SOPHOS

Endpoint Security Buyers Guide

Cyberbedrohungen werden immer komplexer – damit wächst auch der Druck, sich mit der richtigen Endpoint-Lösung optimal zu schützen. Mittlerweile gibt es im Bereich Endpoint Security allerdings so viele verschiedene Lösungen und Werbeversprechen, dass es immer schwerer wird, die richtige Lösung für Ihr Unternehmen zu finden.

Dieser Guide sorgt für Klarheit: Er bietet einen Überblick über die zentralen Endpoint-Security-Technologien, damit Sie beurteilen können, 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[1]. 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[1]. 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 muss Ihr Unternehmen entsprechend gerüstet sein. 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. Damit können Sie eine fundierte Entscheidung darüber treffen, welches Endpoint-Protection-Produkt sich für Ihre Anforderungen am besten eignet.

Produktfunktionen und Bedrohungsarten

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

Bedrohungen entwickeln sich ständig weiter und neue Bedrohungsarten kommen hinzu. Da fällt es schwer, den Überblick zu behalten. Im Folgenden finden Sie deshalb eine Liste der wichtigsten Endpoint-Bedrohungen, 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.

- **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.
- **Extended Detection and Response (XDR):** XDR geht über Endpoints und Server hinaus und berücksichtigt auch weitere Datenquellen (u. a. Firewalls, E-Mails und Mobilgeräte). Es wurde entwickelt, um Unternehmen einen ganzheitlichen Überblick über ihre gesamte Umgebung zu verschaffen und bei Bedarf jederzeit Detailinformationen abzurufen. All diese Informationen sollten an einem zentralen Ort (in der Regel als „Data Lake" bezeichnet) korreliert werden, an dem Benutzer geschäftskritische Fragen stellen und beantworten 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": Eine 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 4. Quartal 2020 durchgeführten Endpoint-Test blockierte Sophos Intercept X die Testbedrohungen zu 100 %. Neben Sophos Intercept X schafften es Bitdefender Endpoint Security und Malwarebytes Endpoint Protection auf die höchste Bewertungsstufe (Level 1). ESET Endpoint Security, F-Secure Computer Protection Premium und Microsoft Windows Defender erhielten Level 2.

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

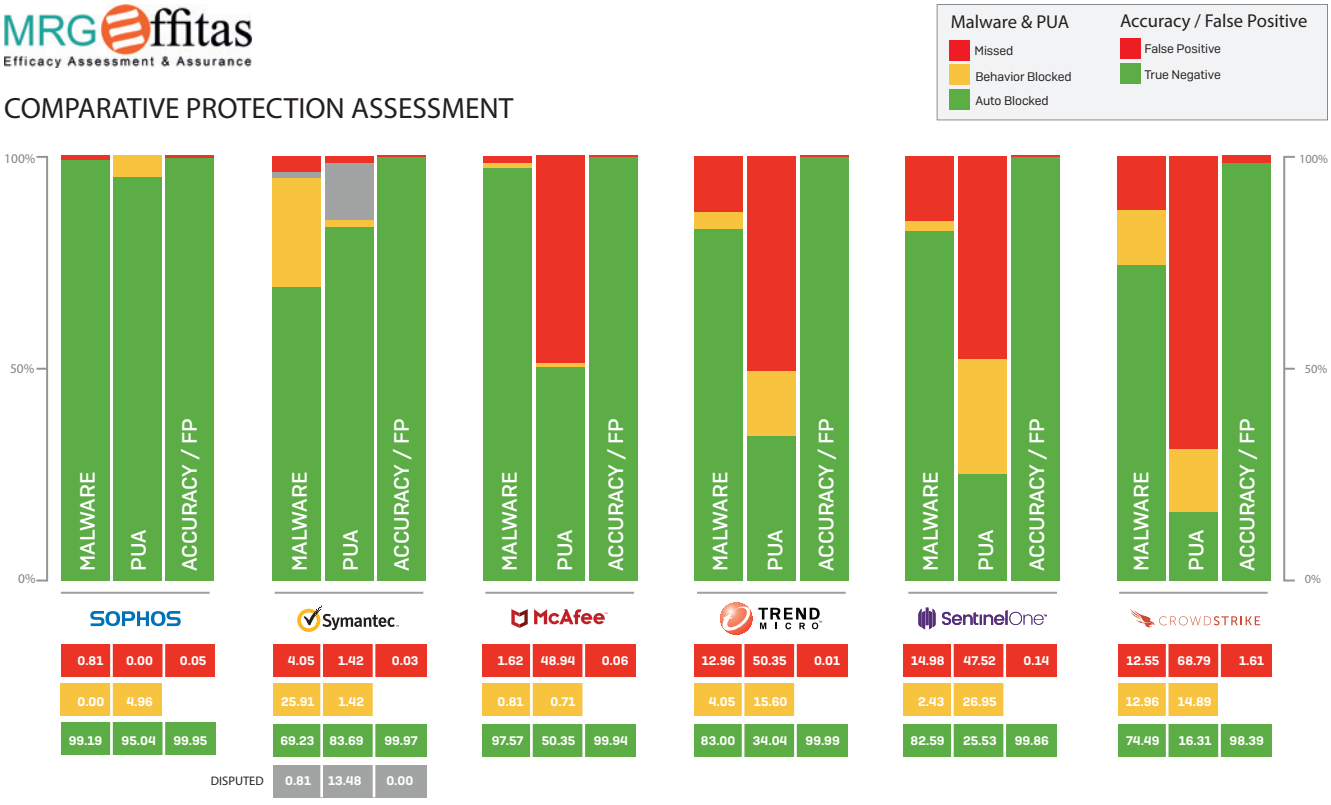
Avast Business Antivirus, Avira Antivirus Pro, Symantec Endpoint Protection und Trend Micro Security fielen bei dem Test durch. Lesen Sie hier den vollständigen Bericht.

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.

MRG Effitas
Efficacy Assessment & Assurance

COMPARATIVE PROTECTION ASSESSMENT



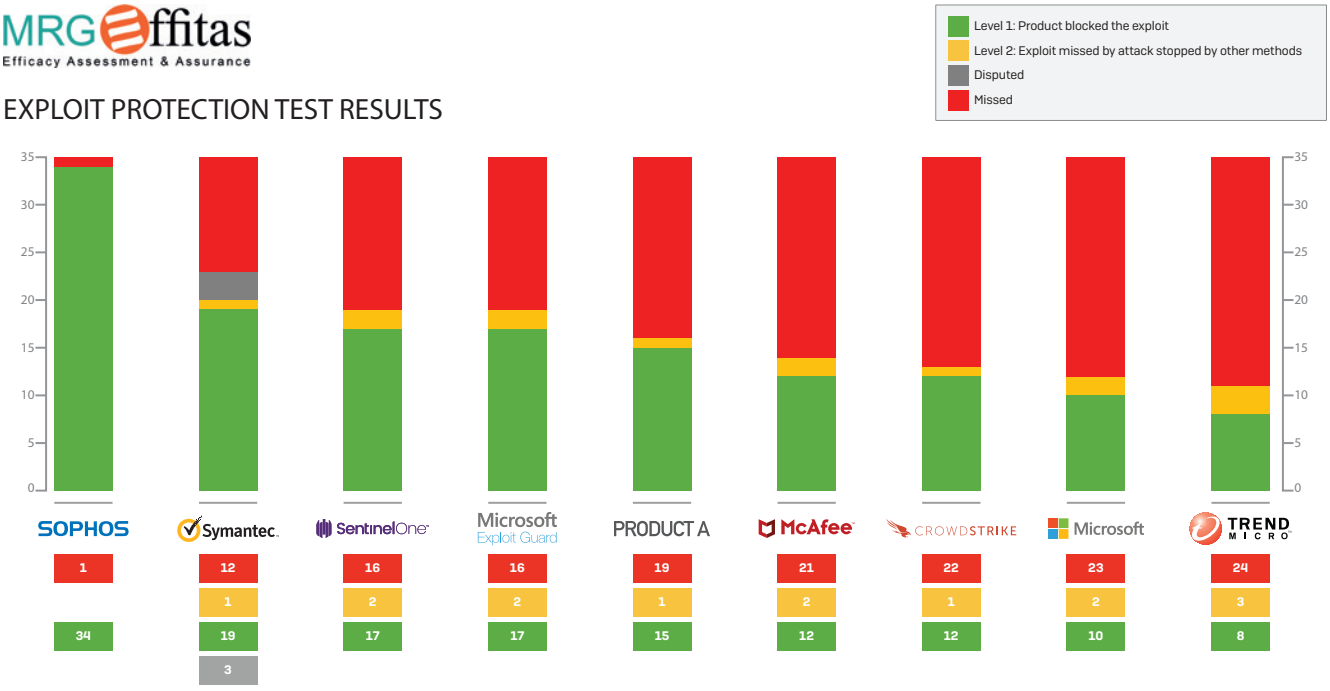
Die vollständigen Testergebnisse finden Sie hier.

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.

MRG Effitas
Efficacy Assessment & Assurance

EXPLOIT PROTECTION TEST RESULTS



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 Small Business Protection, Januar bis März 2020

Gartner Magic Quadrant für Endpoint Protection Platforms

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 zwölften Mal in Folge als Leader im Gartner Magic Quadrant für Endpoint Protection Platforms positioniert. Gartner lobte unseren starken Endpoint-Schutz und stellte dabei insbesondere das Vertrauen unserer Kunden in bewährte Anti-Ransomware-Abwehrmechanismen wie Rollback-Funktionen, weitreichende Features für Endpoint Detection and Response (EDR) Threat Hunting und IT Operations sowie die zentrale Verwaltung aller Sophos-Lösungen über Sophos Central heraus.

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 (englisch).

Rezension von SC Magazine:

Das SC Magazine gab Intercept X die volle Punktzahl und beschrieb die Lösung als:

„... eine lobenswerte, einfach installierbare Endpoint-Security-Lösung, die durch die Bereitstellung von angereicherten Kontext-Informationen Expertise hinzufügt, ohne die Anzahl der Mitarbeiter im Sicherheitsteam zu erhöhen."

Lesen Sie die Rezension 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

Das PC Magazine kam zu dem Schluss, dass Intercept X „eine ausgezeichnete Malware-Schutzlösung für Unternehmen jeder Größe“ ist. Außerdem lobte das PC Magazine die „hervorragende Erkennungs- und Anti-Exploit-Funktionalität“, „vollständig integrierte Endpoint Detection and Response (EDR)“ und „gute Richtlinienkontrolle“ der Lösung.

Quelle: https://uk.pcmag.com/software/121154/sophos-intercept-x-endpoint-protection

AV-Test (Mac)

Sophos erhielt 6.0/6.0 Punkten bei der Schutzwirkung, 6.0/6.0 Punkten bei der Geschwindigkeit und 6.0/6.0 Punkten bei der Benutzbarkeit.

Quelle: https://www.av-test.org/de/antivirus/unternehmen-macos/macos-catalina/juni-2020/sophos-endpoint-9.9-202105/

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

- AV-Test (macOS): Bestnoten
- AV-Test (Android): Bestnoten

Gartner

- Leader: Magic Quadrant für Endpoint Protection Platforms (2020)

Forrester

- Leader: Wave 2019, Endpoint Security

IDC

- Leader: 2019-2020 Enterprise Mobility Management Marketscape
- Leader: 2020 Worldwide Mobile Threat Management Marketscape

Für optimalen Schutz: Umfassende Sicherheitspakete

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.

Mehr Sicherheit: Endpoint Detection and Response (EDR)

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 in IT Operations, um sicherzustellen, dass Sicherheitsvorgaben durchgesetzt werden. Wenn ein Problem gefunden wird, haben Sie per Remote-Zugriff die Möglichkeit, gezielte Maßnahmen zu ergreifen.

Beantworten Sie wichtige Fragen und profitieren Sie von zahlreichen Funktionen in den Bereichen Threat Hunting und IT Security Operations:

- Versuchen Prozesse, eine Netzwerkverbindung über Nicht-Standardports herzustellen?
- Welche Geräte verfügen über bekannte Schwachstellen, unbekannte Dienste oder nicht autorisierte Browser-Erweiterungen?
- Erkennen und bestimmen Sie Ausmaß und Folgen von Sicherheitsvorfällen
- Entdecken Sie Angriffe, die eventuell noch nicht bemerkt wurden
- Suchen Sie im gesamten Netzwerk nach Kompromittierungs-Indikatoren
- Priorisieren Sie Ereignisse für eine weitere Analyse
- Analysieren Sie Dateien, um zu bestimmen, ob es sich bei ihnen um Bedrohungen oder potenziell unerwünschte Anwendungen handelt
- Liefern Sie ohne Probleme jederzeit einen Bericht über den Sicherheitsstatus Ihres Unternehmens

Neuartige Transparenz: Extended Detection and Response (XDR)

Gehen Sie über Endpoints und Server hinaus und erfassen Sie auch Firewall-, E-Mail- und weitere Datenquellen. Mit Sophos XDR erhalten Sie einen ganzheitlichen Überblick über die Cybersicherheit Ihres Unternehmens und haben die Möglichkeit, bei Bedarf jederzeit Detailinformationen abzurufen.

Beantworten Sie wichtige Fragen und profitieren Sie von mehr Transparenz:

- Warum ist die Netzwerkverbindung des Büros langsam?
- Befinden sich in meiner Umgebung nicht verwaltete oder ungeschützte Geräte?
- Erweitern Sie die Analyse auf 30 Tage, ohne dass das betroffene Gerät wieder online gehen muss
- Nutzen Sie die ATP- und IPS-Erkennungen der Sophos Firewall zur Analyse verdächtiger Hosts und Geräte
- Vergleichen Sie E-Mail-Header-Informationen mit anderen Indicators of Compromise
- Prüfen Sie für die letzten 30 Tage auf verloren gegangenen oder zerstörten Geräten Verlaufsdaten auf ungewöhnliche Aktivitäten

Sophos Intercept X bietet viele Vorteile:

- EDR in Kombination mit dem stärksten Endpoint-Schutz
- XDR, die Firewall-, E-Mail- und weitere Datenquellen berücksichtigt, um Ihnen einen vollständigen Überblick über Ihre Umgebung zu geben
- 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

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

FEATURES	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X ADVANCED WITH MTR STANDARD	INTERCEPT X ADVANCED WITH MTR ADVANCED
Basis-Schutz (u. a. Application Control und Verhaltenserkennung)	✓	✓	✓	✓	✓
Next-Gen-Schutz (u. a. Deep Learning, Anti-Ransomware und Schutz vor dateilosen Angriffen)	✓	✓	✓	✓	✓
EDR (Endpoint Detection and Response)		✓	✓	✓	✓
XDR (Extended Detection and Response)			✓	Siehe Fußnote	Siehe Fußnote
MTR (Managed Threat Response – 24/7/365 Threat Hunting and Response Service)				✓	✓
MTR Advanced (Indizienloses Threat Hunting, dedizierter Ansprechpartner und weitere Leistungen)					✓

Bitte beachten: Das MTR-Team kann bei Kunden von MTR Advanced auf XDR-Daten und -Funktionen zurückgreifen. MTR-Kunden sind in ihrer Sophos-Central-Konsole jedoch auf EDR-Funktionen beschränkt und müssen für XDR-Funktionen eine XDR-Lizenz erwerben.

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 ein effektiver Endpoint-Schutz heute unverzichtbar. Wichtig ist: Sie müssen wissen, welche Arten von Bedrohungen existieren, und Sie müssen wissen, welche verschiedenen Schutz-Technologien es gibt, um diese Bedrohungen abzuwehren. Mit diesem Wissen können Sie eine fundierte Entscheidung treffen und den besten Schutz für Ihr Unternehmen finden.

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

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, Q3 2019, von Chris Sherman mit Stephanie Balaouras, Merritt Maxim, Matthew Flug und Peggy Dostie, 23. September 2019

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter
www.sophos.de/intercept-x

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

© Copyright 2021. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

SOPHOS

2021-03-21 DE (MP)