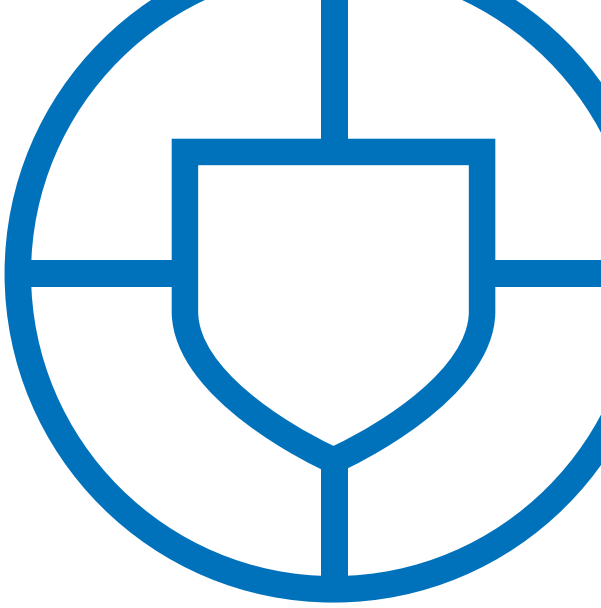
SOPHOS



Endpoint Security Buyers Guide

Cyberbedrohungen werden immer komplexer – somit wächst auch der Druck, die richtige Endpoint-Lösung für Ihr Unternehmen zu finden. Mittlerweile finden sich auf dem Markt für Endpoint Security allerdings so viele verschiedene Lösungen und so viele nicht haltbare Werbeversprechen, dass es immer schwerer wird, eine fundierte Entscheidung für Ihr Unternehmen zu treffen.

Dieser Guide sorgt für Klarheit: Er bietet einen Überblick über die zentralen Endpoint-Security-Technologien, damit Sie wissen, welcher Schutz der für Sie optimale ist. Zudem zeigen wir Ihnen, wie verschiedene Anbieter in unabhängigen Tests abschneiden, damit Sie eine fundierte Entscheidung treffen können.

Die unbequeme Wahrheit über Endpoint Security

Der Endpoint-Security-Markt ist voller übertriebener Behauptungen. Tatsache ist jedoch, dass 68 % aller Unternehmen im vergangenen Jahr Opfer eines Cyberangriffs waren. Deshalb ist ein leistungsstarker Schutz essenziell für den Erfolg jeder effektiven Sicherheitsstrategie.

Starke Schutztechnologien alleine reichen jedoch nicht aus. Vier von fünf Unternehmen räumen ein, dass ihnen kompetente Sicherheitsexperten fehlen*. Vor diesem Hintergrund sind benutzerfreundliche Sicherheitslösungen gefragt, mit denen knapp besetzte IT-Abteilungen das Potenzial ihrer Schutzfunktionen optimal ausschöpfen können. Außerdem sollten Sie sich über Folgendes bewusst sein: Bedrohungen kann es gelingen, Ihre Abwehrmechanismen zu durchbrechen. Für diesen Fall benötigt Ihr Unternehmen einen entsprechenden Schutz. Dazu gehört die vollständige Transparenz darüber, wie Bedrohungen in das Unternehmen eingedrungen sind, wohin Sie gelangt sind und welche Bereiche betroffen sind, damit Sie den Angriff neutralisieren und Sicherheitslücken schließen können.

In diesem Guide erhalten Sie einen Überblick über die verfügbaren Schutztechnologien und können eine fundierte Entscheidung darüber treffen, welches Endpoint Protection-Produkt sich für Ihre Anforderungen am besten eignet.

Produktfunktionen

Endpoint-Security-Lösungen werden manchmal auch einfach als Antivirus-Lösungen bezeichnet und können viele grundlegende (traditionelle) und moderne (Next-Gen) Techniken zur Abwehr von Endpoint-Bedrohungen enthalten. Beim Vergleich der Lösungen sollte Ihre Wahl auf eine Lösung mit einer breiten Palette leistungsstarker Techniken fallen, um möglichst viele Bedrohungen abwehren zu können. Genauso wichtig ist es, die Bedrohungen zu verstehen, die Sie abwehren möchten.

Endpoint-Bedrohungen

Obgleich sich die Bedrohungen ständig weiterentwickeln, haben wir im Folgenden einige der wichtigsten Endpoint-Bedrohungen aufgeführt, die Sie bei der Wahl Ihrer Lösung berücksichtigen sollten:

- **Portable Executables (Malware):** Schädliche Softwareprogramme (Malware) stehen oftmals im Mittelpunkt der Betrachtung rund um den Endpoint-Schutz. Es gibt sowohl bekannte als auch komplett unbekannte Malware. Manche Lösungen tun sich schwer damit, unbekannte Malware zu erkennen. Dieser Fakt ist enorm wichtig – unsere SophosLabs entdecken jeden Tag etwa vierhunderttausend bislang unbekannte Malware-Samples. Lösungen sollten in der Lage sein, gepackte und polymorphe Dateien aufzuspüren, die modifiziert wurden, um ihre Entdeckung zu erschweren.
- **Potenziell unerwünschte Anwendungen (PUAs):** PUAs sind zwar nicht unbedingt schädlich, aber vermutlich auch nicht erwünscht auf Ihrem Computer, wie z. B. Adware. Mit Blick auf Cryptomining und Cryptojacking spielt die PUA-Erkennung eine immer wichtigere Rolle.
- **Ransomware:** Über die Hälfte aller Unternehmen hatte im letzten Jahr Ransomware auf ihren Systemen, was im Durchschnitt zu einem Verlust von umgerechnet ca. 120.000 EUR führte[2]. Dateiverschlüsselung und Festplattenverschlüsselung sind die beiden Hauptformen von Ransomware. Bei der Dateiverschlüsselung werden die Dateien des Opfers verschlüsselt, bevor Lösegeld für ihre Entschlüsselung gefordert wird. Bei der Festplattenverschlüsselung werden nicht nur die Dateien, sondern die gesamte Festplatte des Opfers gesperrt oder vollständig gelöscht.
- **Exploit-basierte und dateilose Angriffe:** Nicht alle Angriffe nutzen Malware. Exploit-basierte Angriffe nutzen Software-Bugs und Schwachstellen aus, um sich Zugriff und Kontrolle über Ihren Computer zu verschaffen. Für diese Angriffe werden häufig schädliche Dokumente und Skripts genutzt. Bei schädlichen Dokumenten handelt es sich in der Regel um eines der Microsoft Office-Programme, das modifiziert wurde, um Schaden anzurichten, und bei schädlichen Skripts um schädlichen Code, der sich in seriösen Programmen und Websites verbirgt. Weitere Beispiele sind Man-in-the-Browser-Angriffe, die Malware nutzen, um einen Browser zu infizieren (damit der Angreifer den Datenverkehr überwachen und manipulieren kann) und Malicious Traffic, wobei Internetverkehr für kriminelle Zwecke genutzt wird, z. B. Kontaktaufnahme zu einem Command-and-Control-Server.

* Seven Uncomfortable Truths of Endpoint Security, März 2019. Von Sophos durchgeführte unabhängige Befragung von 3.100 IT-Managern aus 12 Ländern

- **Active Adversary-Techniken:** Endpoint-Angriffe bestehen häufig aus mehreren Phasen und wenden verschiedene Techniken an. Beispiele für Active Adversary-Techniken sind Privilege Escalation (Angreifer verschaffen sich erweiterten Zugriff auf ein System), Diebstahl von Zugangsdaten (Angreifer stehlen Benutzernamen und Passwort) und Code Caves (Angreifer verbergen schädlichen Code in seriösen Anwendungen).

Moderne (Next-Gen) Techniken und grundlegende (traditionelle) Techniken im Vergleich

Antivirus-Lösungen sind bereits seit einiger Zeit erhältlich, wenn auch mit unterschiedlichen Bezeichnungen, und haben sich bei der Bekämpfung bekannter Bedrohungen als sehr effektiv erwiesen. Traditionelle Endpoint Protection-Lösungen nutzen eine ganze Reihe von grundlegenden Techniken. Die Bedrohungslandschaft befindet sich jedoch im Wandel, und Bedrohungen wie z. B. komplett unbekannte Malware sind keine Seltenheit mehr. Aus diesem Grund haben sich neue Technologien am Markt etabliert. Suchen Sie nach einer Lösung, die eine Kombination aus modernen (Next-Gen) und grundlegenden (traditionellen) Techniken nutzt. Zu den Hauptfunktionen gehören:

Grundlegende Funktionen:

- **Anti-Malware/Antivirus:** Erkennung bekannter Malware auf Signaturbasis. Malware-Engines sollten nicht nur ausführbare Dateien, sondern auch z. B. schädlichen Javascript-Code auf Websites überprüfen können.
- **Application Lockdown:** Abwehr von schädlichen Verhaltensweisen von Anwendungen: Ein modifiziertes Office-Dokument installiert beispielsweise eine Anwendung und führt diese aus.
- **Verhaltensüberwachung/Host Intrusion Prevention Systems (HIPS):** Diese grundlegende Technologie schützt Computer vor unbekannten Viren und verdächtigem Verhalten. Sie sollte Verhaltensanalysen sowohl vor Ausführung als auch während der Laufzeit beinhalten.
- **Web Protection:** URL-Abruf und Blockierung von bekannten Schadseiten. Zu den blockierten Websites sollten Seiten gehören, die JavaScript-Code ausführen könnten (Cryptomining), und Seiten, die Benutzer-Authentifizierungsinformationen und andere sensible Daten stehlen.
- **Web Control:** Mit Endpoint Web Filtering können Administratoren festlegen, welche Dateitypen ein Benutzer aus dem Internet herunterladen kann.
- **Data Loss Prevention (DLP):** Wird ein Angriff zunächst nicht bemerkt, kann dank DLP die letzte Phase mancher Angriffe erkannt und abgewehrt werden, wenn der Angreifer versucht, Daten abzuschöpfen. Hierbei werden eine Reihe sensibler Datentypen überwacht.

Moderne Funktionen:

- **Machine Learning:** Es gibt unterschiedliche Arten von Machine Learning, wie etwa neuronale Deep-Learning-Netzwerke, Random Forest, Bayessche Netze sowie Clustering. Machine-Learning-Engines zur Erkennung von Malware müssen in jedem Fall bekannte und unbekannte Malware ohne Rückgriff auf Signaturen erkennen. Der Vorteil von Machine Learning ist, dass sich damit auch bisher unbekannte Malware erkennen lässt, was die Malware-Erkennungsrate erhöht. Unternehmen sollten auf die Erkennungsleistung, False Positive-Raten sowie mögliche Performance-Einbußen von Lösungen auf der Basis von Machine Learning achten.
- **Anti-Exploit:** Anti-Exploit-Funktionen wehren die Tools und Techniken ab, die sich Hacker bei Angriffen zunutze machen. So wurde die Ransomware WannaCry und NotPetya etwa über Exploits wie EternalBlue und DoublePulsar ausgeführt. Anti-Exploit-Technologie stoppt die verhältnismäßig geringe Anzahl an Techniken zur Verbreitung von Malware und Durchführung von Hacker-Angriffen. Dadurch lassen sich zahlreiche bisher unbekannte Zero-Day-Angriffe abwehren.
- **Spezieller Schutz vor Ransomware:** Manche Lösungen beinhalten Funktionen, um die unbefugte Verschlüsselung von Daten durch Ransomware zu verhindern. Häufig werden betroffene Dateien durch diese Anti-Ransomware-Technologie wieder in ihren Ursprungszustand versetzt. Allerdings sollten sich Anti-Ransomware-Lösungen nicht nur auf Dateien abzielende Ransomware beschränken, sondern auch Festplatten-Ransomware abwehren, die den Master Boot Record durch zerstörerische Löschangriffe schädigt.

- **Credential Theft Protection:** Diese Technologie verhindert den Diebstahl von Authentifizierungspasswörtern und Hash-Informationen aus dem Speicher, von der Registry oder der Festplatte.
- **Process Protection (Privilege Escalation):** Schutz, der explizit nach Prozessen sucht, in die zur Ausweitung der Berechtigungen ein privilegierter Authentifizierungstoken im Rahmen eines aktiven Angriffs eingebunden wurde. Unabhängig davon, welche Schwachstelle (bekannt oder unbekannt) ursprünglich zum Diebstahl des Authentifizierungstokens ausgenutzt wurde, sollte dies ein wirksamer Schutz sein.
- **Process Protection (Code Cave):** Abwehr von Techniken wie Code Cave und AtomBombing, die häufig bei Angriffen eingesetzt werden, die das Vorhandensein seriöser Anwendungen ausnutzen. Angreifer können diese Calls manipulieren und so andere Prozesse dazu bringen, ihren Code auszuführen.
- **Endpoint Detection and Response (EDR):** EDR-Lösungen sollten in der Lage sein, detaillierte Informationen für die gezielte Suche nach evasiven Bedrohungen zu liefern, damit die Durchsetzung von Sicherheitsvorgaben gewahrt bleibt und erkannte Vorfälle zuverlässig analysiert werden können. Es ist wichtig, die Komplexität und Benutzerfreundlichkeit der Lösung Ihrer Wahl auf die Größe und den Spezialisierungsgrad Ihrer Abteilung abzustimmen. Wählen Sie beispielsweise eine Lösung aus, die detaillierte Informationen und Handlungsempfehlungen zu Bedrohungen bietet, damit Sie schnell und einfach auf Bedrohungen reagieren können.
- **Reaktion auf Vorfälle/Synchronized Security:** Endpoint-Tools sollten zumindest Aufschlüsse über die Ursache von Vorfällen bieten, damit weiteren Vorfällen vorgebeugt werden kann. Im Idealfall reagiert die Lösung automatisch – ganz ohne Benutzerzugriff – auf Vorfälle. So können sich Bedrohungen nicht ausbreiten und noch mehr Schaden anrichten. Dabei müssen Tools, die auf Vorfälle reagieren, mit anderen Endpoint- und Netzwerk-Sicherheitstools kommunizieren.
- **Managed Threat Response (MTR):** MTR bietet Managed Detection and Response als 24/7 Fully-Managed-Service von einem Expertenteam Unsere Analysten reagieren auf potenzielle Bedrohungen, suchen nach „Indicators of Compromise" und liefern detaillierte Analysen der Ereignisse – was ist wo, wann, wie und warum passiert?

„Power of the Plus": Kombination verschiedener Techniken für umfassenden Endpoint-Schutz

Unternehmen sollten Endpoint-Lösungen nicht nur nach einer einzigen Hauptfunktion bewerten. Suchen Sie stattdessen nach einer Kombination aus leistungsstarken Funktionen, die sowohl moderne Techniken wie Machine Learning als auch grundlegende Techniken, die sich als sehr effektiv erwiesen haben, und Endpoint Detection and Response (EDR) zur Analyse und Reaktion auf Vorfälle beinhalten. Wenn Sie sich auf eine einzige, wenn auch branchenführende, Hauptfunktion verlassen, heißt das, Sie sind anfällig für eine primäre Fehlerquelle. Eine fundierte Sicherheitsstrategie, die zahlreiche starke Schutzschichten aufweist, wehrt eine breitere Palette an Bedrohungen ab. Das bezeichnen wir als „Power of the Plus" – eine Kombination aus grundlegenden Techniken, plus Machine Learning, plus Anti-Exploit, plus Anti-Ransomware, plus EDR, und vieles mehr.

Fragen Sie verschiedene Anbieter im Rahmen Ihrer Endpoint Security-Bewertung, welche Techniken in ihren Lösungen enthalten sind. Wie leistungsstark sind die Komponenten jeweils? Auf die Abwehr welcher Bedrohungen sind sie ausgelegt? Verlassen sie sich nur auf eine einzige grundlegende Technik? Aber was, wenn dieses Verfahren versagt?

Sophos im Vergleich zum Wettbewerb

Der Vergleich von Produkten mit unterschiedlichen Funktionen ist bereits schwierig. Der Vergleich ihrer Performance während simulierter Angriffe ist jedoch nahezu unmöglich, da die Aktivitäten der Angreifer potenziell unbegrenzt und unbekannt sind. Wenn Sie selbst einen Test durchführen möchten, finden Sie hier einen Testing Guide zur Hilfestellung. Viele Unternehmen setzen jedoch stattdessen auf die Bewertungen unabhängiger Dritter.

360-Grad-Bewertung und Zertifizierung

Im von MRG Effitas im 2. Quartal 2019 durchgeführten Endpoint-Test blockierte Sophos Intercept X die Testbedrohungen zu 100 %. Dies wurde mit den Standardeinstellungen von Intercept X Advanced erreicht, während die meisten anderen Produkte zusätzliche Schutzfunktionen für den Test bereitstellten.

Neben Sophos Intercept X erhielten auch Avira Antivirus Pro, Bitdefender Endpoint Security, CrowdStrike Falcon Protect, ESET Endpoint Security, F-Secure Computer Protection Premium, Kaspersky Small Office Security, Microsoft Windows Defender und Symantec Endpoint Protection eine Benotung der Stufe 1.

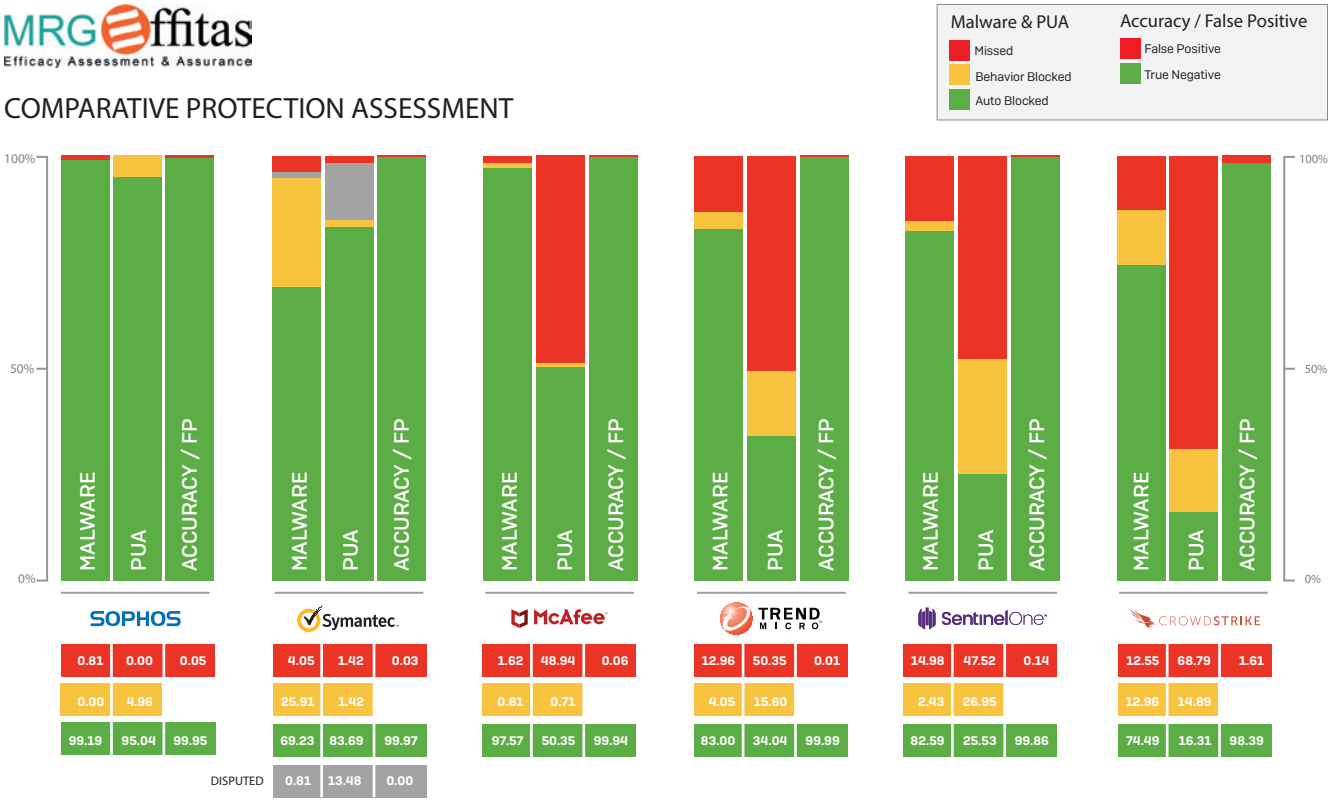
Testart	Ergebnis von Sophos
„In the Wild 360"-/Vollspektrumtest	Blockierrate von 100 %
Finanzielle Malware	Blockierrate von 100 %
Ransomware	Blockierrate von 100 %
PUA-/Adware-Test	Blockierrate von 100 %
„Exploit/dateilos"-Test	Blockierrate von 100 %
False-Positive-Test	0 False Positives

Avast Business Antivirus, McAfee Endpoint Security und Trend Micro Worry-Free Business Security fielen bei dem Test durch.

Lesen Sie hier den vollständigen Bericht.

MRG Effitas Malware Protection Test

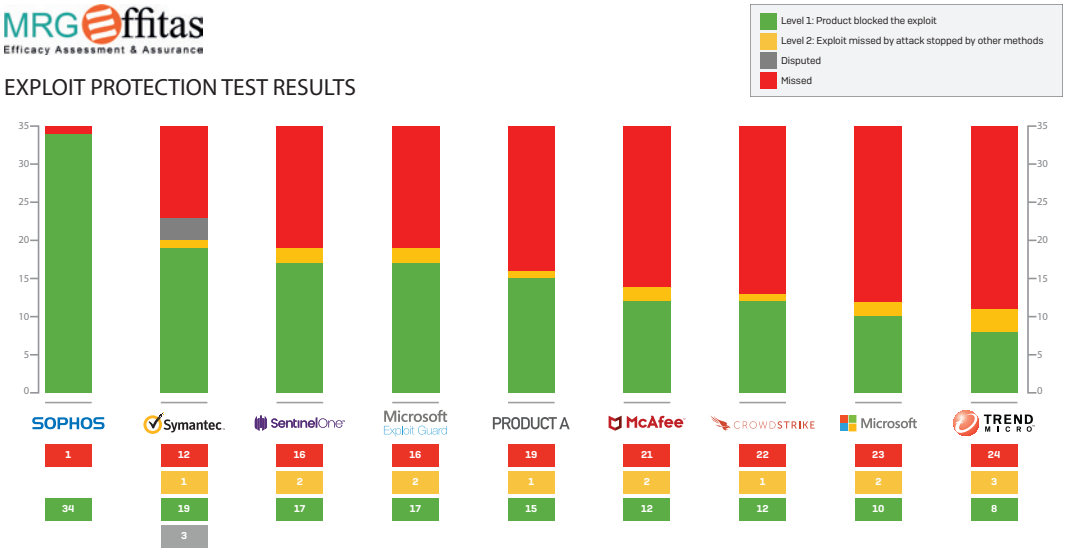
MRG Effitas hat eine Auftragsstudie durchgeführt, bei der die Fähigkeit von verschiedenen Endpoint-Protection-Produkten zur Erkennung von Malware und potenziell unerwünschten Anwendungen (PUAs) getestet und verglichen wurde. Sechs verschiedene Anbieter, darunter Sophos, wurden dabei genauestens unter die Lupe genommen. Sophos ist die Nr. 1 bei der Erkennung von Malware und die Nr. 1 bei der Erkennung von potenziell unerwünschten Anwendungen. Zudem überzeugten wir durch eine sehr niedrige False Positive-Rate.



Die vollständigen Testergebnisse finden Sie hier.

MRG Effitas Exploit and Post-Exploit Protection Test

Im Nachgang zur Auftragsstudie veröffentlichte MRG Effitas einen Bericht zum Vergleich verschiedener Endpoint-Lösungen für die Abwehr spezieller Exploit-Techniken. Sophos Intercept X setzt sich klar gegen die anderen getesteten Lösungen durch. Unsere Lösung konnte im Vergleich zu den meisten anderen getesteten Tools mehr als doppelt so viele Exploit-Techniken abwehren.



Den vollständigen Bericht finden Sie hier.

SE Lab Report: Endpoint Protection

SE Labs Endpoint Protection Report Sophos Intercept X Advanced erhielt im Endpoint Protection Test Report der SE Labs (Januar bis März 2020) sowohl in der Kategorie „Enterprise Endpoint Protection" als auch in der Kategorie „Small Business Endpoint Protection" 100 % in der Gesamtbewertung der Genauigkeit. Intercept X Advanced hat seit April 2018 in jedem Test der SE Labs eine AAA-Bewertung erhalten.

GESAMTBEWERTUNG DER GENAUIGKEIT			
Produkt	**Gesamtbewertung der Genauigkeit**	**Gesamtgenauigkeit (%)**	**Award**
Sophos Intercept X Advanced	1.136	100 %	AAA
ESET Endpoint Security	1.136	100 %	AAA
Kaspersky Small Office Security	1.136	100 %	AAA
Symantec Endpoint Protection Cloud	1.117	98 %	AAA
Trend Micro Worry-Free Security Services	1.114	98 %	AAA
McAfee Endpoint Security	1.107	97 %	AAA
Microsoft Windows Defender Enterprise	1.101	97 %	AAA
Bitdefender GravityZone Endpoint Security	1.099,5	97 %	AAA
Webroot SecureAnywhere Endpoint Protection	993	87 %	A

Quelle: SE Labs Small Business Protection, Januar bis März 2020

GESAMTBEWERTUNG DER GENAUIGKEIT			
Produkt	**Gesamtbewertung der Genauigkeit**	**Gesamtgenauigkeit (%)**	**Award**
Sophos Intercept X Advanced	1.136	100 %	AAA
ESET Endpoint Security	1.136	100 %	AAA
Kaspersky Small Office Security	1.136	100 %	AAA
Symantec Endpoint Protection Cloud	1.117	98 %	AAA
McAfee Endpoint Security	1.107	97 %	AAA
Microsoft Windows Defender Enterprise	1.101	97 %	AAA
Bitdefender GravityZone Endpoint Security	1.099,5	97 %	AAA
Crowdstrike Falcon	1.089	96 %	AAA
VIPRE Endpoint Security	1.087	96 %	AAA
FireEye Endpoint Security	1.052	93 %	AA

Quelle: SE Labs Enterprise Protection, Januar bis März 2020

Gartner Magic Quadrant für Endpoint Protection Platforms

Source: Gartner (August 2019)

Der Gartner Magic Quadrant für Endpoint Protection Platforms bewertet die Position von Anbietern am Markt in Bezug auf ihre Vollständigkeit der Vision und ihre Umsetzungskompetenz. Sophos wurde zum elften Mal in Folge als Leader im Gartner Magic Quadrant für Endpoint Protection Platforms positioniert. Gartner lobte Sophos für seine leistungsstarke Endpoint Security, die praxisgerechte Endpoint Detection and Response (EDR) Usability sowie die zentrale Plattform Sophos Central. Gartner hob unsere bewährte Ransomware-Abwehr, die Deep-Learning-Technologie zur Blockierung komplett unbekannter Malware und unsere Anti-Exploit-Technologie lobend hervor. Gartner zufolge hat Sophos mit dem Erfolg von Sophos Intercept X „seine SMB-Wurzeln hinter sich gelassen und konnte seine Brand Awareness in Unternehmen steigern".

The Forrester Wave™: Endpoint Security Suites

Forrester führt umfangreiche Produkttests für seinen unabhängigen Report durch und befragt dafür sowohl Endpoint-Anbieter als auch Kunden. Die Anbieter werden nach ihrem Produkt und nach ihrer Strategie bewertet. Sophos wurde im Forrester Wave Report erneut als Leader im Bereich Endpoint Protection Suites eingestuft.

Den vollständigen Bericht finden Sie hier.

ESG Labs Review: Intercept X

Die Labs der Enterprise Strategy Group haben Sophos Intercept X getestet und festgestellt:

„Intercept X wehrte 100 % der Exploit-Techniken ab, die von der traditionellen Antivirus-Anwendung übersehen wurden."[3]

Den vollständigen Bericht finden Sie hier.

AV-Comparatives

Intercept X hat erstmals am Business Security Test teilgenommen und erreichte den 1. Platz bei Malware-Erkennung. Die Erkennungsleistung lag bei 99,7 % mit nur einem Fehlalarm unter realen Testbedingungen und bei 99,9 % mit überhaupt keinem Fehlalarm im Malware-Test.

	Malware-Schutzrate	Fehlalarme bei gängiger Geschäftssoftware
Avast, Bitdefender, Panda, Sophos, SparkCognition	99,9 %	0
Cisco, Symantec, Trend Micro	99,8 %	0
K7, McAfee	99,7 %	0
Seqrite	99,6 %	0
FireEye, Microsoft	99,5 %	0
CrowdStrike, Endgame, VIPRE	99,2 %	0
Kaspersky Lab	99,0 %	0
Fortinet	98,9 %	0
ESET	99,5 %	0

Quelle: AV-Comparatives Business Security Test Januar bis März 2020

PC Magazine

Intercept X erhielt eine „Excellent"-Bewertung und den „Editor's Choice"-Preis.

Das PC Magazine bezeichnete Intercept X als „Sofortgewinn für alle, die nach einer Abwehr von Ransomware für Unternehmen jeder Größe suchen". Zudem verfüge Intercept X über „eine Vielzahl leistungsstarker Funktionen zum Schutz vor Malware jeder Art. Intercept X hat sich das Lob mehrerer unabhängiger Institute sowie unser Prädikat „Editor's Choice" für Ransomware-Schutz in der Zusammenfassung unseres Geschäftsberichts verdient."

Quelle: https://www.pcmag.com/review/366727/sophos-intercept-x-endpoint-protection

AV-Test (Mac)

Mit 6/6 Punkten bei der Schutzwirkung, 6/6 Punkten bei der Benutzbarkeit und 6/6 Punkten bei der Geschwindigkeit erreichte Sophos als einziger Anbieter von Endpoint-Schutz für Mac die volle Punktzahl.

Quelle: https://www.av-test.org/en/antivirus/business-macos/macos-mojave/june-2019/sophos-endpoint-9.8-191636/

Intercept X: Bestnoten in unabhängigen Tests und Analyseberichten

SE Labs

- AAA-Bewertung in der Enterprise-Klasse – 100 % in der Gesamtbewertung der Genauigkeit
- AAA-Bewertung in der SMB-Klasse – 100 % in der Gesamtbewertung der Genauigkeit
- AAA-Bewertung in der Consumer-Klasse – 100 % in der Gesamtbewertung der Genauigkeit

AV-Comparatives

- 1. Platz beim Malware-Schutz (99,9 % Erkennungsleistung, keine Fehlalarme)

MRG Effitas

- 1. Platz beim Malware-Schutz
- 1. Platz beim Exploit-Schutz
- Blockierrate von 100 %, keine False Positives – umfassende Bewertung

PC Magazine

- Editor's Choice

AV-Test

- Top-Produkt: Schutzwirkung: 6/6 – Benutzbarkeit: 6/6 – Geschwindigkeit: 5,6/6
- Nr. 1 beim MacOS-Schutz: Schutzwirkung: 6/6 – Benutzbarkeit: 6/6 – Geschwindigkeit: 6/6
- AV-Test (Android): Bestnoten

Gartner

- Leader: Magic Quadrant für Endpoint Protection Platforms (2019)

Forrester

- Leader: Wave 2018, Endpoint Security

Sorgen Sie für noch mehr Sicherheit: Sicherheitspakete für umfassenden Schutz

Eine Endpoint Security-Lösung ist jedoch nur ein Teil einer unternehmensweiten Sicherheitsstrategie. Unternehmen sollten sich heute nicht mehr ausschließlich auf Endpoint-Schutz konzentrieren, sondern die gesamte Umgebung berücksichtigen.

Idealerweise bietet Ihnen ein einziger Anbieter ein Komplettpaket an Lösungen, die perfekt aufeinander abgestimmt sind und im gesamten Unternehmen für einheitliche Sicherheit und Richtliniendurchsetzung sorgen. So erhalten sie nicht nur bessere IT-Sicherheit, sondern können auch ihren Verwaltungsaufwand und ihre Kosten senken.

Wir empfehlen, neben Endpoint-Schutz auch die folgenden Technologien in Erwägung zu ziehen: Festplattenverschlüsselung, Mobile Device Management, Mobile Security, Secure Email Gateway, spezieller Schutz für Server oder virtuelle Maschinen sowie Synchronized Security zwischen Endpoints und Netzwerkgeräten.

Sorgen Sie für noch mehr Sicherheit: Endpoint Detection & Response

Sophos Intercept X Advanced ist die erste EDR-Lösung, die speziell entwickelt wurde, um IT-Administratoren und Sicherheitsanalysten bei Anwendungsfällen in IT Operations und beim Threat Hunting zu unterstützen. Mit Sophos Intercept X Advanced können Sie beliebige Abfragen dazu erstellen, was in der Vergangenheit passiert ist und was momentan auf Ihren Endpoints passiert. Diese Abfragen können Sie entweder zum Threat Hunting nutzen, um aktive Angreifer zu erkennen, oder aber um sicherzustellen, dass in IT Operations Sicherheitsvorgaben eingehalten werden. Wenn ein Problem gefunden wird, haben Sie per Remote-Zugriff die Möglichkeit, gezielte Maßnahmen zu ergreifen.

Erstellen Sie Threat Hunting und IT Security Operations Reports, z. B.:

- Versuchen Prozesse, eine Netzwerkverbindung über Nicht-Standardports herzustellen?
- Welche Geräte verfügen über bekannte Schwachstellen, unbekannte Dienste oder nicht autorisierte Browser-Erweiterungen?
- Ausmaß und Folgen von Sicherheitsvorfällen verstehen
- Angriffe aufspüren, die eventuell noch nicht bemerkt wurden
- Netzwerkweite Suche nach Kompromittierungsindikatoren
- Ereignisse für die weitere Analyse priorisieren
- Dateien analysieren und bestimmen, ob es sich um Bedrohungen bzw. potenziell unerwünschte Anwendungen handelt
- Jederzeit den aktuellen Sicherheitsstatus ihres Unternehmens melden

Sophos Intercept X bietet viele Vorteile:

- EDR in Kombination mit dem stärksten Endpoint-Schutz
- Leistungsstarke, vorformulierte SQL-Abfragen, die Ihnen die erforderlichen Details liefern
- Deep Learning-Malware-Analyse übernimmt die Aufgaben von Malware-Analysten
- Jederzeit abrufbare Bedrohungsdaten aus den SophosLabs
- Machine Learning zur Erkennung und Priorisierung verdächtiger Ereignisse
- Schnell erreichbare, leistungsstarke EDR dank geführter Analysen
- Reaktion auf Vorfälle mit einem einzigen Klick

24/7 Experten-Service: Managed Threat Response

Mit Sophos MTR (Managed Threat Response) erhält Ihr Unternehmen ein Expertenteam, das für Sie gezielte Maßnahmen ergreift, um selbst hochkomplexe Bedrohungen unschädlich zu machen. Vorteile:

- 24/7 indizienbasiertes Threat Hunting
- Security Health Checks
- Aktivitätsreports
- Direkter Telefon-Support und dedizierter Ansprechpartner
- Modernster Schutz vor aktuellen Bedrohungen mit Intercept X

	Sophos Intercept X Advanced	Sophos Intercept X Advanced with EDR	Sophos MTR Standard	Sophos MTR Advanced
Traditionelle Techniken	✓	✓	✓	✓
Deep Learning	✓	✓	✓	✓
Anti-Exploit	✓	✓	✓	✓
CryptoGuard Anti-Ransomware	✓	✓	✓	✓
Endpoint Detection and Response (EDR)		✓	✓	✓
24/7 Monitoring und Reaktion			✓	✓
Indizienbasiertes Threat Hunting			✓	✓
Erweitertes indizienloses Threat Hunting				✓

Endpoint Security bewerten: 10 Fragen, die Sie auf jeden Fall stellen sollten

Bei der Auswahl der richtigen Endpoint Protection-Lösung sollten Sie dem Anbieter zunächst folgende Fragen stellen:

1. Nutzt das Produkt grundlegende oder moderne Techniken oder eine Kombination aus beiden? Welche speziellen Funktionen stehen im Mittelpunkt der Technologie?
2. Wie spürt das Produkt unbekannte Bedrohungen auf? Nutzt das Produkt Machine Learning?
3. Bei Angabe, dass Machine Learning genutzt wird: Welche Form von Machine Learning wird genutzt? Woher stammen die Trainingsdaten? Wie lange wird dieses Modell bereits genutzt?
4. Sind Funktionen zum Schutz vor Exploit-basierten und dateilosen Angriffen vorhanden? Welche Anti-Exploit-Technologien werden eingesetzt und welche Angriffsmethoden erkennen sie?
5. Beinhaltet die Lösung eine spezielle Technologie zur Abwehr von Ransomware?
6. Kann der Anbieter seinen Ansatz durch unabhängige Testergebnisse bestätigen?
7. Kann das Produkt detaillierte Fragen zum Threat Hunting und zu IT Security Operations beantworten? Wie lange werden die Daten der Suchanfragen gespeichert?
8. Welche Informationen liefert der Anbieter über Bedrohungen, z. B. Ursachenanalyse?
9. Reagiert das Produkt automatisch auf eine Bedrohung? Kann es Bedrohungen automatisch entfernen und auf Vorfälle reagieren?
10. Ermöglicht das Produkt Remote-Zugriff auf Geräte, um weitere Analysen vorzunehmen und erforderliche Maßnahmen zu ergreifen?

Fazit

Cyberbedrohungen entwickeln sich nach wie vor mit alarmierender Geschwindigkeit und werden immer raffinierter. Aus diesem Grund ist effektiver Endpoint-Schutz unerlässlich. Das Wissen um die Bedrohungen, die Sie abwehren müssen, und um die verschiedenen Technologien, die Ihnen dafür zur Verfügung stehen, helfen Ihnen, eine fundierte Entscheidung zu treffen und den besten Schutz vor den Angriffen von heute für Ihr Unternehmen zu finden.

Quelle:

1 State of Endpoint Security Survey 2018

2 State of Endpoint Security Survey 2018

3 MRG Effitas Comparative Malware Protection Assessment, Februar 2018

Gartner Magic Quadrant für Endpoint Protection Platforms, Ian McShane, Eric Ouellet, Avivah Litan, Prateek Bhajanka, 24. Januar 2018 Gartner befürwortet in seinen Forschungsbeiträgen keine bestimmten Hersteller, Produkte oder Dienstleistungen und rät Technologie-Nutzern nicht ausschließlich zu Anbietern mit besten Bewertungen. Forschungsbeiträge von Gartner sind als Meinungsäußerungen des Gartner Forschungsinstituts einzustufen und in keinem Fall als Tatsachenfeststellung zu werten. Gartner übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus.

The Forrester Wave™: Endpoint Security Suites, Q4 2016 von Chris Sherman, 19. Oktober 2016.

Sophos Intercept X jetzt kostenfrei testen

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2020-05-13 WP-DE (PS)

SOPHOS