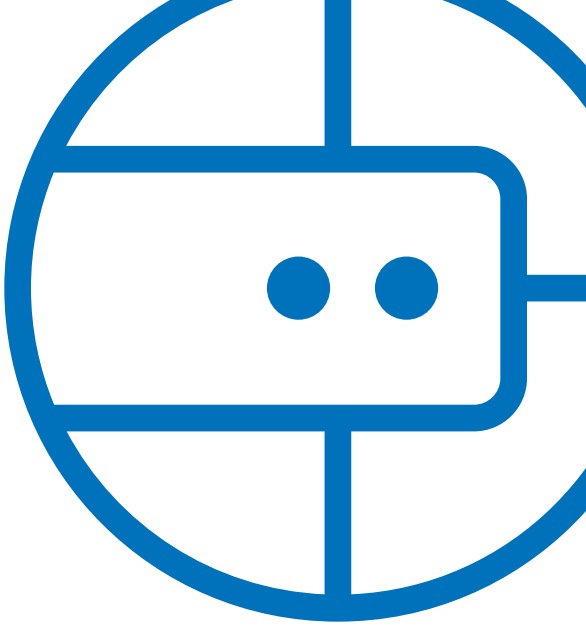
SOPHOS



Server Protection Buyers Guide

Auf Server abzielende Cyberbedrohungen entwickeln sich nach wie vor mit alarmierender Geschwindigkeit. Und sie werden immer raffinierter. Verheerende Ransomware-Ausbrüche, wie etwa WannaCry und NotPetya, haben aufgezeigt, wie wichtig robuste Anti-Ransomware-Funktionen sind. Zudem demonstrierten systemische Sicherheitslücken, die von Spectre oder Meltdown ausgenutzt wurden, dass Anti-Exploit-Technologie, Application Control und Analyse-Tools wie EDR zentrale Komponenten einer Server-Security-Strategie darstellen.

Und da Server nicht selten die wichtigsten Endpoints des Unternehmens sind, sehen sich IT-Manager mit der Herausforderung konfrontiert, adäquaten, effizienten Schutz auszuwählen. Es reicht nicht aus, für Desktops konzipierte Sicherheitslösungen auf Servern laufen zu lassen: Unternehmen benötigen dedizierte Lösungen, die speziell auf den Schutz von Server-Workloads ausgerichtet sind.

In unserem Guide bieten wir Ihnen praktische Tipps zu wichtigen Funktionen, die es bei der Auswahl von Server-Security zu beachten gilt. Darüber hinaus gehen wir auf Fragen ein, die Sie an Anbieter richten sollten, um die gewünschte Funktionsweise der jeweiligen Funktionen sicherzustellen.

Server-Umgebungen

Je nach den Gegebenheiten in Ihrem Unternehmen verfügen Sie vielleicht über Ihre eigenen lokalen Server, hosten Ihre Daten in der Public Cloud, z.B. über Amazon Web Services (AWS), Microsoft Azure oder Google Cloud, oder nutzen eine Kombination aus beidem. In jedem Fall benötigen Sie als absolutes Minimum eine Sicherheitslösung, mit der sich die unterschiedlichen Bereitstellungen einfach und zentral verwalten lassen.

Idealerweise bietet die Lösung weitere Vorteile, wie etwa die Bereitstellung von einheitlichen, zentral verwalteten Richtlinien für alle Server. Die automatisierte Bereitstellung von Server-Schutz (etwa mit Hilfe von Skripts) in der Cloud ist von zentraler Bedeutung, um die Server ohne Admin-Zugriff nach Bedarf hoch- und herunterfahren zu können.

Da Unternehmen sich häufig für gemischte Umgebungen entscheiden, sind unkomplizierte Lizenzmodelle wichtiger denn je. Achten Sie darauf, dass der Anbieter Ihrer Wahl sämtliche Bereitstellungsszenarien (Cloud, lokal oder eine Kombination der beiden) in einem einzigen Lizenztyp abdeckt. So ersparen Sie sich eine aufwändige Lizenzzusammenstellung.

Zentrale Produktfunktionen

Server Security hat sich angesichts zunehmend komplexerer Bedrohungen enorm weiterentwickelt. Zum Schutz Ihrer Server – lokal und in der Cloud – sollten Sie nach Funktionen Ausschau halten, die Schutz bieten vor unbekannten Bedrohungen, Ransomware, Exploits sowie Hackerangriffen.

- **Anti-Ransomware** – Manche Lösungen beinhalten Funktionen, um die unbefugte Verschlüsselung von Daten durch Ransomware zu verhindern. Häufig werden betroffene Dateien durch solche Anti-Ransomware-Technologien zudem in ihren Ursprungszustand zurückversetzt. Allerdings sollten sich Anti-Ransomware-Lösungen nicht auf Dateien abzielende Ransomware beschränken, sondern auch Festplatten-Ransomware abwehren, die den Master Boot Record durch zerstörerische Löschangriffe schädigt. Speziell bei Servern muss darüber hinaus verhindert werden, dass Remote- oder unbefugte Endpoints Dateien in Netzlaufwerken oder auf anderen verbundenen Servern verschlüsseln.
- **Server Lockdown/Whitelisting/standardmäßige Sperrung** – Durch das Whitelisting erlaubter Anwendungen wird verhindert, dass nicht zulässige Programme auf Ihren Servern laufen. Achten Sie beim Kauf darauf, dass die Anwendung Ihrer Wahl vertrauenswürdige Anwendungen automatisch erkennt und dabei Anpassungen durch die User zulässt, um die zeit- und arbeitsaufwändige Erstellung sicherer Regeln zu minimieren. Wichtig ist zudem, dass es beim Sperren und Entsperren von Servern nicht zu Ausfallzeiten kommt.
- **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 relativ geringe Anzahl an Techniken, die zur Verbreitung von Malware und Durchführung von Angriffen genutzt werden. Dadurch lassen sich zahlreiche bisher unbekannte Zero-Day-Angriffe abwehren, ohne dass eine Signatur benötigt wird. Umfassende Exploit Prevention schützt auch Server, die nicht schnell gepatcht werden können oder für die keine Patches verfügbar sind.

[1] Gartners Top 10 Sicherheitsprojekte für 2018

- **Endpoint Detection and Response (EDR)** – Dank EDR können IT-Manager evasive Bedrohungen unschädlich machen sowie Ausmaß und Folgen von Sicherheitsvorfällen verstehen. Idealerweise sollte die Lösung Ihrer Wahl eine EDR-Funktionalität beinhalten, die Ihnen hilft, sich auf das Wesentliche zu konzentrieren: Die Flut an Informationen wird verringert, verdächtige Dateien werden analysiert. So können Sie eine fundierte Entscheidung treffen.
- **Anti-Hacker-Schutz** – Hacker haben es besonders auf Server abgesehen, da sich darauf in der Regel die sensibelsten Unternehmensdaten befinden. Ihre Lösung sollte spezielle Funktionen zur Abwehr persistenter Hacker-Angriffe in Echtzeit umfassen. Zu erforderlichen Anti-Hacker-Funktionen zählen unter anderem Credential Harvesting Prevention, Verhinderung lateraler Bewegungen, Schutz vor Code Caving, vor Rechteausweitung sowie vor Prozessmigration.
- **Machine Learning** – Es gibt unterschiedliche Arten von Machine Learning, z.B. 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.
- **Reaktion auf Vorfälle/Synchronized Security** – Server-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. Achten Sie darauf, dass Server-Sicherheits-Tools mit anderen Netzwerk-Sicherheits-Tools wie der Firewall kommunizieren. So erkennen Sie kompromittierte Server und erhalten Transparenz über alle Anwendungen, die auf dem Server ausgeführt werden.
- **File Integrity Monitoring** – Sie sollten in der Lage sein, kritische Systemdateien und Daten vor unautorisierten Änderungen zu schützen und optional die wichtigsten Speicherorte Ihrer Anwendungen zu überwachen. Sophos Central Server Protection hält kontinuierlich Ausschau nach ungeplanten und unerwarteten Änderungen und identifiziert potenzielle PCI DSS-Sicherheitslücken.
- **Application Control** – Mit dieser Funktion lässt sich steuern, welche Anwendungen auf dem Server ausgeführt werden dürfen, um die Angriffsfläche zu reduzieren. Idealerweise sollten sich Anwendungen nach Kategorien filtern lassen, um eine einfache, schnelle Konfiguration zu ermöglichen.
- **Zentrales Management** – Die Konsole sollte durch einfaches Management überzeugen und Transparenz über gemischte Serverumgebungen bieten – beispielsweise Alerts, Ereignisse und Reports, die in einer leicht zugänglichen, benutzerfreundlichen Plattform zusammenlaufen.
- **Workload-Erkennung und -Schutz** – Der Schutz in der Cloud hängt vom Schutz jeder Instanz oder virtuellen Maschine (VM) und jedes Buckets ab. Die Erkennung von Workloads und Buckets in Public Cloud-Umgebungen wie Amazon Web Services (AWS) und Microsoft Azure ist von entscheidender Bedeutung, da Angreifer bekanntermaßen ungenutzte Cloud-Bereiche für andere Zwecke verwenden, z.B. Cryptomining. Produkte mit nativer API-Integration in Public-Cloud-Plattformen melden neue Workload-Instanzen und Buckets sowie möglicherweise aktuell ungenutzte Regionen.

Management und Reporting

In der Regel loggen Sie sich nur dann am Server ein, wenn ein Problem auftritt. Aus diesem Grund muss das Server-Management vor allem die beiden folgenden Anforderungen erfüllen:

1. Unkomplizierte Bereitstellung und Überwachung von allen Servern
2. Bedienerfreundliche Benutzeroberfläche, die eine schnelle Reaktion auf Probleme ermöglicht

Oft führt die Bereitstellung von Einzellösungen unterschiedlicher Anbieter für verschiedene Server in unterschiedlichen Umgebungen zu Verwaltungs-Problemen, da mehrere Konsolen genutzt werden müssen. Bei größeren Serveranlagen kann dies schnell zur Belastung werden. Allerdings ist bei schwerwiegenden Vorfällen schnelles, entschlossenes Handeln gefordert. Die mühsame Suche nach wichtigen Informationen zur Entscheidungsfindung kann wichtige Zeit kosten. Suchen Sie nach einer Lösung, bei der alle Informationen in einer zentralen Konsole zusammengeführt werden, damit sich wichtige Informationen schnell und einfach auffinden lassen.

Mitunter können Lösungen auch in den Server mit Ihrer Netzwerk-Sicherheit (Firewall) integriert werden und so Bedrohungsdaten mit anderen Systemen austauschen. So kann ein betroffener Server etwa vom Netzwerk isoliert werden, um weitere Schäden zu verhindern. Zudem bietet die Konsole eine zuverlässige Übersicht über Datenverkehr und Anwendungen, was die Priorisierung wichtiger Anwendung oder Blockierung unerwünschter Apps erleichtert.

Setup-Skripts sorgen, insbesondere bei Cloud-Implementierungen, für eine einfache Bereitstellung und schaffen wertvolle Zeit für Serveradmins, sich um andere Dinge zu kümmern. Application Whitelisting, das Anwendungen standardmäßig sperrt, oder kategoriebasierte Application Control beschleunigen die Konfiguration erlaubter und unzulässiger Programme auf dem Server.

Checkliste zum Produktvergleich

Nachdem Sie im vorangegangen Abschnitt Ihre Basisanforderungen ermittelt haben, können Sie Lösungen unterschiedlicher Anbieter in unserer Tabelle vergleichen und auf ihre Eignung für Ihr Unternehmen prüfen.

Funktionsvergleich			Intercept X Advanced for Server with EDR	Trend Micro Deep Security	Symantec Schutz von Workloads in der Cloud	Microsoft Enterprise Mobility und Security	CrowdStrike Falcon Prevent / Falcon Spotlight
VERWALTUNG		Eine zentrale Konsole zum Schutz von Servern, Endpoints, Mobilgeräten, E-Mails und WLAN	✓	×	×	×	×
		AWS-/Azure-Workload-Erkennung	✓	✓	✓	✓	✓
		Automatische Scan-Ausnahmen (z. B. Exchange, SQL Server)	✓	×	✓	✓	×
		Virtualisierung: Thin Agent mit zentralem Scanner	✓	✓	×	×	×
ABWEHR	REDUZIEREN DER ANGRIFFSFLÄCHE	Web-Filterung (Blockieren schädlicher Webseiten)	✓	✓	✓	✓	×
		Web Control (Einschränken des Zugriffs auf potenziell unangebrachte Webseiten)	✓	×	×	×	×
		Application Whitelisting (Server Lockdown)	✓	✓	×	✓	×
		Kategoriebasierte Application Control	✓	×	×	×	×
		Peripheral/Device Control	✓	×	×	×	×
		Patch-Analyse	×	✓	✓	✓	✓
	VOR DER AUSFÜHRUNG	Malware-Schutz mit Machine Learning	✓	✓	✓	✓	✓
		Exploit-Abwehr	✓	✓	✓	✓	✓
		Data Loss Prevention	✓	×	×	✓	×
ERKENNUNG		Anti-Hacker-Funktionen (z. B. Abwehr von Identitätsdiebstahl und Code Caving)	✓	×	×	✓	×
		Schutz vor Ransomware (Verhaltenserkennung und -Rollback)	✓	✓	×	Erkennung ohne Rollback	Erkennung ohne Rollback
		Disk & Boot Record Protection	✓	×	×	×	×
		File Integrity Monitoring (FIM)/Änderungsüberwachung	✓	✓	✓	✓	×
REAKTION		Synchronized Security (Sofort-Integration mit der Firewall)	✓	×	×	×	×
		Visualisierung der Bedrohungskette	✓	×	×	Defender ATP erforderlich	✓
		Bedrohungssuche	✓	×	×	Defender ATP erforderlich	✓

Zentralisierte Sicherheit

Der Schutz aller Server spielt eine zentrale Rolle in der Sicherheitsstrategie von Unternehmen. Wenn es jedoch auch andere Endpoint-Geräte, Mobiltelefone, Netzwerk-Sicherheit, Verschlüsselung und mehr zu berücksichtigen gilt, gestaltet sich die Verwaltung oft äußerst aufwändig. Hinzu kommt, dass bei vielen Anbietern eine zusätzliche Sicherheitsebene mit einer zusätzlichen Konsole mit einer anderen Benutzeroberfläche und einem gesonderten Richtlinienrahmen einhergeht. Häufig lassen sich die einzelnen Sicherheitskomponenten nicht über die verschiedenen Geräte und Infrastrukturen hinweg integrieren.

Mit Sophos Central verwalten Sie sämtliche Sophos Security-Lösungen über eine einzige Konsole. Über eine intuitive, einheitlich gestaltete Schnittstelle wechseln Sie ganz einfach von einem Produkt zum anderen. Ein weiteres Plus: Unsere Lösungen arbeiten perfekt zusammen und bieten Ihnen so besseren Schutz. So arbeiten Ihre Server etwa automatisch mit Ihren Firewalls zusammen, um kompromittierte Server automatisch zu ermitteln, zu isolieren und zu bereinigen.

Bewertung von Server Security: 10 Fragen, die Sie auf jeden Fall stellen sollten

Bei der Auswahl der richtigen Server-Schutz-Lösung sollten Sie dem Anbieter zunächst folgende Fragen stellen:

1. Unterstützt das Produkt unterschiedliche Server-Bereitstellungen, wie lokal, Cloud und gemischte Umgebungen?
2. Umfasst das Produkt automatisiertes Application Whitelisting/standardmäßiges Sperren ohne zusätzliche Kosten?
3. Beinhaltet die Lösung Technologie zur Abwehr von Ransomware mit anschließender automatischer Wiederherstellung betroffener Dateien?
4. Sind Funktionen zum Schutz vor Exploits sowie Angriffen ohne Dateien vorhanden? Welche Anti-Exploit-Technologien werden eingesetzt und welche Angriffsmethoden erkennen sie?
5. Wie schützt das Produkt vor persistenten Angriffen durch aktive Gegner?
6. Mit welchen Techniken erkennt das Produkt unbekannte Malware? Nutzt das Produkt Machine Learning zur kontinuierlichen Suche nach schädlichen Attributen und Verhaltensweisen?
7. Bei Lösungen, die angeben, Machine Learning zu nutzen: Werden die Erkennungsraten durch unabhängige Tests belegt? Wie steht es mit False-Positive-Raten?
8. Welche Informationen liefert der Anbieter über Bedrohungen, z. B. Ursachenanalyse?
9. Reagiert das Produkt automatisch auf Bedrohungen? Kann es Bedrohungen automatisch als Reaktion auf einen Vorfall bereinigen?
10. Lässt sich das Produkt nativ in die Public Cloud (beispielsweise AWS/Azure/Google) integrieren und verfügt es über die Fähigkeit zur automatischen Erkennung von Workloads in der Cloud?

Fazit

Cyberbedrohungen entwickeln sich nach wie vor mit alarmierender Geschwindigkeit und werden immer raffinierter. Aus diesem Grund ist effektiver Serverschutz unerlässlich. Wenn Sie verstehen, welche Bedrohungen es gibt und welche Technologien zu ihrer Abwehr erforderlich sind, können Sie den bestmöglichen Serverschutz für Ihr Unternehmen auswählen. Dabei gilt es zu beachten, dass der Schutz speziell auf Serverworkloads ausgerichtet ist. An Server angepasste Endpoint Protection reicht nicht aus.

Sophos Intercept X for Server
jetzt kostenlos testen

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

09.05.2019 DSDE (PS)

SOPHOS