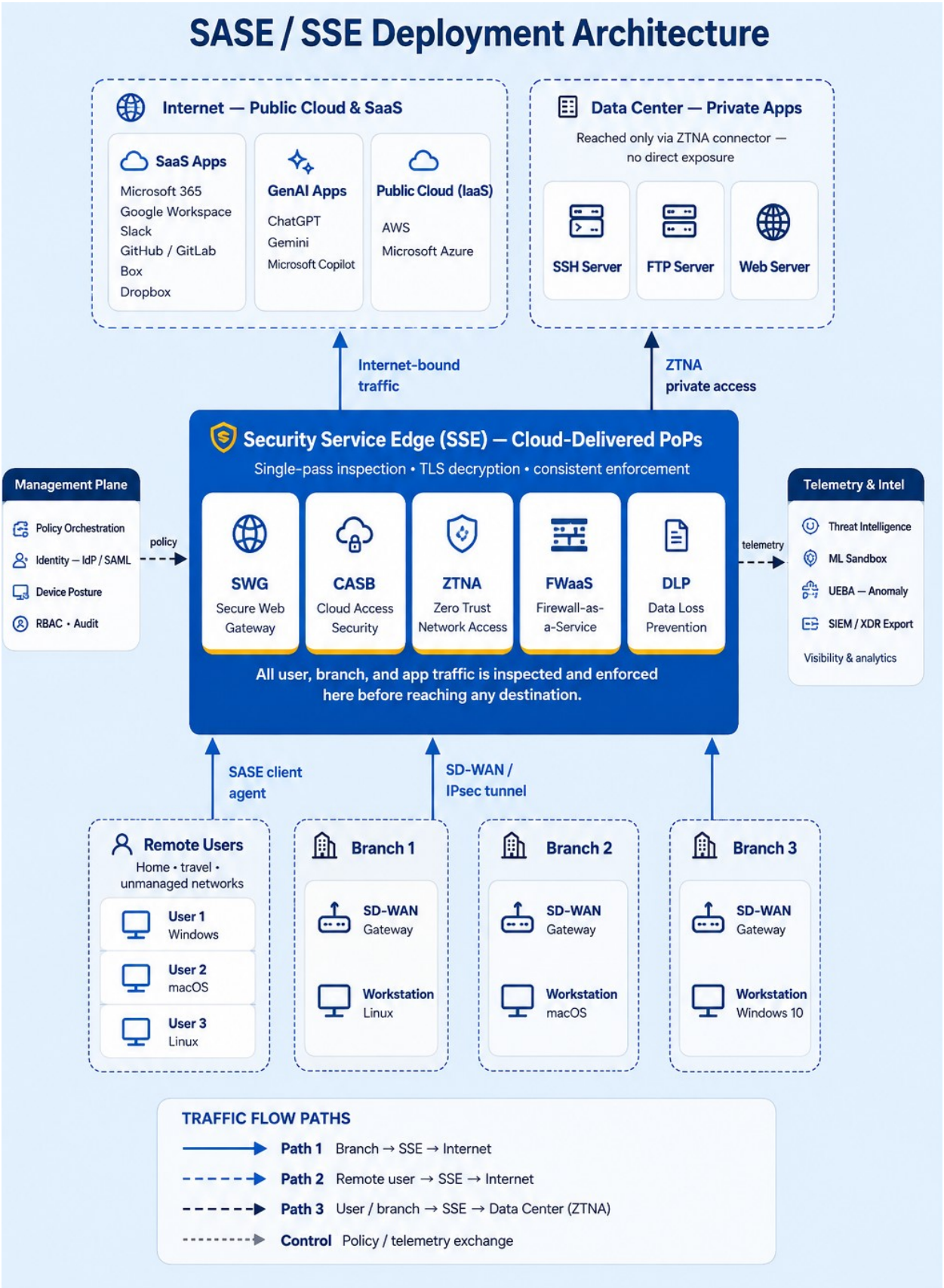

Figure 4. Deployment Architecture Diagram for the SecureIQLab SSE evaluation.

03
Security Efficacy Comparative

Effective security architecture delivers consistent protection for users, applications, SaaS services, private applications, and internet traffic regardless of location or device. Unlike traditional product evaluations that examine security controls independently, SecureIQLab evaluates the SSE platform as a unified cloud-delivered security architecture. The validation measures the effectiveness of the four core SSE pillars: Firewall-as-a-Service (FWaaS), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA) and Secure Web Gateway (SWG), while also assessing Operational Efficiency and False Positives.

The evaluation included 1,725 test cases designed to assess security efficacy across a diverse range of enterprise use cases, threat scenarios, applications, and access environments. This comprehensive testing reflects SecureIQLab's commitment to delivering independent, relevant, and continuously evolving security validation.

3.1 Scoring Methodology

FWaaS, CASB[2], and ZTNA scores are calculated as the average of the protection rates across their respective high-level test categories. The Overall Security Efficacy Score is the arithmetic mean of the four pillar scores. SWG scoring uses a graded point system defined in section 3.2.4.1. Operational Efficiency scoring is defined in section 4.

SSE Validation Categories	Vendors and Products					
	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange	Group Average
Firewall-as-a-Service (FWaaS) Overall Score	60.8%	86.4%	67.2%	99.6%	61.8%	75.2%
Cloud Access Security Broker (CASB) Overall Score	40.2%	42.6%	79.6%	91.7%	57.3%	62.3%
Zero Trust Network Access (ZTNA) Overall Score	77.8%	100.0%	100.0%	100.0%	77.8%	91.1%

[2] N/A entries are counted as 0 in the aggregate CASB Total Protection Rate. See 3.1.2 for scoring methodology.

SSE Validation Categories	Vendors and Products					
	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange	Group Average
Secure Web Gateway (SWG) Overall Score	72.0%	83.8%	71.7%	94.5%	82.5%	80.9%
Overall Security Efficacy Score	**62.7%**	**78.2%**	**79.6%**	**96.5%**	**69.8%**	**77.4%**

Table 2: Overall Security Efficacy Scores

The group average for Overall Security Efficacy was 77.4% as shown in Table 2.

3.2 SSE Security Pillars

3.2.1 Firewall as a Service (FWaaS)

Firewall as a Service (FWaaS) is a cloud-native security service within an SSE architecture that delivers enterprise firewall capabilities from distributed cloud points of presence (PoPs). FWaaS enforces security policies by inspecting and filtering network traffic, controlling application access, and preventing network-based threats for remote users, branch offices, and cloud workloads.

SecureIQLab's evaluation included 26 test categories and 543 attacks, measuring each platform's ability to enforce enterprise security policies and defend against network-based threats, including policy enforcement, tunneling techniques, command-and-control communications, malware downloads, advanced persistent threats (APTs), browser-based attacks, and advanced evasion methods.

Test Categories	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange	Group Average
Policy Enforcement	100.0%	99.5%	99.8%	100.0%	99.8%	99.8%
Tunneling Tests	25.0%	50.0%	37.5%	100.0%	75.0%	57.5%
Command and control	100.0%	100.0%	90.0%	100.0%	50.0%	88.0%
Malware Download over Network	32.1%	73.7%	51.9%	97.4%	44.9%	60.0%
Advanced Persistent Threats	0.0%	100.0%	0.0%	100.0%	0.0%	40.0%

Test Categories	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange	Group Average
Browser-Based-Threats	100.0%	100.0%	100.0%	100.0%	91.7%	98.3%
Advanced Evasion Methods	68.8%	81.3%	91.3%	100.0%	71.3%	82.5%
Total Protection Rate	**60.83%**	**86.36%**	**67.21%**	**99.63%**	**61.80%**	**75.2%**

Table 3: Firewall as a Service (FWaaS) Results

Table 3 presents the protection rates achieved by the Firewall-as-a-Service (FWaaS) component of the evaluated SSE solutions across the tested threat categories. Cisco, Netskope, and Zscaler each recorded a 0% score in Advanced Persistent Threat (APT) since none of the APT test cases included in this specific test category were successfully blocked under the tested configurations and conditions.

The Total Protection Rate represents each SSE solution's overall effectiveness in its FWaaS component across all evaluated threat categories.

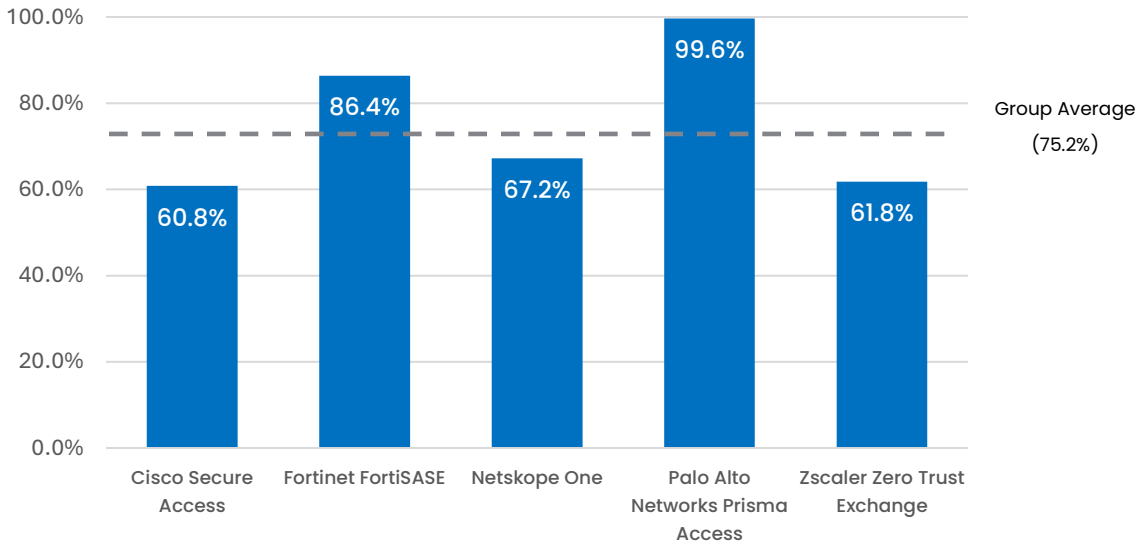

Figure 5. Firewall as a Service (FWaaS) Scores

Figure 5 shows that Palo Alto Networks Prisma Access achieved the highest overall FWaaS protection rate at 99.63%, demonstrating consistently strong protection across all evaluated threat categories with perfect scores in six of the seven categories.

Fortinet FortiSASE achieved an overall protection rate of 86.36%, providing excellent protection against command-and-control communications, advanced persistent threats (APTs), and browser-based threats. Netskope One (67.21%), Zscaler Zero Trust Exchange (61.80%) and Cisco Secure Access (60.83%)

demonstrated strong policy enforcement capabilities but showed lower protection rates in several advanced threat categories.

Test Categories	Sub Categories	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange
Policy Enforcement	Protocol/Service Based Policy Enforcement	100%	98%	100%	100%	100%
	Application Based Policy Enforcement	100%	100%	100%	100%	100%
	Time based Policy Enforcement	100%	100%	100%	100%	100%
	Geo-Location Based Policy Enforcement	100%	100%	100%	100%	99%
	Web Category Policy Enforcement	100%	100%	99%	100%	100%
Tunneling Tests	DNS Tunneling	0%	0%	50%	100%	100%
	HTTPs Tunneling	0%	100%	0%	100%	100%
	ICMP Tunneling	100%	100%	100%	100%	100%
	SSH Tunneling	0%	0%	0%	100%	0%
Command and Control	Botnet Traffic Simulation	100%	100%	80%	100%	100%
	Heuristic & Anomaly Detection	100%	100%	100%	100%	0%
Malware Download over Network	Malware download over HTTP	4%	85%	96%	100%	98%
	Malware download over HTTPS	25%	54%	60%	92%	37%
	Malware download over SMTP	67%	83%	0%	100%	0%
Advanced Persistent Threats	Caldera Based Attack	0%	100%	0%	100%	0%
Browser-Based-Threats	Browser Exploits	100%	100%	100%	100%	75%
	HTML Smuggling	100%	100%	100%	100%	100%
	Obfuscated JavaScript	100%	100%	100%	100%	100%
Advanced Evasion Methods	Encrypted or Obfuscated Payloads	100%	100%	100%	100%	100%
	Fragmentation & Split Attacks	100%	100%	100%	100%	100%
	Living off the Land	0%	100%	100%	100%	100%
	Multiple Layers of Encryption	100%	100%	100%	100%	100%
	Evasive Command and Control	50%	50%	50%	100%	50%
	Polymorphic and Metamorphic Payloads	100%	100%	100%	100%	100%
	Protocol Evasion Techniques	0%	0%	100%	100%	0%
	Traffic Padding or Randomization Evasion	100%	100%	80%	100%	20%
Total Protection Rate		**60.83%**	**86.36%**	**67.21%**	**99.63%**	**61.80%**

Table 4: Detailed Results for Firewall as a Service (FWaaS)

3.2.2 Cloud Access Security Broker (CASB)

SecureIQLab evaluated the Cloud Access Security Broker (CASB) capabilities of the evaluated SSE solutions to assess their ability to provide visibility, policy enforcement, and data protection across enterprise SaaS and generative AI applications. The assessment was organized into five functional areas: Activity Control, Tenant Control, Data Control, Out-of-Band CASB, and SaaS Security Posture Management (SSPM).

Testing included a total of 643 test cases, measuring each platform's ability to monitor user activities, enforce access and tenant policies, protect sensitive data, identify cloud security risks, and assess the security posture of connected SaaS environments.

Test Categories	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange	Group Average
Activity Control	35.7%	41.8%	84.6%	90.7%	51.7%	60.9%
Tenant Control	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Data Control	37.9%	62.1%	74.3%	82.0%	71.0%	65.5%
Out of Band CASB	27.3%	9.1%	100%	90.9%	44.4%	54.3%
SSPM	N/A[3]	N/A[4]	39.0%	95.1%	19.5%	30.7%
Total Protection Rate	**40.2%**	**42.6%**	**79.6%**	**91.7%**	**57.3%**	**62.3%**

Table 5: Cloud Access Security Broker (CASB) Results

Table 5 presents the CASB protection rates achieved by the evaluated SSE solutions across the five assessed functional areas.

Lower Out-of-Band CASB results for Fortinet, Cisco, and Zscaler were primarily driven by limited API-based application coverage. Within the applications included in this evaluation, FortiSASE provided API-based CASB coverage for fewer of the tested applications than some of the other evaluated solutions; Cisco CASB API coverage for Google Workspace includes Google Drive but not Gmail, while Microsoft 365 coverage includes OneDrive but not Outlook; and in Zscaler, GitHub is supported as an SSPM connector but is not available for secret-exposure scanning through the Zscaler CASB API.

Regarding SSPM, Netskope and Zscaler demonstrated limited functionality, with multiple security controls either unsupported, invalid, or unable to be tested across applications such as Google

[3] no native SSPM; relies on AppOmni integration
[4] SSPM was not commercially available during testing (introduced later in July 2026)

Workspace and Salesforce. Cisco Secure Access was marked N/A, as the platform does not provide native SSPM capability[5]; SSPM capabilities are available through a third-party integration with AppOmni. Fortinet FortiSASE was marked as N/A, as its SSPM capability[6] was not commercially available at the time of testing and was subsequently introduced in July 2026. For scoring purposes, N/A results are treated as 0% in the aggregate CASB Total Protection Rate.

All evaluated SSE solutions achieved 100% in Tenant Control, indicating consistent enforcement of managed and unmanaged tenant policies.

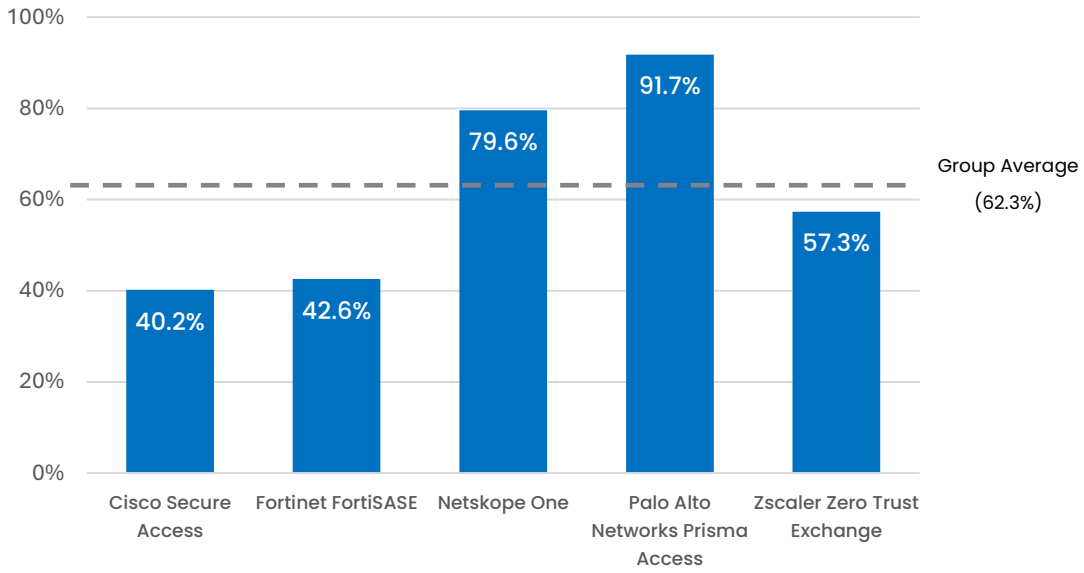

Figure 6. Cloud Access Security Broker (CASB) Scores

Figure 6 presents the overall CASB protection scores achieved by the evaluated SSE solutions. The group average for CASB protection was 62.3%, with only Palo Alto Networks Prisma Access and Netskope One exceeding the group average.

[5] https://appomni.com/partners/cisco/

[6]https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/d4c89936-6f12-11f0-a9d0-d2b0d2e22f7d/FortiSASE-26.1.107_Feature-Release_Notes.pdf

Table 6 below provides a detailed view of the CASB protection results, illustrating the performance of evaluated SSE solutions across each CASB functional area.

The CASB testing included 643 test cases across a diverse set of Tier 1 enterprise and GenAI applications, including Google Workspace, Microsoft Office 365, Salesforce, Dropbox, GitHub, Slack, ChatGPT, and others. The testing covered key application categories such as communication, collaboration, file sharing, cloud storage, code repositories, CRM, and AI services.

Test Categories	Sub Categories	Application Category	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange
Activity Control	Enterprise Application Category	Communication and Collaboration	40.0%	75.0%	75.0%	95.0%	30.0%
		File Sharing	42.9%	42.9%	85.7%	83.3%	69.1%
		Instant Messaging	0.0%	7.7%	88.5%	96.2%	11.5%
		Video Conferencing	14.3%	21.4%	75.0%	96.4%	3.6%
		Cloud Storage	81.8%	45.5%	95.5%	86.4%	86.4%
		Collaboration	83.3%	75.0%	83.3%	100.0%	83.3%
		Code Repository	70.0%	50.0%	100.0%	100.0%	60.0%
	Application GenAI Category	Gen AI Security	0.00%	50.00%	81.8%	81.82%	90.91%
Tenant Control	Enterprise Application Category	Collaboration and Communication	100%	100%	100%	100%	100%
		File Sharing	100%	100%	100%	100%	100%
Data Control	Enterprise Application Category	File Sharing	47.3%	71.4%	75.8%	90.1%	96.4%
		Video Conferencing	0.0%	39.6%	83.3%	87.5%	52.1%
		Code Repository	53.6%	82.1%	71.4%	50.0%	92.9%
		Cloud Storage	21.2%	36.5%	76.9%	82.7%	44.2%
		Collaboration	26.9%	40.4%	80.8%	86.5%	51.9%
		Communication and Collaboration	33.9%	71.4%	75.0%	92.9%	48.2%
		Multi-channel DLP Inspection	50.0%	100.0%	100.0%	100.0%	100.0%
	Application GenAI Category	Gen AI Security	76.0%	76.0%	42.0%	54.0%	94.0%
Out of Band CASB	Enterprise Application Category	File Sharing	50.0%	25.0%	100.0%	100.0%	75.0%
		Cloud Storage	25.0%	N/A	100.0%	100.0%	25.0%
		Code Repository	N/A	N/A	N/A	100.0%	N/A
		Communication and Collaboration	N/A	N/A	100.0%	50.0%	N/A
SSPM	Enterprise Application Category	Collaboration & Communication	N/A	N/A	33.3%	93.94%	12.12%
		CRM	N/A	N/A	62.5%	100%	50.0%
Total Protection Rate			**40.2%**	**42.6%**	**79.6%**	**91.7%**	**57.3%**

Table 6: Detailed Cloud Access Security Broker (CASB) Results

3.2.3 Zero Trust Network Access (ZTNA)

SecureIQLab evaluated the Zero Trust Network Access (ZTNA) capabilities of the assessed SSE solutions to determine their ability to securely control access to private enterprise applications based on user identity, device posture, and continuous trust verification.

The evaluation validated 9 test cases, including unauthenticated access blocking, identity-based access enforcement, device posture assessment, least-privilege access, continuous authorization, split tunneling, application enumeration prevention, session management, and clientless access policy enforcement. Together, these test cases measured each platform's ability to prevent unauthorized access, restrict lateral movement, and enforce secure application access throughout the user session.

Test Cases	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange
Total Score	77.8%	100%	100%	100%	77.8%

Table 7: Zero Trust Network Access (ZTNA) Scores

Table 7 and Figure 7 show the overall score for Zero Trust Network Access with three vendors achieving the perfect score of 100%.

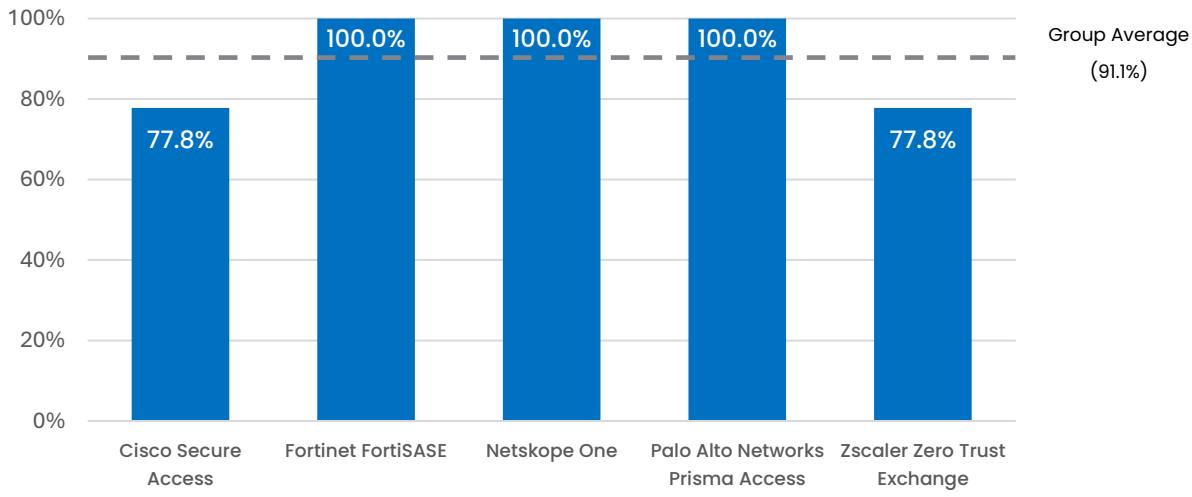

Figure 7. Zero Trust Network Access (ZTNA) Scores with group average

Table 8 presents the ZTNA protection results for the evaluated SSE solutions across nine Zero Trust access control test cases. Palo Alto Networks Prisma Access, Fortinet FortiSASE, and Netskope One achieved a 100% overall score, successfully passing all evaluated test cases, including identity-based

access enforcement, device posture validation, continuous authorization, application enumeration prevention, and clientless access policy enforcement.

The group average for Zero Trust Network Access (ZTNA) was 91.1%.

Test Case	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange
Unauthenticated Access Block	Pass	Pass	Pass	Pass	Pass
Identity-Based Access Enforcement	Pass	Pass	Pass	Pass	Pass
Device Posture Gate	Pass	Pass	Pass	Pass	Fail
Least-Privilege / Lateral Movement Block	Pass	Pass	Pass	Pass	Pass
Continuous Authorization	Fail	Pass	Pass	Pass	Fail
Split Tunneling Enforcement	Pass	Pass	Pass	Pass	Pass
Application Enumeration Prevention	Pass	Pass	Pass	Pass	Pass
Session Timeout & Re-authentication	Fail	Pass	Pass	Pass	Pass
Clientless Access Policy Enforcement	Pass	Pass	Pass	Pass	Pass
Overall Score	**77.78%**	**100.00%**	**100.00%**	**100.00%**	**77.8%**

Table 8. Detailed Results for Zero Trust Network Access (ZTNA)

3.2.4 Secure Web Gateway (SWG)

SecureIQLab evaluated the Secure Web Gateway (SWG) capabilities of the assessed SSE solutions to determine their effectiveness in protecting users from modern web-based threats through advanced URL filtering and real-time threat inspection.

The evaluation included 1,394 unique URLs, consisting of 656 malicious URLs and 738 legitimate URLs. The malicious URL corpus combined established and emerging threats sourced from public and commercial threat intelligence feeds and SecureIQLab's internal threat repository with custom-developed attack scenarios hosted on SecureIQLab-controlled infrastructure.

The custom-developed scenarios were designed to assess protection against modern adversary techniques, including QR code phishing, phishing kits, command-and-control (C2) infrastructure, open redirects, adversary-in-the-middle (AitM) attacks, deepfake-enabled attacks, HTTP refresh-based attacks, and LLM-obfuscated JavaScript.

3.2.4.1 SWG Scoring

Security Efficacy measures a product's ability to identify and prevent access to malicious URLs. Categorization Accuracy measured each product's ability to correctly classify benign URLs. This metric was limited to benign test cases and reflects whether the product assigned the expected URL category without incorrectly identifying the site as malicious.

The Scoring Criteria were applied as follows:

Benign URL Categorization Accuracy

- URL correctly categorized = 1.00
- URL assigned a generic category = 0.75
- URL assigned an incorrect category = 0.25
- URL not categorized (no detection) = 0.00

Malicious URL Security Efficacy

- URL blocked with a malicious category recorded in the log = 1.00
- URL blocked without a malicious category recorded in the log = 0.75
- URL blocked with no supporting log evidence explaining the block or no category = 0.25
- URL not blocked = 0.00

The Total Security Efficacy Score represents the overall effectiveness of each solution in protecting against malicious web-based threats. The score is calculated by dividing the total points earned across all malicious URLs evaluated by the total number of malicious URLs evaluated and multiplying the result by 100%.

$$\text{Total Security Efficacy Score} = \frac{(\text{Total malicious URLs points earned})}{\text{Total Malicious URLs Evaluated}} \times 100\%$$

Equation 1. SWG Security Efficacy Scores

Categorization Accuracy was calculated as:

$$\text{Categorization Accuracy Score} = \frac{(\text{Correctly categorized benign URLs points earned})}{\text{Total Benign URLs Evaluated}} \times 100\%$$

Equation 2. SWG Categorization Accuracy Scores

Categorization Accuracy is excluded from Total Security Efficacy Score because it measures the classification accuracy of benign URLs rather than the detection and prevention of malicious threats.

3.2.4.2 Complete Secure Web Gateway Score

SecureIQLab evaluated each SSE Solution against 656 malicious URLs across the Known Threats and Advanced Threats evaluations representing a diverse set of established, emerging, and sophisticated URL-based threats.

Test Categories	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange
Known Threats (Threat Intelligence Feeds)	77.2%	87.5%	76.7%	95.9%	86.4%
Advanced Threats (Patient Zero)	35.2%	57.4%	37.0%	*83.2%	55.6%
Complete SWG Score	**72.0%**	**83.8%**	**71.7%**	**94.5%**	**82.5%**

Table 9. Complete Secure Web Gateway (SWG) Score

* Palo Alto Networks achieved an 83.2% Advanced Threat Efficacy Score using URL Filtering with log categorization, while other evaluated solutions supplemented their coverage to varying degrees through non-URL filtering controls.
* While Palo Alto Networks Prisma Access achieved a raw 97% block rate, its 83.2% Security Efficacy Score reflects the benchmark's weighted methodology.

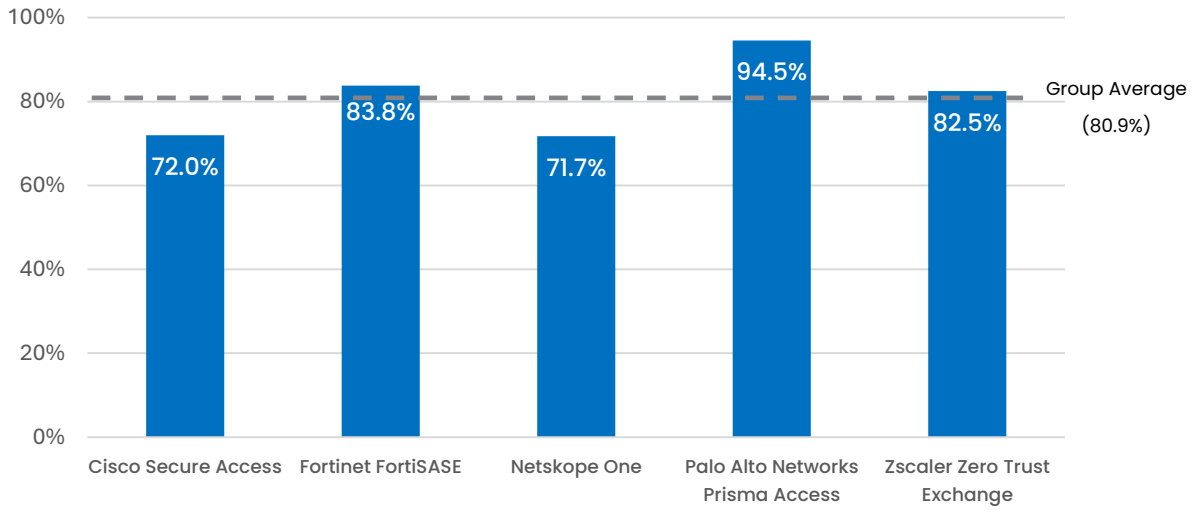

Figure 8. Secure Web Gateway (SWG) Score with group average

Palo Alto Networks Prisma Access achieved the highest overall SWG Security Efficacy Score at 94.5%, demonstrating consistently strong protection across the evaluated URL-based threat scenarios. Fortinet FortiSASE followed at 83.8%, with Zscaler Zero Trust Exchange close behind at 82.5%, while Cisco Secure Access and Netskope One achieved 72.0% and 71.7%, respectively, reflecting greater variation in protection across the evaluated threat scenarios.

3.2.4.2.1 Known Threats (Threat Intelligence Feeds)

The Known Threats Evaluation measured each solution's ability to detect and block active malicious websites observed in real-world environments while continuing to allow legitimate web traffic. This evaluation combines a broad corpus of established malicious URLs with a newly collected set of emerging threats sourced from public and commercial threat intelligence feeds, providing a comprehensive assessment of protection against both prevalent and recently observed web-based attacks.

Evaluated Test Categories	Vendor Products				
	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange
Known Threats (Threat Intelligence Feeds) Security Efficacy Score	77.2%	87.5%	76.7%	95.9%	86.4%

Table 10. Known Threats (Public Threat Intelligence Feeds) Security Efficacy Score

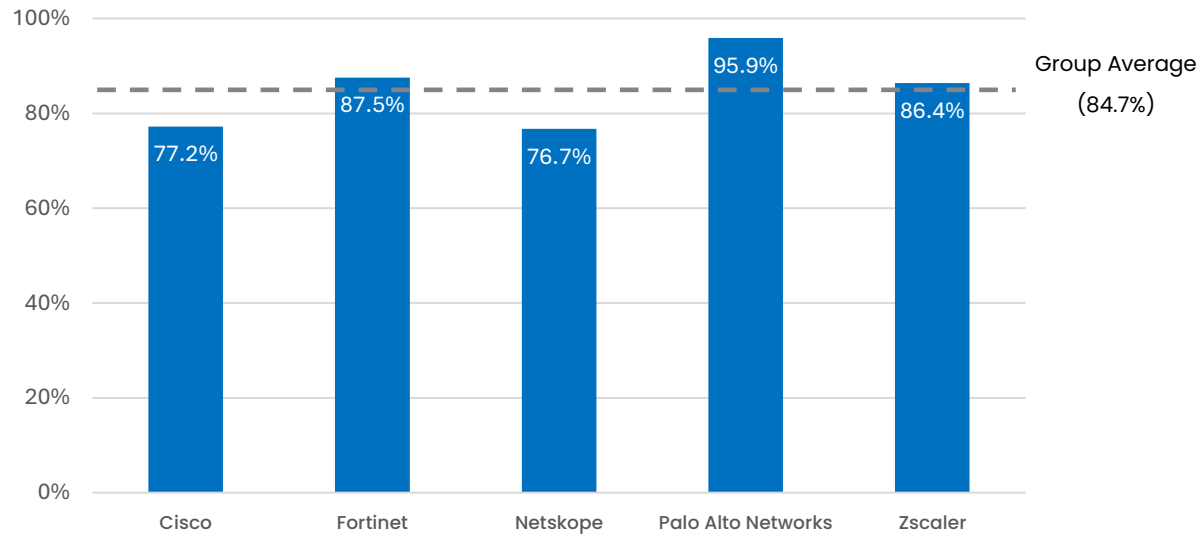

Figure 9. Known Threats (Public Threat Intelligence Feeds) Security Efficacy Score with Group Average

3.2.4.2.2 Advanced Threats (Patient Zero)

SecureIQLab evaluated Advanced Threat URLs to measure each solution's ability to protect against sophisticated, custom-crafted web attack techniques designed to emulate modern adversary tactics that may not yet be widely represented in public threat intelligence feeds. The evaluation included

SecureIQLab-developed attack scenarios utilizing managed synthetic test pages, such as QR code phishing, phishing kits, command-and-control (C2) infrastructure, open redirects, AitM (Adversary-in-the-Middle) Attacks, deepfake-enabled attacks, HTTP refresh-based attacks, and LLM-obfuscated JavaScript.

The evaluation was executed over three independent iterations to assess detection consistency and repeatability. Each iteration included 81 malicious URLs, resulting in a total of 243 malicious URL measurements per vendor across all three iterations.

Evaluated Test Categories	Vendor Products				
	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange
Advanced Threats (Patient Zero) Security Efficacy Score	35.2%	57.4%	37.0%	83.2%	55.6%

Table 11. Advanced Threats (Patient Zero) Security Efficacy Score

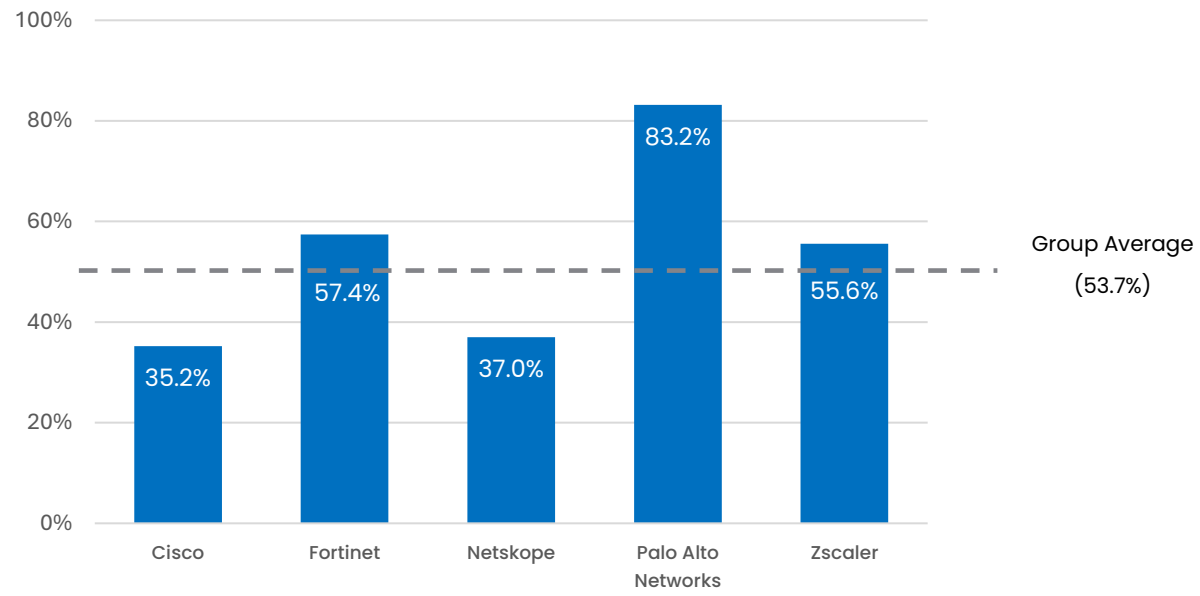

Figure 10. Advanced Threats (Patient Zero) Security Efficacy Score with Group Average

Across the Advanced Threat URL evaluation, Palo Alto Networks Prisma Access achieved the highest Security Efficacy score at 83.2%, followed by Fortinet FortiSASE at 57.4%, Zscaler Zero Trust Exchange at 55.6%, Netskope One at 37.0%, and Cisco Secure Access at 35.2%. These scores represent the percentage of available security efficacy points earned based on each solution's ability to block malicious URLs and provide supporting threat classification and log evidence.

3.2.4.3 Categorization Accuracy Score

Categorization Accuracy measured each solution's ability to correctly classify legitimate URLs into their appropriate web categories. Accurate URL categorization is important for enforcing web usage policies, enabling administrators to apply granular access controls while minimizing unnecessary disruption to legitimate web traffic.

The evaluation assessed categorization performance across 738 legitimate URLs, measuring how consistently each solution classified legitimate web content into the expected categories.

Test Category	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange
Overall Categorization Accuracy Score	93.4 %	91.7 %	59.8 %	96.2 %	89.9 %

Table 12. Overall Categorization Accuracy Score

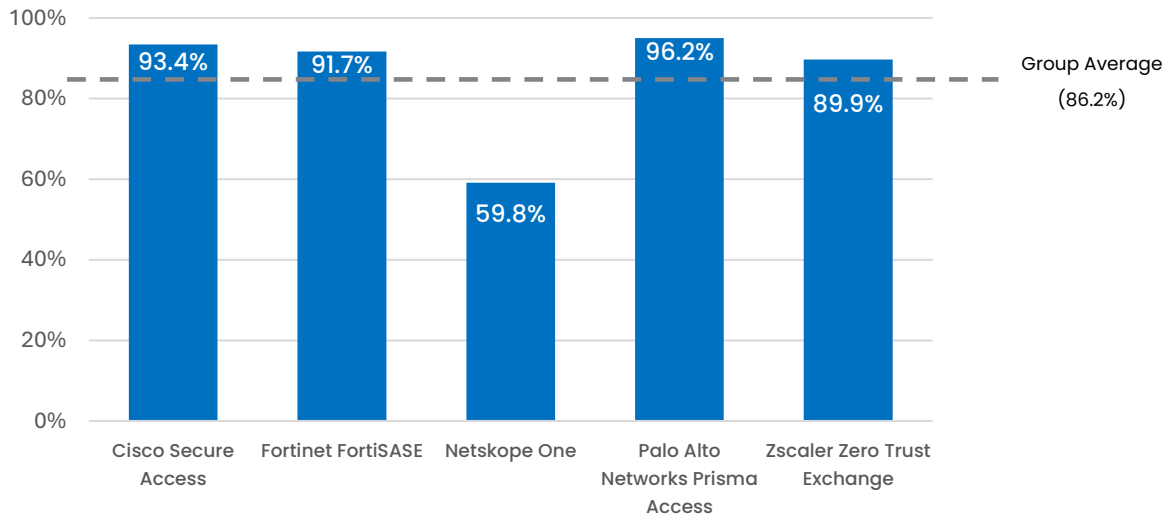

Figure 11. Overall Categorization Accuracy Score with group average

Figure 11 illustrates the Overall Categorization Accuracy Score, calculated by dividing the total categorization points earned across the legitimate URL corpus by the maximum available points.

The score was generally strong across the evaluated solutions, with four of the five products exceeding the group average of 86.2%.

Netskope One recorded the lowest score at 59.8%, indicating less consistent categorization of benign web content across the evaluated test categories. Netskope's lower benign URL categorization accuracy was driven by inconsistencies in URL categorization and telemetry observed during testing, including "Unknown" actions and discrepancies between syslog classifications and actual browser behavior. These visibility and validation challenges made it more difficult to consistently confirm the correct categorization and handling of benign URLs.

04
Operational Efficiency

Operational Efficiency is an important consideration when evaluating SSE platforms. By consolidating security capabilities into a unified cloud-native platform, organizations can reduce management complexity, improve policy consistency, decrease operational costs, and allow security teams to focus more on risk reduction than infrastructure maintenance.

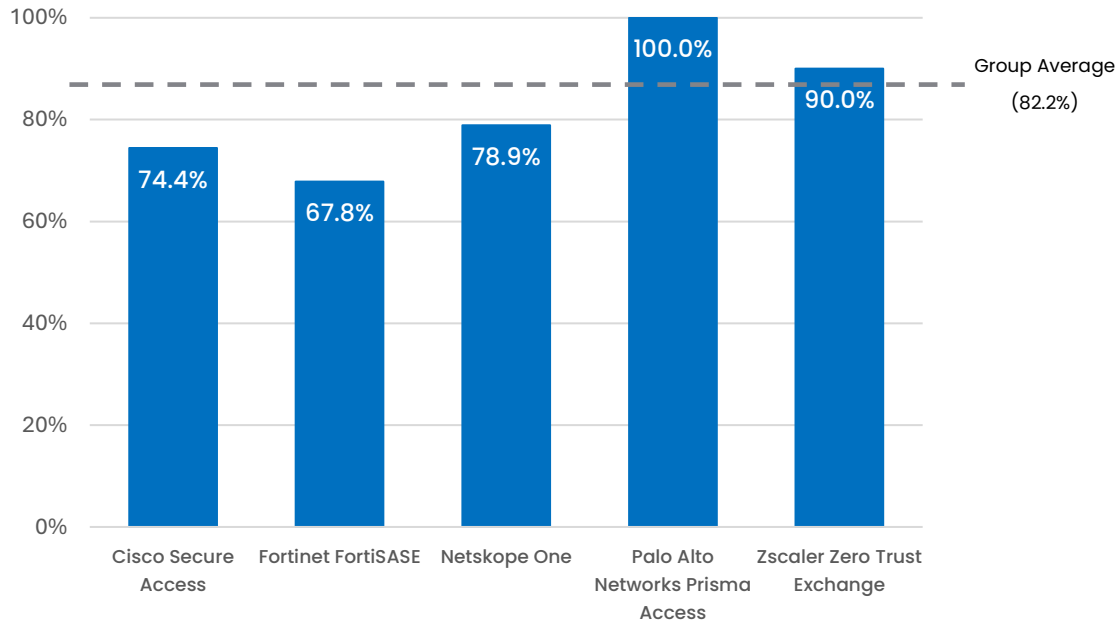

Figure 12. Operational Efficiency Rating

The Operational Efficiency Rating was calculated by adding together the total points for each category, then dividing this number by the maximum potential points and multiplying that number by 100%.

The features and functions within each category are awarded scores based on their capabilities. These scores are then tallied together to form a rating of high, medium, or low.

Points (integers 0 – 3) are earned for each feature within a category as follows:

- High or Yes = 3 Points
- Medium = 2 Points
- Low = 1 Point
- NA/No = 0 Points

As shown in Equation 3, the Final Operational Efficiency Rating is calculated as the percentage of operational efficiency points earned relative to the total points available.

$$\text{Final Operational Efficiency Rating} = \frac{\text{Total Operational Efficiency Points Earned}}{\text{Maximum Points Available}} \times 100\%$$

Equation 3. Final Operational Efficiency Rating

Test Cases	Cisco Secure Access	Fortinet FortiSASE	Netskope One	Palo Alto Networks Prisma Access	Zscaler Zero Trust Exchange	Group Average
Management & Policy Orchestration	83.30%	77.80%	72.20%	100.00%	83.30%	83.32%
Service Assurance & Observability	83.30%	66.70%	83.30%	100.00%	100.00%	86.66%
Automation & Programmability	75.00%	62.50%	79.20%	100.00%	91.70%	81.68%
Deployment & Infrastructure Scalability	77.80%	83.30%	83.30%	100.00%	88.90%	86.66%
Compliance & Resilience	41.70%	41.70%	75.00%	100.00%	83.30%	68.34%
Final operational Efficiency Rating	**74.40%**	**67.80%**	**78.90%**	**100.00%**	**90.00%**	**82.22%**

Table 13: Operational Efficiency Scores

05
False Positives

False Positives occur when legitimate websites, applications, or user activities are incorrectly identified as malicious and are blocked or alerted by the security solution. Excessive false positives can disrupt business operations, reduce user productivity, and increase the administrative effort required to investigate and remediate incorrect detections.

SecureIQLab evaluated each solution's ability to allow legitimate enterprise traffic while security protections remained enabled. To validate this capability, SecureIQLab used 790 benign test cases to verify that legitimate enterprise traffic was not incorrectly blocked.

Where appropriate, SecureIQLab applied consistent policy-tuning principles and vendor-supported exception-handling mechanisms across the evaluated solutions to reduce false positives while preserving overall security efficacy. This approach ensured that the evaluated solutions were assessed not only on their ability to prevent malicious activity but also on their ability to accurately permit legitimate enterprise traffic with minimal operational impact.

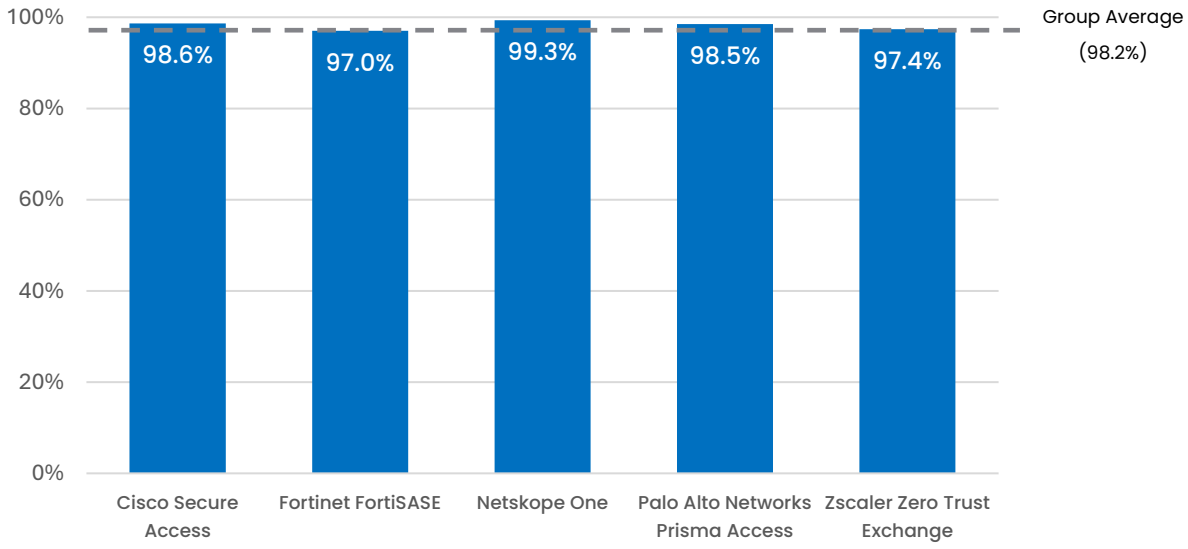

Figure 13. False Positive Avoidance Scores

06
Conclusion

The SecureIQLab 2026 Security Service Edge (SSE) CyberRisk Validation evaluated five SSE solutions across the four core security pillars - Firewall-as-a-Service (FWaaS), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Secure Web Gateway (SWG), along with Operational Efficiency and False Positive Avoidance.

Palo Alto Networks Prisma Access recorded the highest scores across the two primary CyberRisk Ripple dimensions, with 96.5% Overall Security Efficacy and 100% Operational Efficiency. Prisma Access also led the FWaaS and CASB evaluations. Netskope One achieved 79.6% Security Efficacy and 78.9% Operational Efficiency, Fortinet FortiSASE achieved 78.2% and 67.8%, Zscaler Zero Trust Exchange achieved 69.8% and 90.0%, and Cisco Secure Access achieved 62.7% and 74.4%, respectively. Prisma Access, FortiSASE, and Netskope One each achieved a perfect 100% score in ZTNA, highlighting strong performance in this security pillar.

False Positive Avoidance remained consistently strong across the group, averaging 98.2%, indicating that the evaluated solutions were generally able to maintain effective security protections while minimizing disruption to legitimate enterprise traffic.

Overall, the evaluation demonstrates measurable differences among the tested SSE solutions across CASB, SWG, ZTNA, FWaaS and operational capabilities. Based on the combined results of the evaluation, Palo Alto Networks is positioned as the Leader, Netskope as the Contender, and Fortinet, Cisco, and Zscaler as Visionaries, reflecting their relative performance, breadth of security capabilities, and operational effectiveness within the scope of SecureIQLab's 2026 SSE CyberRisk Validation.

07
Appendix, Copyright and Disclaimer

7.1 Appendix

Below is the list of licenses available across all vendors.

Vendor	Product	Licenses
Palo Alto Networks	Prisma Access	Prisma Access Mobile User Enterprise
		Prisma Access Net Enterprise
Fortinet	FortiSASE	Remote user subscriptions (Advanced subscription)
		Network add-on subscriptions (FortiGate SPA)
		Edge device subscriptions (FortiSASE branch thin edge - FortiExtender-200F FortiSASE branch thin edge - FortiExtender-200F)
Netskope	Netskope One	Borderless WAN Software – 1Y Enterprise Edition, 100 Mbps
		Hardware Support for NSG-101
		Premium Support
		Netskope Security Service Edge (SSE) SkopeAI ENTERPRISE Package
		Remote Browser Isolation (RBI) Level 3
		Private Application Access Level 2
		Next Gen SWG PROFESSIONAL for Machine Traffic
		NAA for Machine Traffic
		DNS Based Security
		DNSaaS Authenticated User
		DNSaaS Unauthenticated User/Device
		Premium Support
		Netskope Advanced Analytics Base
		IPS for Non-Web
		Premium Support
		Borderless WAN Software – 1Y Enterprise Edition, 100 Mbps
Cisco	Cisco Secure Access	Cisco Secure Access – Advantage (Intrusion Prevention System (IPS), Layer 7 Firewall, Secure Malware Analytics, Remote Browser Isolation (RBI), Data Loss Prevention (DLP))
Zscaler	Zscaler Zero Trust Exchange	Advanced Cloud Firewall
		Advanced Threat Protection
		Anti Virus and Anti Spam
		AppTotal Third Party
		BC Device Connector VM
		BC Device ZIA
		BC Device Advanced Logging
		BC Device Tunnel Encryption
		Bandwidth Controls
		Basic Reporting

Vendor	Product	Licenses
		CASB Basic SKU
		CASB SKU
		Cloud App Controls
		Cloud Browser Isolation STD
		Cloud Identity Broker
		Cloud Sandbox
		Cloud to Cloud Streaming FW
		Cloud to Cloud Streaming Web
		Custom Root Certificate
		DLP Endpoint
		DLP Web Basic SKU
		DNS Advanced
		DNS Essential
		DP Isolation SAAS STD
		Data Leak Protection (DLP)
		Encrypted VPN
		Firewall Basic
		IPv6 Advanced SKU
		IPv6 Basic SKU
		Isolation Adv
		Isolation Adv Plus (Trial)
		Mobile Security
		NSS Log Feed for Firewall
		NSS Log Feed for Web
		SIPA SKU
		SKU for Threat Insights
		Standard FW Full Logging
		URL Filter
		Virtual Service Edge
		Workload Advanced Log
		Workload Connector VM
		Workload Tunnel Encryption
		Workload ZIA
		Z-API
		ZIA Bandwidth Premium
		ZIA-SSL
		ZIA Inline Guest WiFi
		Server and IOT Protection
		ZS-DECEPTION-STANDARD
		ZS-INSP-PRV
		ZSCALER CLIENT CONNECTOR
		Firewall Cloud IPS
		VPN - Site-to-site

Table 14. Vendor, Product and Licensing Details

7.2 Copyright and Disclaimer

THE CONTENT OF THIS REPORT IS PROTECTED BY UNITED STATES AND INTERNATIONAL COPYRIGHT LAWS AND TREATIES. YOU MAY ONLY USE THIS REPORT FOR YOUR PERSONAL, NON-COMMERCIAL, INFORMATIONAL PURPOSES. THIS REPORT WAS PREPARED BY SECUREIQLAB AS A COMMISSIONED REPORT. SUBJECT TO THE TERMS OF THE APPLICABLE AGREEMENT WITH SECUREIQLAB, THE COMMISSIONING PARTY MAY REPRODUCE, DISTRIBUTE, PUBLICLY DISPLAY, AND USE THIS REPORT, IN WHOLE OR IN PART, FOR COMMERCIAL, MARKETING, PROMOTIONAL, SALES, AND INFORMATIONAL PURPOSES. SUCH USE MUST NOT MATERIALLY ALTER OR MISREPRESENT THE FINDINGS, RESULTS, OR CONCLUSIONS OF THE REPORT. 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 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.

www.secureiqlab.com

COPYRIGHT © 2026 SECUREIQLAB INC. ALL RIGHTS RESERVED.

About Us

SecureIQLab Inc. is a U.S.-based independent, third-party cybersecurity solution validation and advisory provider. The SecureIQLab security methodology is tailored to what enterprises want, blending research, risk management, and data modeling performed by our deep bench of security experts. SecureIQLab is a member of the Anti-Malware Testing Standards Organization (AMTSO).

SECUREIQLAB INC.

9600 Great Hills Trail, Suite #150W

Austin, TX 78759 USA

+1.512.575.3457

www.secureiqlab.com

info@secureiqlab.com

SecureIQLab

Independent. Rigorous. Reproducible.

Evidence you can trust.