Independent Tests of
Anti-Virus Software

Secure Access Service Edge

SASE-Vergleichsbericht im Auftrag von Palo Alto Networks

Testzeitraum: September 2021 bis Februar 2022

Letzte Überarbeitung: 14. April 2022

Im Auftrag von: Palo Alto Networks

www.av-comparatives.org

Inhalt

Einleitung

Dieser Test wurde von Palo Alto Networks in Auftrag gegeben und sollte die Effizienz der führenden SASE-Lösungen (Secure Access Service Edge) in Bezug auf die Anforderungen moderner hybrider Arbeitsplätze evaluieren und vergleichen. Palo Alto Networks wählte die zu testenden Produkte, die in den eigenen Lösungen verwendeten Konfigurationen und die Testszenarien aus. Für die Konfiguration der anderen beiden Produkte wurden die vom jeweiligen Anbieter öffentlich empfohlenen Best Practices beachtet. Es ist möglich, dass die Testergebnisse mit anderen Einstellungen anders ausgefallen wären.

Heutzutage beschäftigen viele Unternehmen Mitarbeiter an diversen Standorten weltweit, zum Beispiel am Hauptsitz und in Filialen, und aufgrund der COVID-19-Pandemie hat auch die Zahl der Angestellten im Homeoffice zugenommen. Aber alle Beschäftigten müssen unabhängig von ihrem Standort auf die IT-Services, Anwendungen und Daten zugreifen können, die sich ebenfalls an unterschiedlichen physischen Standorten befinden. Dazu gehören Unternehmens-LAN, Rechenzentren (private Cloud) oder öffentliche Clouds. Die IT-Abteilungen stehen nun vor der Herausforderung, den Benutzern mithilfe passender Lösungen sicheren und standortunabhängigen Zugriff auf zulässige und verteilte Inhalte zu ermöglichen.

In der Vergangenheit wurden häufig mehrere Produkte eingesetzt, um den Benutzerzugriff auf verteilte Daten zu kontrollieren, doch dabei entsteht schnell ein Geflecht aus zahlreichen unterschiedlichen Systemen, die keinen umfassenden Überblick über die Zugriffsrichtlinien und Sicherheitseinstellungen ermöglichen. SASE-Lösungen (*Secure Access Service Edge*) sollen Abhilfe schaffen, da IT-Administratoren alle erforderlichen Sicherheitsmaßnahmen und Zugriffsberechtigungen über eine zentrale cloudbasierte Managementoberfläche/-architektur verwalten können.

Diese Lösungen bieten sicheren, optimierten und automatisierten Zugriff auf Anwendungen und Workloads in der Cloud, indem die softwaredefinierten Netzwerk- und Sicherheitsfunktionen bis zum Perimeter der großen IaaS- und SaaS-Anbieter erweitert werden. So ermöglichen sie standortunabhängigen, sicheren Zugriff über eine Managementplattform.

Ältere SASE-Lösungen boten zwar bereits eine bessere Kontrolle, waren aber extrem langsam. Mit den neuen Technologien jedoch müssen Unternehmen keine Abstriche mehr machen. Die neuen SASE-Lösungen ermöglichen Netzwerktraffic und Sicherheitsprioritäten, umfassenden Schutz vor Bedrohungen und Datenschutz sowie extrem schnelle, direkte Verbindungen zwischen Netzwerk und Cloud.

Sie werden eingesetzt, um einheitliche, umfassende Sicherheitsmaßnahmen für Benutzer und Anwendungen bereitzustellen, unabhängig von deren Standorten und den verwendeten Ports/Protokollen, und schädliche Aktivitäten von Insidern und/oder Benutzern, die sich versehentlich von einem infizierten Host verbinden, zu erkennen und zu verhindern. Aus diesem Grund sind umfassende Funktionen für den Bedrohungsschutz und die vollständige Abdeckung der Angriffsfläche (mehrere Angriffsvektoren) für Remotebenutzer und Mitarbeiter in Filialen wichtig. Dazu gehören auch Funktionen für die Kategorisierung von harmlosem und schädlichem Datenverkehr, die schnelle Prävention, Identifizierung und Erkennung von Bedrohungen, die Berichterstellung und einen umfassenden Überblick.

Getestete SASE-Lösungen

Über einen Testzeitraum von sechs Monaten (September 2021 bis Februar 2022) wurden die folgenden Produkte evaluiert:

- Cisco Umbrella
- Palo Alto Networks Prisma Access Enterprise
- Zscaler Internet Access

Vorbereitung des SASE-Tests

Für die Konfiguration der SASE-Lösungen wurden die Best Practices berücksichtigt. Palo Alto Networks gab die Einstellungen für seine eigenen Lösungen vor und bei den anderen beiden Produkten wurden die öffentlich verfügbaren Empfehlungen des jeweiligen Anbieters beachtet. Dazu gehörten verschiedene nahtlos integrierte Sicherheits- und Complianceanwendungen wie URL Filtering, Antivirenprogramme, Sandbox, Firewall, Funktionen zum Schutz vor komplexen Bedrohungen und vor Datenverlust (Data Loss Prevention), Funktionen zum Schutz von Cloud-Anwendungen und für das Bandbreitenmanagement für den Netzwerktraffic. Die Präventions- und Schutzfunktionen (Blockieren) waren aktiviert. Produktupdates waren zulässig. Alle Testszenarien wurden ohne Unterbrechung ausgeführt, sofern möglich.

Überblick über den SASE-Test

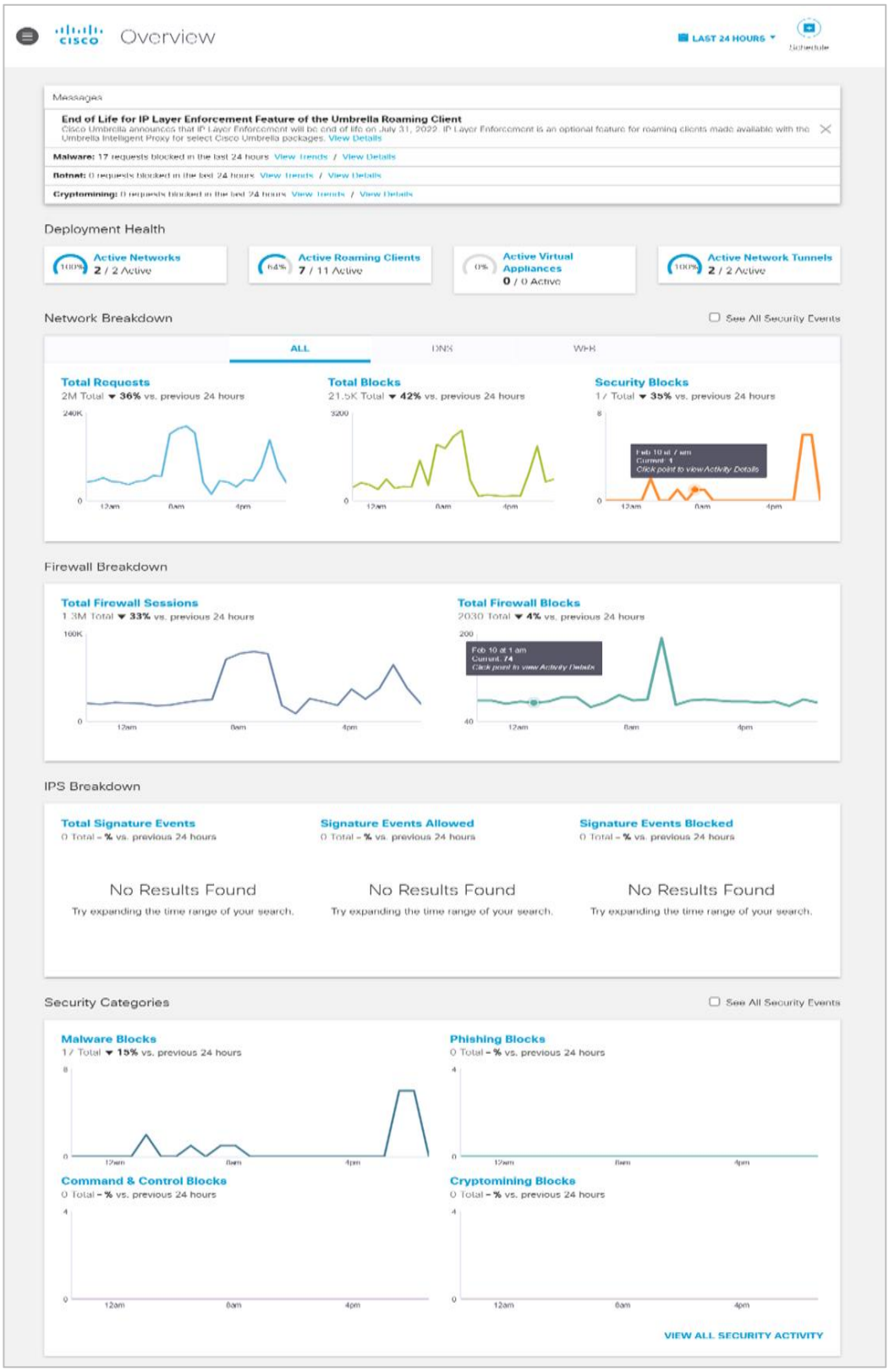
Im Rahmen des Tests wurden acht unterschiedliche untergeordnete Tests durchgeführt, von denen jeder einen wichtigen praxisrelevanten Aspekt der jeweiligen Produktfunktionen abdeckte. Die Tests für Web URL Filtering, DNS-Sicherheit und Malwareschutz wurden in weitere Unterkategorien aufgeteilt:

1. Web URL Filtering (Blockierungsrate für CnC-Verbindungen, Blockierungsrate für Malware, Blockierungsrate für Phishing, durchschnittliche Zahl der als harmlos eingestuften URLs)
2. DNS-Sicherheit (Verhinderung von DNS-Tunnelling, Schutz vor DGA)
3. Malwareschutz (Dauer der Sandbox-Analyse, Schutz vor modifizierter Malware, Malwareschutz für E-Mail-Protokolle, Extraktion von Artefakten, Dateiübertragung)
4. Sicherheit für öffentliche SaaS-Anwendungen
5. Sicherheit für private SaaS-Anwendungen
6. Schutz vor Sicherheitslücken
7. Schutz vor Umgehungsmethoden
8. Schutz vor dem Diebstahl von Anmeldedaten

Die detaillierten Testergebnisse für jedes Produkt werden im Bericht aufgeführt. Die Einstellungen der jeweiligen Lösung finden Sie im Anhang dieses Berichts im Abschnitt „Produkteinstellungen“.

Produktansichten

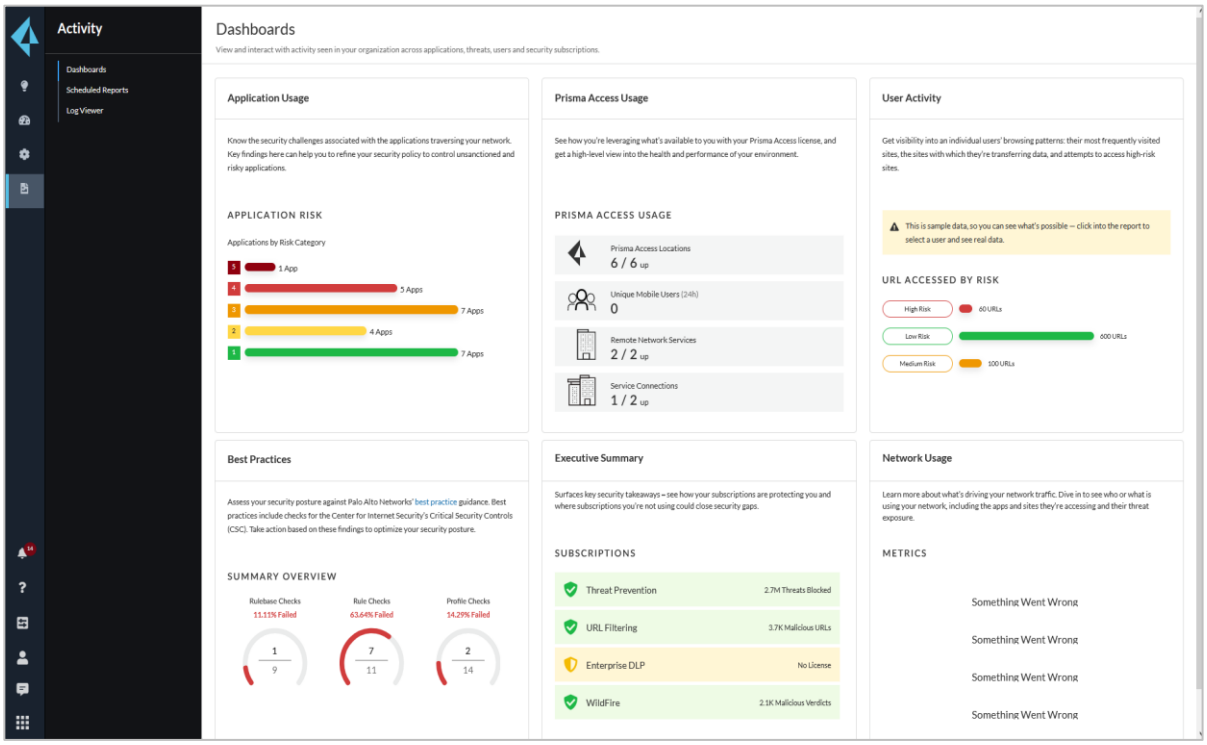
Cisco Umbrella



Cisco Umbrella

Die SASE-Lösung von Cisco erzielte in den folgenden Bereichen ausgezeichnete Ergebnisse: Verhinderung von DNS-Tunnelling, Schutz vor unbekannter Malware und Schutz vor modifizierter Malware.

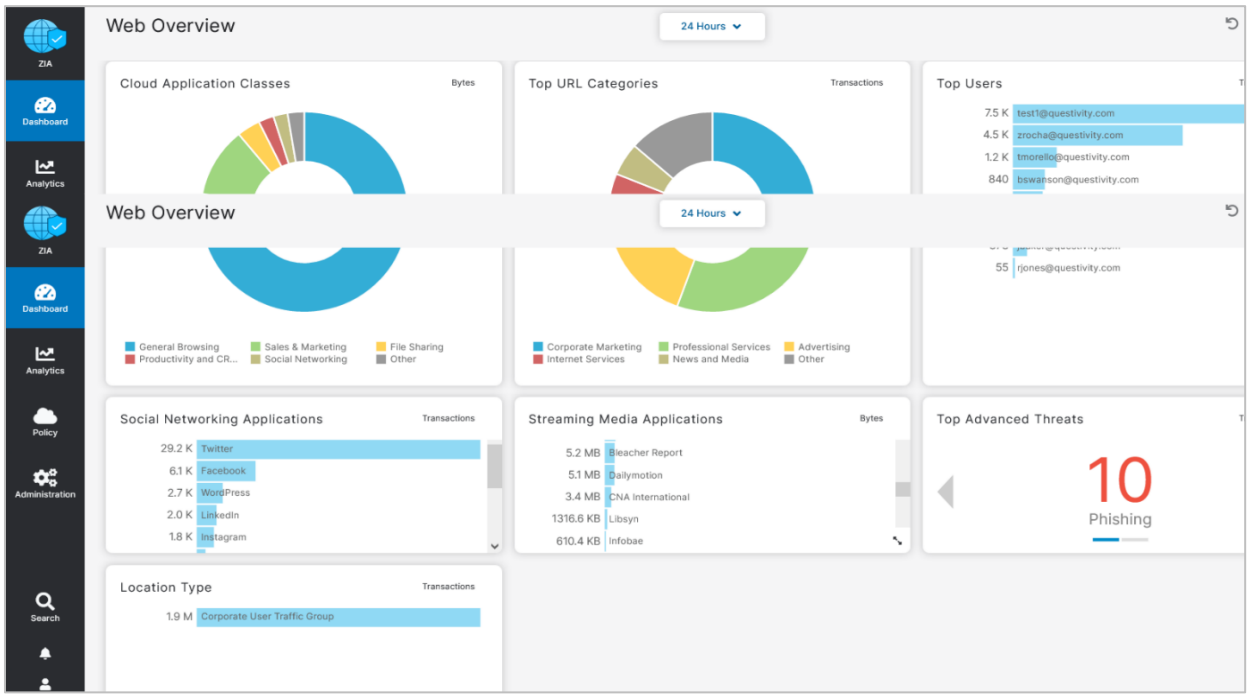
Palo Alto Networks Prisma Access Enterprise



Palo Alto Networks Prisma Access Enterprise

Die SASE-Lösung von Palo Alto Networks erzielte in den meisten Testbereichen ausgezeichnete Ergebnisse, zum Beispiel: Blockierungsrate für CnC-Verbindungen, Blockierungsrate für Malware, Blockierungsrate für Phishing, durchschnittliche Zahl der als harmlos eingestuften URLs, Schutz vor DNS-Tunnelling, Schutz vor DGA, Schutz vor modifizierter Malware, Malwareschutz für E-Mail-Protokolle, Dateiübertragung, Sicherheit für öffentliche SaaS-Anwendungen, Sicherheit für private SaaS-Anwendungen, Schutz vor Sicherheitslücken, Schutz vor Umgehungsmethoden und Schutz vor dem Diebstahl von Anmeldedaten. Bei dem Malwareschutz für E-Mail-Protokolle deckt Palo Alto Networks sowohl IMAP als auch SMTP ab. Bei der Extraktion von Artefakten unterstützt Palo Alto Networks zusätzlich zu PDF auch PPT.

Zscaler Internet Access



Zscaler Internet Access

Die SASE-Lösung von Zscaler erzielte ausgezeichnete Ergebnisse bei der durchschnittlichen Zahl der als harmlos eingestuften URLs.

Vergleichende Analyse von AV-Comparatives zu SASE-Lösungen

Aus der Übersicht über die wichtigsten Ergebnisse geht hervor, wie die drei Produkte in den acht unterschiedlichen Kategorien abgeschnitten haben.

SASE-Sicherheitskategorien	Cisco	Palo Alto Networks	Zscaler
1. Web URL Filtering			
Blockierungsrate für CnC-Verbindungen	37 %	**91 %**	63 %
Blockierungsrate für Malware	37 %	**84 %**	66 %
Blockierungsrate für Phishing	23 %	**78 %**	35 %
Durchschnittliche Zahl der als harmlos eingestuften URLs	81 %	**98 %**	97 %
2. DNS-Sicherheit			
Verhinderung und Protokollierung von DNS-Tunnelling	100 %	**100 %**	75 %
Schutz vor DGA	64 %	**100 %**	76 %
3. Malwareschutz			
Sandbox zum Schutz vor unbekannter Malware	n. v.	**Ja**	Ja
Schutz vor modifizierter Malware	85 %	**100 %**	16 %
Malwareschutz für E-Mail-Protokolle	SMTP	**IMAP/SMTP**	–
Extraktion von Artefakten	PDF	**PDF/PPT**	PDF
Dateiübertragung	n. v.	**Ja**	n. v.
Sicherheit für SaaS-Anwendungen			
4. Sicherheit für öffentliche SaaS-Anwendungen	Ja	**Ja**	Ja
5. Sicherheit für private SaaS-Anwendungen	n. v.	**Ja**	–
6. Schutz vor Sicherheitslücken	71 %	**100 %**	29 %
7. Schutz vor Umgehungsmethoden	50 %	**100 %**	100 %
8. Schutz vor dem Diebstahl von Anmeldedaten	n. v.	**Ja**	n. v.

Fazit

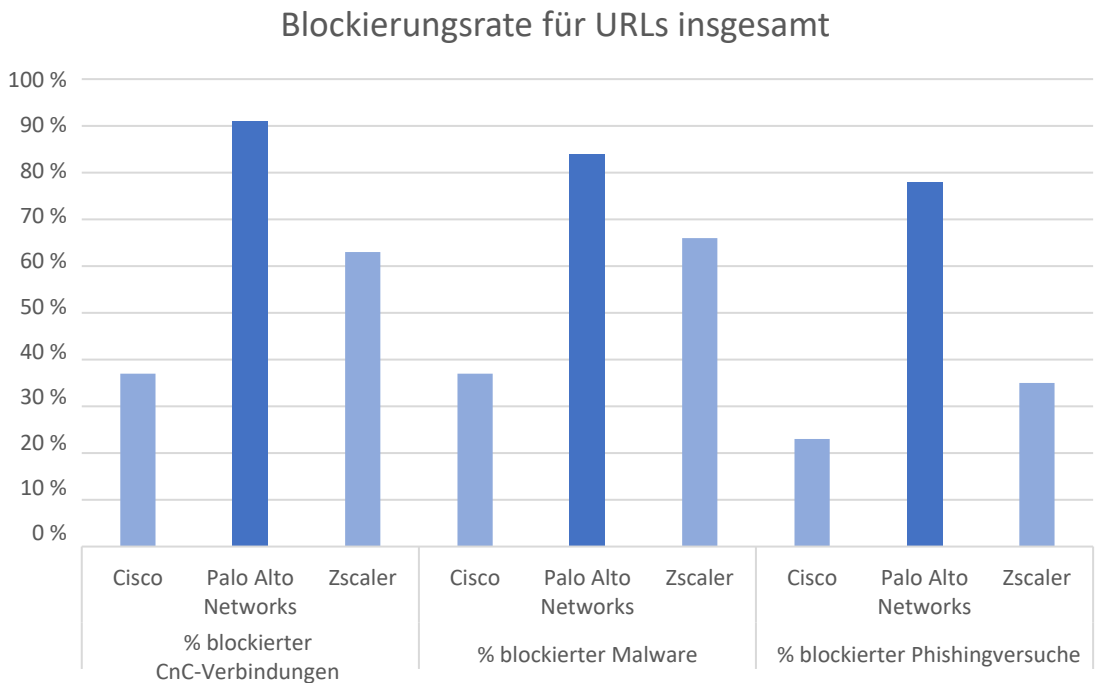
Bei diesem Vergleich der SASE-Lösungen, den Palo Alto Networks in Auftrag gegeben hatte, wurden verschiedene Funktionen getestet, die für Sicherheit an hybriden Arbeitsplätzen sorgen sollen, zum Beispiel URL Filtering, DNS-Sicherheit, Malwareschutz, Schutz vor Sicherheitslücken und Schutz vor dem Diebstahl von Anmeldedaten. In den meisten Testkategorien hat Palo Alto Networks am besten oder ebenso gut wie einer der anderen beiden Anbieter abgeschnitten. Bei den Tests zu URL Filtering hat es in allen drei Kategorien die höchsten Werte erzielt. Die Lösung von Palo Alto Networks bot auch als einziges Produkt Schutz vor dem Diebstahl von Anmeldedaten und Malwareschutz für das IMAP-Protokoll.

Die einzelnen untergeordneten Tests

In den folgenden Abschnitten sind die detaillierten Ergebnisse für die einzelnen untergeordneten Tests aufgeführt.

1. Web URL Filtering

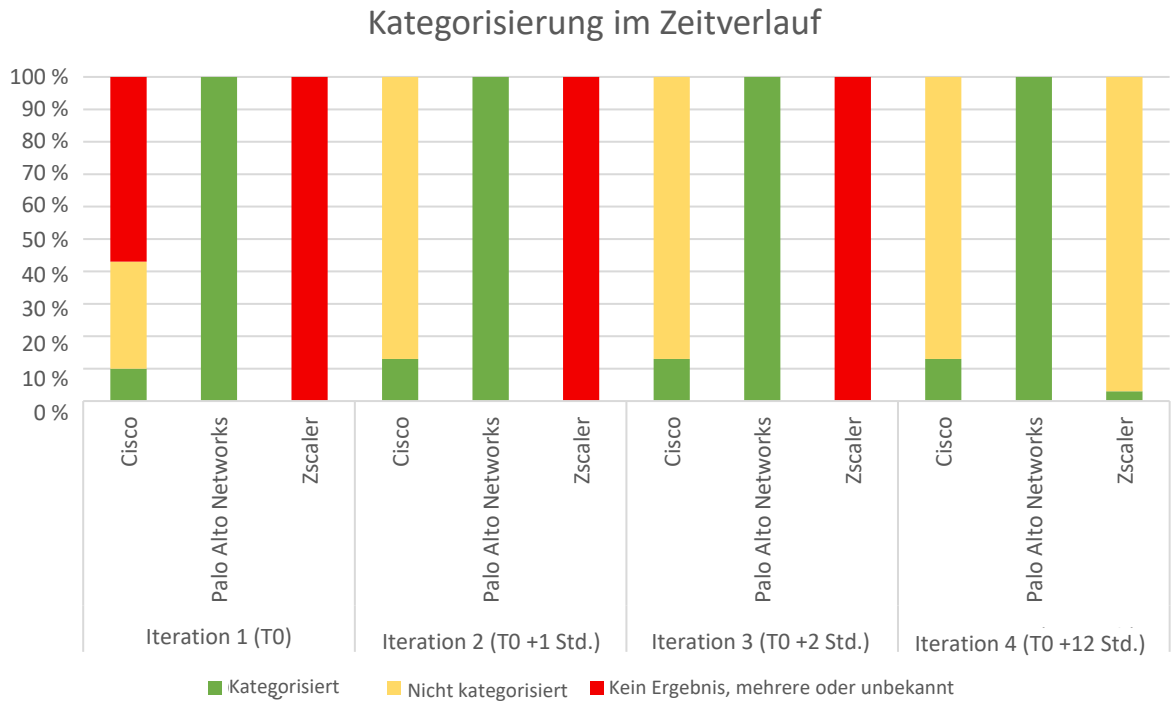
Unternehmen müssen festlegen, welchen Netzwerktraffic sie zulassen, und anschließend sicherstellen, dass sich die Beschäftigten daran halten. Effektive SASE-Lösungen sollten Inhalte korrekt identifizieren und gegebenenfalls blockieren können, falls diese gegen die Unternehmensrichtlinien verstoßen. Außerdem müssen sie in der Lage sein, URL-Kategorien zu unterscheiden und nach Bedarf Einschränkungen für bestimmte Kategorien durchzusetzen. Die Blockierung schädlicher URLs ist ein wichtiger Bestandteil des Bedrohungsschutzes in Unternehmen, doch ebenso wichtig ist, dass die Benutzer weiterhin harmlose, zulässige URL-Kategorien aufrufen können.



Blockierungsrate für URLs insgesamt

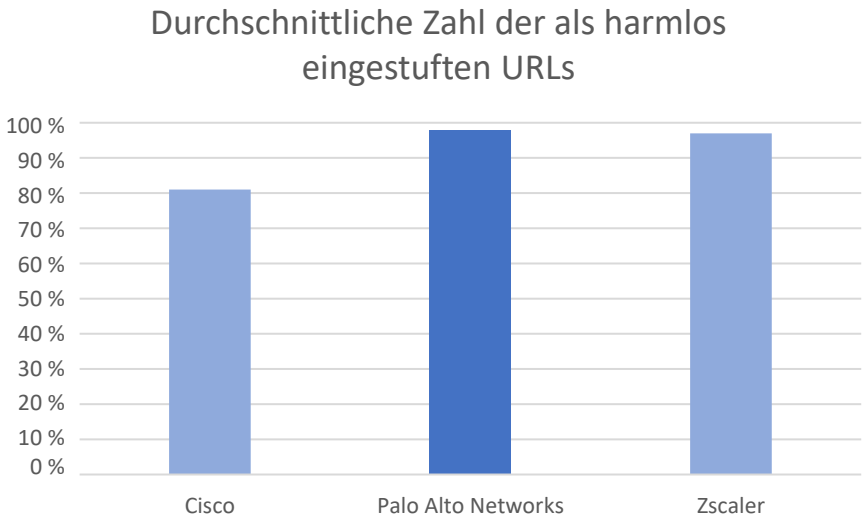
AV-Comparatives hat insgesamt mehr als 1.700 URLs in Bezug auf den Schutz vor schädlichen CnC-Verbindungen (Command-and-Control), Malware und Phishing getestet. Es soll an dieser Stelle noch einmal darauf hingewiesen werden, dass bei den Tests alle gemäß den Best Practices der jeweiligen Anbieter erforderlichen Funktionen aktiviert waren. Web-Filtering ist häufig eine Kombination aus DNS- und URL Filtering. Die DNS-Schutzfunktionen waren während des Tests aktiviert, um ein praxisrelevantes Szenario zu schaffen und die Best Practices zu berücksichtigen. Daher wurden eventuell einige URLs auf DNS-Ebene blockiert. In dem Diagramm oben sind die effektiven URL-Blockierungsraten für jeden Anbieter in jeder Testkategorie aufgeführt.

Es ist eindeutig erkennbar, dass Palo Alto Networks einen besseren Schutz vor schädlichen URLs bietet als seine Mitbewerber. Dies trifft auf alle Kategorien zu – CnC-Verbindungen, Malware und Phishing.



Kategorisierung neuer URLs/Domains im Zeitverlauf

Im Diagramm oben ist die Kategorisierung im Zeitverlauf für 30 neu erstellte URLs zu sehen. Der Kategorisierungstest startete einen Tag nach der Erstellung. Der erste Scan der neu erstellen URLs ist T0. Die nachfolgenden Iterationen fanden zu T0 plus 1 Stunde, 2 Stunden und 12 Stunden statt. Palo Alto Networks kategorisierte alle Domains/URLs bei der ersten Iteration. Die Kategorisierungs- und Alarmfunktionen von Cisco erreichten bei der ersten Iteration etwa 45 Prozent, bei Zscaler waren es 0 Prozent. Sowohl Cisco als auch Zscaler verbesserten ihre URL-/Domainkategorisierung in den nachfolgenden drei Iterationen.



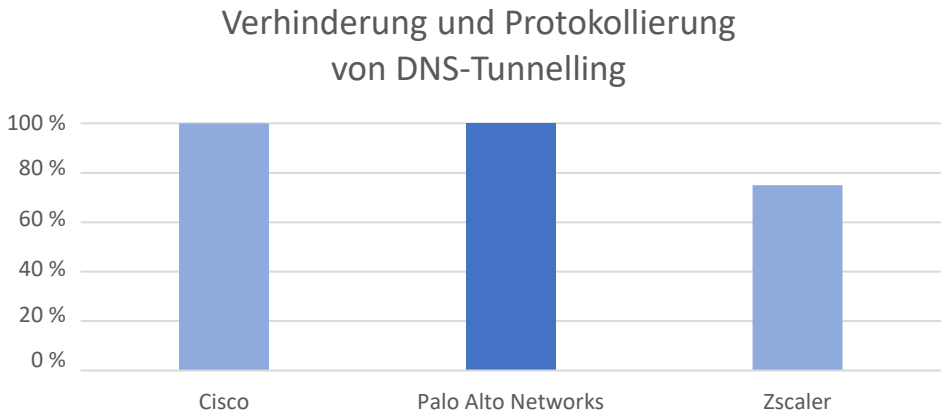
Durchschnittliche Zahl der als harmlos eingestuften URLs (%)

Im Diagramm oben ist die durchschnittliche Zahl der als harmlos eingestuften URLs in 429 Testfällen zu sehen. Zscaler erzielte mit durchschnittlich 97 Prozent in den sieben evaluierten Kategorien ein ausgezeichnetes Ergebnis für die Einstufung harmloser URLs für Mitarbeiter in Filialen und Remotebenutzer. Cisco erreichte einen Durchschnitt von 81 Prozent. Palo Alto Networks schnitt mit 98 Prozent am besten ab.

2. DNS-Sicherheit

Schutz vor DNS-Tunnelling

Hacker nutzen häufig DNS-Protokolle, um Daten auszuschleusen, Malware zu verbreiten oder CnC-Verbindungen einzurichten. Unternehmen hingegen überwachen nur selten den ein- und ausgehenden DNS-Datenverkehr in ihrer IT-Infrastruktur. SASE-Lösungen sollten Schutz vor DNS-Tunnelling bieten und DGA (Domain Generation Algorithms) erkennen können. Im nachfolgenden Diagramm sind die Ergebnisse unserer Tests zu vier unterschiedlichen DNS-Tunnelling-Methoden mit öffentlich verfügbaren Tools zu sehen. Dieser Funktionstest wurde mit den Standardports durchgeführt.

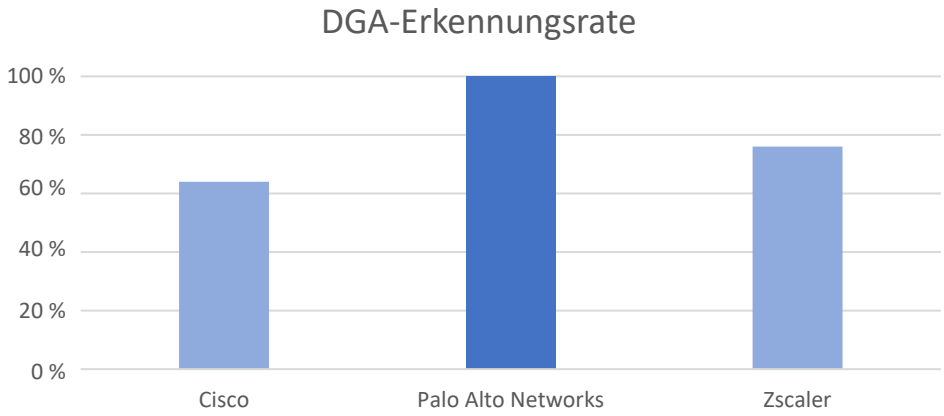


Verhinderung und Protokollierung von DNS-Tunnelling

Zwei Produkte bestanden alle vier DNS-Tunnelling-Tests.

Schutz vor DGA

DGA (Domain Generation Algorithms) werden schon lange von Malware-Entwicklern für CnC-Aktivitäten eingesetzt, da sie eine der effektivsten Methoden zur Umgehung von reputationsbasierten Abwehrmaßnahmen sind. Wir haben relevante Malwarefamilien ausgewählt, die während des Testzeitraums aktiv waren, und dann daraus fünf DGA mit jeweils fünf Samples generiert. Im nachfolgenden Diagramm sind die Erkennungs- und Blockierungsraten der SASE-Lösungen dargestellt.



Schutz vor DGA

Wie oben zu sehen ist, bot Palo Alto Networks eine effektive Abdeckung: Die Lösung identifizierte die schädliche DGA-Domain, stufte sie korrekt ein und blockierte sie anschließend. Die Lösung von Cisco konnte 64 Prozent der getesteten DGA-Techniken blockieren. Zscaler erzielte eine Erkennungs- und Blockierungsrate von 76 Prozent.

3. Malwareschutz

Unbekannte Malware

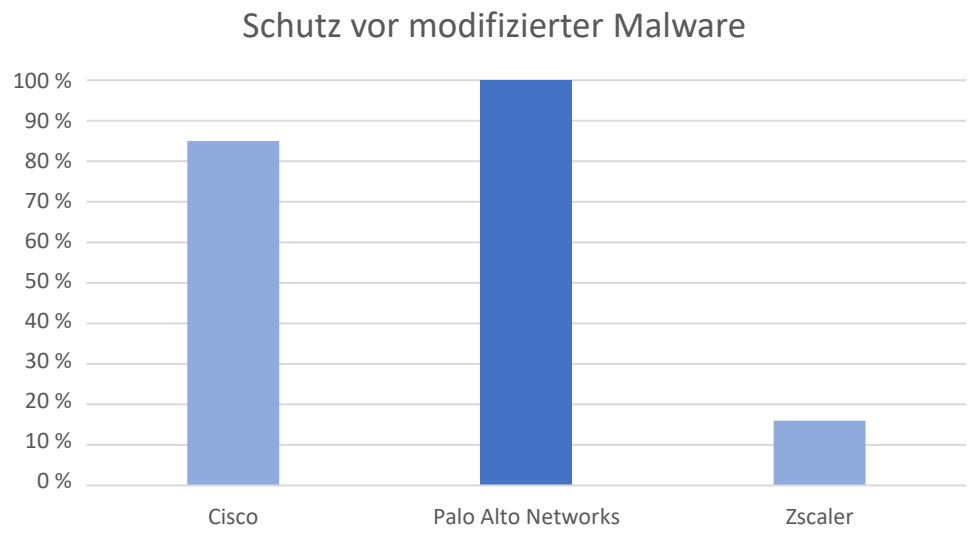
Die Blockierung unbekannter Malware ist eine wichtige Funktion der SASE-Lösungen. Damit wird sichergestellt, dass Benutzer vor unbekannten Angriffen geschützt sind, die andere Technologien nicht erkennen würden. SASE-Lösungen setzen dazu vor allem Sandboxes ein. Auf diese Weise können sie nicht nur Informationen zu den Angriffen ermitteln, sondern daraus auch angemessene Sicherheitsmaßnahmen ableiten. Sowohl Palo Alto Networks als auch Zscaler bietet eine Sandbox-Funktion für unbekannte Bedrohungen.

	Cisco	Palo Alto Networks	Zscaler
Sandbox zum Schutz vor unbekannter Malware	–	✓	✓

Sandbox-Funktion

Modifizierte Malware

Hacker verändern die zugrunde liegende Bedrohung, die bereits bekannt ist, mit unterschiedlichen Mechanismen, um Signatur-, Heuristik- oder Verhaltensschutzfunktionen zu umgehen. AV-Comparatives hat verschiedene Modifizierungstechniken eingesetzt, um die Schutzfunktionen der SASE-Lösungen zu unterwandern.



Schutz vor modifizierter Malware

Cisco und Palo Alto Networks verfügen über zuverlässige Sicherheitsfunktionen zur Abwehr solcher Angriffe.

Malwareschutz für E-Mail-Protokolle

SASE-Lösungen sollten die gängigen E-Mail-Protokolle unterstützen. Außerdem sollten sie relevante Informationen aus den E-Mail-Bedrohungen extrahieren können, zum Beispiel URLs, Verpackungstechniken oder Befehlszeilenparameter. Palo Alto Networks schützt sowohl vor IMAP- als auch vor SMTP-Protokollen, die Lösung von Cisco war nur bei dem SMTP-Protokoll effektiv. Zscaler konnte weder vor IMAP- noch vor SMTP-Protokollen schützen. Im nachfolgenden Diagramm sind die Ergebnisse zum Schutz für E-Mail-Protokolle dargestellt:

Anbieter	IMAP-Schutz	SMTP-Schutz
Cisco	–	✓
Palo Alto Networks	✓	✓
Zscaler	–	–

Malwareschutz für E-Mail-Protokolle

In der nachfolgenden Tabelle ist vermerkt, ob die Lösung der jeweiligen Anbieter relevante Threat Intelligence aus zwei gängigen Dateitypen extrahieren konnte:

Anbieter	Extraktion von Artefakten aus PDF	Extraktion von Artefakten aus PPT
Cisco	✓	–
Palo Alto Networks	✓	✓
Zscaler	✓	–

Funktionen zur Extraktion relevanter Threat Intelligence

Dateiübertragung

SASE-Lösungen sollten vor der bidirektionalen Übertragung von Schaddateien schützen. SMB ist eines der Protokolle, die Angreifer für diese Zwecke häufig ausnutzen. Palo Alto Networks konnte vor über SMB übertragener Malware schützen, die Lösungen von Cisco und Zscaler boten keinen Schutz vor diesem Angriffsvektor.

Anbieter	Schutz vor Dateiübertragung über SMB
Cisco	–
Palo Alto Networks	✓
Zscaler	–

Schutz vor Dateiübertragung über das SMB-Protokoll

4. Zugriff und Sicherheit für öffentliche cloudbasierte SaaS-Anwendungen

Eine umfassende Zero-Trust-SASE-Lösung sollte den bidirektionalen Datenverkehr sorgfältig überprüfen, unabhängig vom Standort der Benutzer und von den Ports oder Protokollen, die für den Zugriff auf öffentliche SaaS-Anwendungen in der Cloud genutzt werden. Außerdem sollten für solche Anwendungen detaillierte Zugriffskontrollen durchgesetzt werden.

Öffentliche SaaS-Anwendung	Cisco	Palo Alto Networks	Zscaler
Konsistente Unterscheidung zwischen Google Drive Business und der Version für Verbraucher	–	–	–
Konsistente Unterscheidung zwischen OneDrive Business und der Version für Verbraucher	–	✓	✓

Zugriffskontrolle für SaaS-Anwendungen

Bei der Evaluierung, ob die SASE-Lösungen bestimmte Anwendungstypen in der Cloud identifizieren und dann den Zugriff kontrollieren können, haben wir festgestellt, dass keines der drei getesteten Produkte in der Lage ist, konsistent zwischen der Business- und der Verbraucherversion von Google Drive zu unterscheiden. Diese Fertigkeit steht allerdings nicht unbedingt in direktem Zusammenhang mit der Bedrohungsprävention. Cisco war der einzige Anbieter, dessen Lösung nicht zwischen den beiden Versionen von OneDrive unterscheiden konnte (siehe Tabelle oben).

Effizienz der Sicherheitsmaßnahmen – Upload			
Öffentliche SaaS-Anwendung	Cisco	Palo Alto Networks	Zscaler
Box	–	✓	✓
Dropbox	–	✓	✓
Google Drive	–	✓	–
OneDrive	–	✓	✓

Übertragung schädlicher Dateien von Benutzern an öffentliche SaaS-Anwendungen

Palo Alto Networks erzielte konsistent hohe Erkennungs- und Blockierungsraten, wenn Benutzer versuchten, schädliche Samples (als Datei und in anderen Formaten) an öffentlich gehostete SaaS-Anwendungen zu übertragen. Die Lösung von Cisco verfügt über keine Funktionen, um diese Übertragungen in die Cloud zu erkennen. Zscaler erzielte ebenfalls hohe Erkennungs- und Blockierungsraten für Dropbox und OneDrive, konnte aber keine Übertragung an Google Drive erkennen (siehe Tabelle oben).

Effizienz der Sicherheitsmaßnahmen – Download			
Öffentliche SaaS-Anwendung	Cisco	Palo Alto Networks	Zscaler
Box	✓	✓	✓
Dropbox	✓	✓	✓
Google Drive	–	✓	–
OneDrive	✓	✓	✓

Übertragung schädlicher Dateien von öffentlichen SaaS-Anwendungen an Benutzer

Palo Alto Networks erzielte konsistent hohe Erkennungs- und Blockierungsraten für die Übertragung schädlicher Samples von öffentlichen SaaS-Anwendungen an Benutzer. Cisco erreichte ebenfalls hohe Erkennungs- und Blockierungsraten für Box und Dropbox, hatte aber kaum oder gar keinen Einblick in

Übertragungen von Google Drive und OneDrive. Zscaler erzielte konsistent akzeptable Erkennungs- und Blockierungsraten für Box, Dropbox und OneDrive, konnte aber keine Übertragungen von Google Drive erfassen. In der Tabelle oben ist erkennbar, welche Anbieter angemessene Sicherheitsmaßnahmen für die getesteten öffentlichen SaaS-Anwendungen boten.

5. Zugriff und Sicherheit für private/interne SaaS-Anwendungen

Testszenario	Cisco	Palo Alto Networks	Zscaler
Insiderbedrohung	n. v.	✓	–
Ausnutzung von Remotebenutzern	n. v.	✓	–
Bidirektionaler Malwareschutz (Standardports)	n. v.	✓	–
Bidirektionaler Malwareschutz (keine Standardports)	n. v.	✓	–

Inhaltsprüfung von Palo Alto Networks für private/interne SaaS-Anwendungen

Hinweis: Zum Zeitpunkt der Tests bot Cisco nicht die erforderlichen Funktionen an, sodass das Ergebnis „nicht verfügbar“ lautete. Die Lösung von Zscaler umfasste zwar entsprechend konfigurierte Funktionen, konnte aber für die oben genannten Szenarien keinen Schutz bieten.

Die Lösung von Palo Alto Network blockierte die Ausnutzung eines anfälligen Remotebenutzers von einer schädlichen Anwendung und umgekehrt (Insiderbedrohung). Nur Palo Alto Networks ermöglichte bidirektionalen Malwareschutz in ein- und ausgehendem Datenverkehr auf Standard- und anderen Ports für Remotebenutzer.

	Cisco	Palo Alto Networks	Zscaler
Zugriffskontrolle nach Benutzer	n. v.	✓	✓

Zugriffskontrolle nach Benutzer

Hinweis: Zum Zeitpunkt der Tests bot Cisco nicht die erforderlichen Funktionen an, sodass das Ergebnis „nicht verfügbar“ lautete. Bei den Lösungen von Palo Alto Networks und Zscaler konnten für einzelne Anwendungen detaillierte Zugriffsrichtlinien für jeden Benutzer durchgesetzt werden (siehe Tabelle oben).

6. Schutz vor Sicherheitslücken

Obwohl inzwischen viele Ressourcen ausgelagert werden, haben Netzwerkarchitekturen immer noch einen Perimeter, den der ein- und ausgehende Datenverkehr passieren muss. Auch die Benutzer benötigen – unabhängig von ihrem Standort – eine Verbindung zum Unternehmensnetzwerk. Aus diesem Grund müssen SASE-Lösungen sowohl den Client als auch den Server vor Sicherheitslücken schützen, deren Schweregrad im Common Vulnerability Scoring System (CVSS) als hoch oder kritisch eingestuft wurde. Es wurden sieben Sicherheitslücken mit einer CVSS-Bewertung von über 7,5 getestet.

Schutz vor Sicherheitslücken	Cisco	Palo Alto Networks	Zscaler
Schutz vor aktuellen Sicherheitslücken	100 %	100 %	50 %
Schutz von Remotebenutzern	100 %	100 %	50 %
Schutz von Remoteanwendungen	33 %	100 %	0 %
Schutz vor Sicherheitslücken insgesamt	**71 %**	**100 %**	**29 %**

Schutz vor Sicherheitslücken

Die Lösungen von Palo Alto Networks und Cisco haben die beiden aktuellen Sicherheitslücken identifiziert und entsprechende Bedrohungen erfasst und abgewehrt. Zscaler konnte bei dem Test nur vor einer der aktuellen Sicherheitslücken schützen.

Palo Alto Networks und Cisco konnten ihre Remotebenutzer vor Angriffen schützen, wenn diese versuchten, manipulierte oder schädliche Anwendungen im öffentlichen Internet aufzurufen oder zu nutzen. Zscaler bot in diesem Fall nur einen 50-prozentigen Schutz (siehe Tabelle oben unter „Schutz von Remotebenutzern“).

Palo Alto Networks erzielte konsistente Sicherheit für Remotebenutzer und Mitarbeiter in Filialen für alle Testszenarien in Bezug auf die Ausnutzung anfälliger Anwendungen im öffentlichen Internet. In der Tabelle oben ist erkennbar (unter „Schutz von Remoteanwendungen“), dass Palo Alto Networks 100-prozentigen Schutz für anfällige Anwendungen bot. Dies ist wichtig, wenn ein böswilliger Benutzer oder ein Angreifer versucht, über ein manipuliertes Benutzerkonto Remoteanwendungen oder -dienste im öffentlichen Internet auszunutzen. Die Rate von Cisco fiel in diesem Testszenario auf 33 Prozent und Zscaler erzielte 0 Prozent.

Das bedeutet, dass die Lösungen von Cisco und Zscaler zwar Remotebenutzer bis zu einem gewissen Grad vor schädlichen Anwendungen schützen, aber öffentlich erreichbaren Anwendungen keinen Schutz vor manipulierten Benutzerkonten oder Insiderbedrohungen bieten.

7. Schutz vor Umgehungsmethoden

Mit Umgehungsmethoden kann ein Angreifer die Malware/Exploits über einen gesonderten Pfad einschleusen oder die Inhalte modifizieren, um von den Sicherheitsfunktionen nicht entdeckt zu werden. Außerdem kann er bereits vorhandene Angriffstechniken ausnutzen, um die Sicherheitskontrollen zu unterwandern. In diesem Test haben wir überprüft, wie gut die Lösungen Umgehungsmethoden in sechs gängigen Angriffskategorien verhindern konnten.

Umgehungstechniken	Cisco	Palo Alto Networks	Zscaler
Kombination von Umgehungsmethoden	50 %	100 %	100 %
Grundlegende Drive-by-Umgehung	50 %	100 %	100 %
HTML-Umgehung	50 %	100 %	100 %
HTTP-Umgehung	50 %	100 %	100 %
Skriptverschleierung	50 %	100 %	100 %
TCP/IP-Umgehung	50 %	100 %	100 %

Schutz vor Umgehungsmethoden (Summe der Ergebnisse mit Standard- und anderen Ports)

Für jede Umgehungstechnik haben wir zwei Tests durchgeführt: einen mit den Standardports und einen mit anderen Ports. Mit den Standardports boten alle drei Lösungen Schutz vor Umgehungstechniken. Bei nicht standardmäßigen Ports war der Schutz der Lösung von Cisco allerdings in allen sechs getesteten Kategorien unzureichend.

8. Schutz vor dem Diebstahl von Anmeldedaten

Es sollte unbedingt verhindert werden, dass Anmeldedaten des Unternehmens auf verdächtigen Websites eingegeben oder durch Methoden kompromittiert werden, die Datenlecks hervorrufen. SASE-Lösungen müssen Phishingangriffe identifizieren und erfassen sowie anschließend die Übertragung von Benutzernamen oder Anmeldedaten für das Unternehmen erkennen und verhindern können. In der Tabelle unten sind die Ergebnisse für die Tests zu verschiedenen Phishingmethoden aufgeführt. Wir haben zwei Testszenarien überprüft.

Diebstahl von Anmeldedaten – Validierungstyp	Cisco	Palo Alto Networks	Zscaler
Identifizierung und Erfassung von Phishingangriffen im Zusammenhang mit Anmeldedaten	n. v.	✓	n. v.
Erkennung und Verhinderung der Übertragung von Benutzernamen auf Phishingwebsites	n. v.	✓	n. v.
Erkennung und Verhinderung der Übertragung von Anmeldedaten des Unternehmens	n. v.	✓	n. v.

Schutz vor dem Diebstahl von Anmeldedaten

Zum Zeitpunkt der Tests unterstützten Cisco und Zscaler keine Funktion zum Schutz vor dem Diebstahl von Anmeldedaten.

Anhang

Produkteinstellungen

Nachfolgend sind alle Produkteinstellungen, Konfigurationen und Funktionen der jeweiligen SASE-Lösung aufgeführt, die bei diesem Test aktiviert waren. Palo Alto Networks wählte die Konfigurationen für Prisma Access basierend auf seinen Best Practices aus. Für die Konfiguration der anderen beiden Produkte wurden die vom jeweiligen Anbieter öffentlich empfohlenen Best Practices beachtet. Es ist möglich, dass die Ergebnisse für diese Produkte mit anderen Einstellungen anders ausgefallen wären.

Palo Alto Networks:
URL Filtering: hohes Risiko, nicht jugendfrei, Command-and-Control, Urheberrechtsverletzungen, dynamisches DNS, Extremismus, Glücksspiel, Grayware, Hacking, unzureichende Inhalte, Malware, neu registrierte Domains, geparkte Domains, Peer-to-Peer, Phishing, Proxy-Umgehung und Anonymisierer, fragwürdig, unbekannt und Waffen.
DNS-Sicherheit: Command-and-Control-Domains, dynamische DNS-Domains, Grayware-Domains, Malwaredomains, neu registrierte Domains, geparkte Domains, Phishingdomains sowie Proxy-Umgehung und Anonymisierer.
Malwareschutz: Aktiviert.
IPS-Schutz: Für die Evaluierung des Schutzes vor Sicherheitslücken aktiviert.

Cisco:
URL Filtering: Command-and-Control-Callbacks und Phishingangriffe.
DNS-Sicherheit: Malware, neu entdeckte Domains, Command-and-Control-Callbacks, Phishingangriffe, dynamisches DNS, potenziell schädliche Domains, DNS-Tunnelling-VPN und Cryptomining.
Malwareschutz: Aktiviert.
IPS-Schutz: Für die Evaluierung des Schutzes vor Sicherheitslücken aktiviert.

Zscaler:
URL Filtering: Anonymisierer, Browserexploits, Command-and-Control-Server, Command-and-Control-Netzwerktraffic, Cookiediebstahl, Cryptomining, Sicherheitslücken zum Dateiformat, IRC-Tunnelling, bekannte Adware- und Spywarewebsites, bekannte Phishingwebsites, schädliche Inhalte und Websites, potenziell schädliche Anfragen, Spyware-Callback, SSH-Tunnelling, mutmaßliche Phishingwebsites, anfällige ActiveX-Steuerelemente, Webspam, Viren, unerwünschte Anwendungen, Trojaner, Würmer, Ransomware, Adware und Spyware.
DNS-Sicherheit: Phishing, schädliche Inhalte, neu registrierte Domains und DNS-over-HTTPS-Services.
Malwareschutz: Aktiviert.
IPS-Schutz: Für die Evaluierung des Schutzes vor Sicherheitslücken aktiviert.

Copyright und Haftungsausschluss

Weitere Informationen zu AV-Comparatives und den Testmethoden finden Sie auf der Website von AV-Comparatives.

AV-Comparatives
(April 2022)