SOPHOS
Security made simple.

Endpoint Buyers Guide

Mit diesem Buyers Guide möchten wir Ihnen helfen, die passende Endpoint-Lösung zu finden. Dazu haben wir unabhängige Recherche- und Testergebnisse zusammengestellt, in denen die größten Anbieter verglichen werden: Sophos, Kaspersky Lab, McAfee, Symantec und Trend Micro.

Reine Antiviruslösungen sind heutzutage nicht mehr ausreichend, um Bedrohungen effektiv abzuwehren. Wenn Sie Ihre Unternehmensdaten erfolgreich schützen wollen, brauchen Sie eine umfassende Endpoint-Sicherheitslösung. Diese sollte in der Lage sein, Malware und moderne Bedrohungen zu erkennen, abzuwehren und zu beseitigen. Außerdem sollte sie über Funktionen wie Web-Filterung und Device Control verfügen, mit denen Sie im gesamten Unternehmen einheitliche Sicherheitsrichtlinien durchsetzen können. Darüber hinaus sollte die Lösung einfach zu installieren und zu verwalten sowie skalierbar sein, damit sie den Zeitaufwand für die IT-Abteilung minimiert und Ihnen langfristig umfassenden Schutz bietet.

In diesem Buyers Guide vergleichen wir die Anbieter, die gemessen an ihrem Marktanteil und auf Grundlage von Branchenanalysen als führend eingestuft werden: Sophos, Kaspersky Lab, Intel Security (McAfee), Symantec und Trend Micro. Die Vergleichskriterien:

- Produkt-Features und -Funktionen
- Bewertungen von Branchenanalysten
- Testergebnisse von Drittanbietern
- Community Feedback

Außerdem haben wir weitere Informationen für Sie zusammengestellt, die Sie bei der Wahl einer geeigneten Endpoint-Lösung für Ihr Unternehmen unterstützen:

- Sorgen Sie für noch mehr Sicherheit: Sicherheitspakete für umfassenden Schutz
- Endpointschutz bewerten: Fragen, die Sie stellen sollten

Produkt-Features und -Funktionen

Einfache Endpoint-Security-Lösungen verfügen über Antivirus-, Anti-Malware- und Anti-Spyware-Funktionen. Solche einfachen Sicherheitsmaßnahmen reichen nach Einschätzung von Branchenanalysten nicht aus, um moderne Bedrohungen von heute effektiv abzuwehren und Datenverlusten vorzubeugen. Features wie Malicious Traffic Detection, Device Control, Application Control, Web Productivity Filtering und Data Loss Prevention können helfen. Selbst wenn Sie momentan noch nicht alle Funktionen dieser umfassenden Lösungen benötigen, so sind diese Funktionen vermutlich in absehbarer Zeit in Ihrem Unternehmen unverzichtbar, da Sicherheitsbedrohungen zunehmend komplexer werden.

Außerdem sollten Unternehmen unbedingt die verfügbaren Verwaltungsfunktionen prüfen, um beurteilen zu können, ob die Bereitstellung, Konfiguration und Wartung des Produkts komfortabel und einfach sind.

Die folgende Tabelle zeigt, welche Funktionen in den zentral verwalteten Endpointschutz-Produkten der einzelnen Anbieter enthalten sind:

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
Lokale Verwaltung	✔	✔	✔	✔	✔
Cloudbasierte Verwaltung (SaaS)	✔	✔	✗	✔	✔
Richtlinien auf Gerätebasis	✔	✔	✔	✔	✔
Richtlinien auf Benutzerbasis	✔	✔	Begrenzt	✔	✗
Device Control	✔	✔	✔	✔	✔
Data Loss Prevention (DLP)	✔	✔	✗	✔	✔
Application Control	✔	✔	✔	✔	✗
Web-Filterung auf Basis von Kategorien	✔	✔	✔	✔	✔
Malicious Traffic Detection	✔	✔	✗	✗	✔
Active-Directory-Synchronisation	✔	✔	Nur Import	✔	✔
Synchronized Security (Endpoint + Netzwerk)	✔	Add-on	✗	✗	✗

Bewertungen von Branchenanalysten

Branchenanlysten wie Gartner und die Info-Tech Research Group sind unabhängige Unternehmen, die Technologieanbieter im Auftrag von Firmenkunden bewerten. In ihren jährlich veröffentlichten Berichten wie den unten aufgeführten stellen sie objektive Informationen zur Verfügung, die es Unternehmen erleichtern, eine informierte Kaufentscheidung zu treffen.

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
Gartner Magic Quadrant für Endpoint Protection Platforms	Leader	Leader	Leader	Leader	Leader
Info-Tech Endpoint Protection Vendor Landscape	Champion & Best Overall Value	Market Pillar	Innovator	Market Pillar	Champion

Gartner Magic Quadrant für Endpoint Protection Platforms

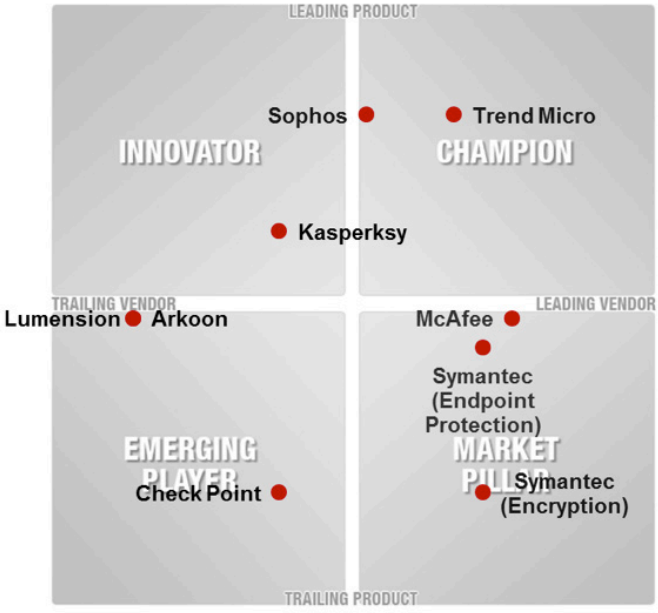
Im Gartner Magic Quadrant für Endpoint Protection Platforms, der die Vollständigkeit der Lösungsangebote sowie die Handlungsfähigkeit verschiedener Anbieter bewertet, wurden 2014 18 Hersteller verglichen. Sophos, Kaspersky Lab, Intel Security (McAfee), Symantec und Trend Micro konnten sich im Leader Quadrant platzieren. Sophos ist zum achten Mal in Folge Leader.

Magic Quadrant für Endpoint Protection Platforms von Peter Firstbrook, John Girard, Neil MacDonald, 22. Dezember 2014

HAFTUNGSAUSSCHLUSS: 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.

Info-Tech Endpoint Protection Vendor Landscape

In diesem Bericht bewertet die Info-Tech Research Group Anbieter nach ihrer Produktpalette und strategischen Ausrichtung. Laut Bericht werden diejenigen Anbieter als Champions ausgezeichnet „die bei den meisten Bewertungskriterien hohe Punktzahlen erzielen und ein exzellentes Preis-Leistungs-Verhältnis bieten. Sie haben eine starke Marktpräsenz und sind Trendsetter der Branche." Im Bericht für das Jahr 2014 ist Sophos einer von nur zwei Champions. Info-Tech verlieh Sophos außerdem das Prädikat „Best Overall Value".



Testergebnisse von Drittanbietern

Unabhängige Tests wie die nachstehend aufgeführten vergleichen Erkennungs- und False-Positive-Raten sowie die Performance (Auswirkung auf die Leistung eines Computers) in einer kontrollierten Laborumgebung. Laborbedingungen spiegeln jedoch nicht immer wider, wie gut der Schutz und die Performance unter Realbedingungen tatsächlich sind. Sie sollten daher auch berücksichtigen, welche Funktionen zur Erkennung, Abwehr und Beseitigung die einzelnen Lösungen vorweisen können.

		Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
AV-Test Business Windows Client Mai–Juli 2015	**Bewertung des Schutzes**	6.0/6.0	6.0/6.0	6.0/6.0	6.0/6.0	6.0/6.0
Dennis Technology Labs Small Business Anti-Virus Protection Januar–März 2015	**Auszeichnung**	AAA	A	AAA	AAA	B
	Genauigkeit insgesamt	94 %	84%	100%	100 %	73 %
AV-Comparatives Performance Test Mai 2015	**Auszeichnung**	Advanced+ ★★★	Advanced+ ★★★	Advanced+ ★★★	Nicht getestet	Advanced ★★

Community Feedback

Um sich eine objektive Meinung über einen Anbieter zu verschaffen, ist es manchmal am besten, bestehende Kunden nach ihrer Meinung zu fragen. Genau das tut Spiceworks. Das über sechs Millionen Mitglieder zählende Netzwerk für IT-Experten holt Online-Bewertungen von seiner Community ein und dient damit als verlässliche Quelle für eine objektive Anbieterbewertung.
So schneiden die führenden Endpoint-Security-Anbieter auf Spiceworks ab:

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
Durchschnittliche Bewertung (von insgesamt 5 Sternen)	★★★★½	★★	★★★★	★★½	★★★½

Darüber hinaus baten das Information Security™ Magazine und SearchSecurity.com über 1.700 Führungskräfte und Vorgesetzte im Informationssicherheitssektor, ihre bevorzugten Produkte in insgesamt 22 Kategorien zu benennen. Sophos war 2014 einer der zwei Gewinner des vom Magazin vergebenen Readers' Choice Award in der Kategorie „Endpoint Security".

Sorgen Sie für noch mehr Sicherheit: Sicherheitspakete für umfassenden Schutz

Eine Endpoint-Security-Lösung schützt Ihre Computer vor Malware und sorgt für die Durchsetzung Ihrer Sicherheitsrichtlinien. Dies ist jedoch nur ein Teil einer unternehmensweiten Sicherheitsstrategie. Unternehmen sollten sich heute nicht mehr ausschließlich auf Endpointschutz konzentrieren, sondern die gesamte Endbenutzer-Umgebung berücksichtigen. Idealerweise sollten sie von nur einem Anbieter ein ganzes Paket an Lösungen beziehen, 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 Endpointschutz auch die folgenden Technologien in Erwägung zu ziehen:

- Festplattenverschlüsselung
- Mobile Device Management (MDM)
- Mobile Security (Antivirus)
- Secure Email Gateway (Anti-Spam, Anti-Malware, Verschlüsselung)
- Secure Web Gateway (Inhaltsfilterung, Anti-Malware, Reporting)
- Spezieller Schutz für Server oder virtuelle Maschinen
- Synchronized Security – Zusammenarbeit zwischen Endpoint und Netzwerk ermöglicht schnellere Entscheidungen

Endpointschutz bewerten: Fragen, die Sie stellen sollten

Endpoint-Sicherheitslösungen werben mit diversen Funktionen. Um ein bestimmtes Produkt zu beurteilen, sollten Sie dem Anbieter zunächst die folgenden Fragen stellen:

1. Welcher Aufwand ist notwendig, um die Lösung bereitzustellen und unter Berücksichtigung geltender „Best Practices“ für optimalen Schutz zu konfigurieren?
2. Welche Schritte sind erforderlich, um Ausnahmen für Richtlinien einzurichten (z. B. Zugriff auf einen bestimmten USB-Stick zulassen oder den Besuch einer bestimmter Website erlauben)?
3. Welche Auswirkung (Performance und Benutzerfreundlichkeit) hat das Produkt auf die Endbenutzer?
4. Wie viel Support (Level und Stunden) ist standardmäßig im Produkt enthalten?
5. Wie wurde das Produkt in der jüngsten Vergangenheit weiterentwickelt, um vor neuen, modernen Bedrohungen zu schützen?
6. Sind Web-Schutz und -Filterung des Produkts auch dann aktiv, wenn Benutzer außerhalb des Netzwerks im Internet surfen?
7. Haben Sie auch Bundles/Suites im Angebot, mit denen sich das Endpoint-Produkt erweitern lässt, um umfassenden Schutz für Benutzer und Daten zu erhalten?
8. Welche Möglichkeiten zur Funktionserweiterung meines Endpointschutzes durch die Integration von Endpoint- und Netzwerk-Sicherheit bieten Sie?

Advantix.
Groupware AG
Bahnhofstrasse 33b
CH - 8703 Erlenbach
Tel +41 44 914 88 44
Fax +41 44 914 88 45
welcome@advantix.ch

SOPHOS