SOPHOS

Cybersecurity System Buyers Guide

83% aller IT-Manager bestätigen, dass Cyberbedrohungen seit dem letzten Jahr immer schwerer abzuwehren sind. Immer mehr Unternehmen steigen daher auf ein Cybersecurity-System um und verlassen sich nicht mehr auf individuelle Einzellösungen.

Die Entscheidung für ein Cybersecurity-System fällt oft nicht leicht. Viele Anbieter werben zunehmend mit produktübergreifender Integration. Da stellt sich die Frage, worauf genau es zu achten gilt und wie Sie die richtige Wahl treffen.

Unser Guide erklärt, auf welche wichtigen Punkte Sie bei der Wahl Ihres Cybersecurity-Systems achten sollten. Anschließend zeigen wir, wie unser Synchronized-Security-System im Vergleich zu anderen Anbietern wie Fortinet, SonicWall, Cisco, Palo Alto Networks und Microsoft abschneidet.

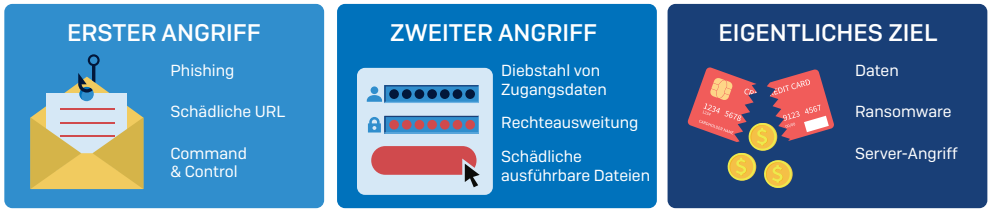
Individuelle Einzellösungen reichen nicht mehr aus

Trotz kontinuierlicher technischer Innovation und einem hohen Investitionsvolumen ist effektive Cybersecurity nach wie vor eine große Herausforderung für Unternehmen. So bestätigen 87 % aller IT-Manager, dass Malware-Bedrohungen seit dem letzten Jahr deutlich komplexer geworden sind, und Unternehmen wenden im Durchschnitt sieben Arbeitstage pro Monat für das Identifizieren und die Bereinigung infizierter Computer auf.

Cyberbedrohungen arbeiten als System

Um die Ursache von Sicherheitsproblemen ermitteln zu können, müssen wir zunächst die Bedrohungen genauer unter die Lupe nehmen, die wir stoppen möchten. Cyberkriminelle nutzen bei ihren Angriffen keine einzelnen Techniken oder Technologien, sondern kombinieren mehrere verschiedene Techniken für konzertierte, koordinierte Angriffe.

So kann ein Angriff beispielsweise mit einer Phishing-E-Mail beginnen, die einen schädlichen Link enthält. Klickt ein Mitarbeiter auf den Link, wird er mit einem Command and Control Center verbunden. Durch eine Kombination aus Zugangsdatendiebstahl, Rechteausweitung und schädlichen ausführbaren Dateien stehlen Hacker Ihre Daten oder verschlüsseln sie und verlangen Lösegeld für die Herausgabe.



Getrennt voneinander arbeitende Einzellösungen können solche komplexen, koordinierten Angriffe nur schwer abwehren. Hier schaffen Cybersecurity-Systeme Abhilfe: Integrierte Produkte arbeiten zusammen, um Hacker zu überlisten.

System
(altgr. sýstēma, ‚aus mehreren Einzelteilen zusammengesetztes Ganzes'

Ihre IT-Infrastruktur arbeitet als System

Ihr IT-System ist von zentraler Bedeutung für effektive, sichere Betriebsabläufe in Ihrem Unternehmen. Der Verbund aus Geräten, Netzwerken, Daten und Workloads ermöglicht ein produktives Arbeiten (Datenaustausch, Zugriff auf Dokumente, Nachverfolgung von Aktivitäten).

Mit der Weiterentwicklung der Technologie haben sich auch unsere IT-Systeme weiterentwickelt: Cloudbasierte Workloads werden mittlerweile parallel zu traditionellen Elementen betrieben. Zwar bringt diese Weiterentwicklung der IT eine Vielzahl an Vorteilen für Unternehmen, doch gleichzeitig entstehen dadurch neue Herausforderungen, beispielsweise bei der Transparenz: Nur 16% aller CISOS können 75% oder mehr ihrer Telemetriedaten zu sicherheitsrelevanten Ereignissen erfassen, analysieren und auf diese reagieren.

Wie wollen Sie Dinge kontrollieren, die Sie nicht sehen können? Dank der Korrelation und Konsolidierung von Daten aus der gesamten IT-Infrastruktur liefern Cybersecurity-Systeme mehr Einblicke in Sicherheitsrisiken und das Benutzerverhalten im gesamten Unternehmen. So kann die IT-Abteilung verborgene Bedrohungen sehen und entsprechend reagieren.

Was zeichnet ein System aus?

Viele Anbieter werben zunehmend mit produktübergreifender Integration und Cybersecurity-Systemen. Je nach Anbieter verbergen sich hinter diesen Begriffen allerdings sehr unterschiedliche Dinge. Deshalb besprechen wir im Folgenden, was genau ein Cybersecurity-System eigentlich auszeichnet.

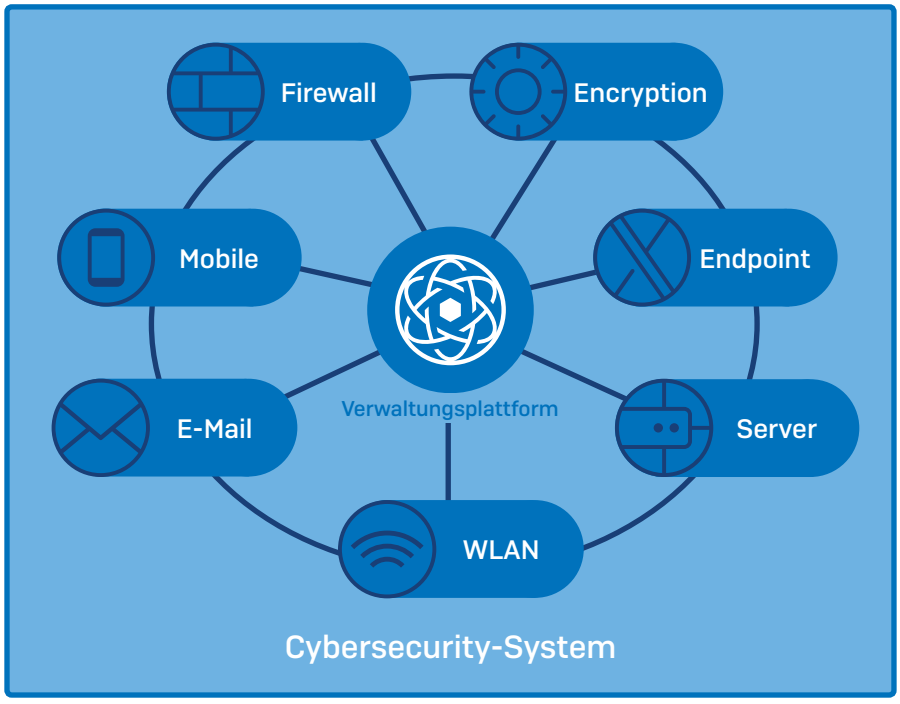
Ein effektives System zeichnet sich immer durch vier Kernelemente aus:

1. **Zentrale Verwaltung:** Möglichkeit, alles von einem Ort aus zu sehen und zu steuern
2. **Integrierte Komponenten:** Unterschiedliche Elemente arbeiten harmonisch zusammen
3. **Automatisierte Aktionen:** Sequenzielles Verhalten basierend auf vordefinierten Kriterien
4. **Skalierbarkeit:** Das System kann mit den Anforderungen wachsen

Diese vier Elemente machen Einzelprodukte zum System. Je leistungsstärker die Einzelkomponenten sind, umso stärker ist das System. Stark integrierte Systeme übertreffen Systeme mit schwacher Integration.

Diese Prinzipien gelten auch für die Cybersecurity. Den Kernpunkt des Systems bildet eine zentrale Cybersecurity-Plattform, über die sich alle Security Services (Endpoint Protection, Firewall, Schutz von Mobilgeräten, E-Mails, WLAN, Verschlüsselung sowie Mitarbeitertraining) steuern lassen. Die einzelnen Services arbeiten aktiv zusammen, tauschen Daten aus und reagieren automatisch auf Probleme und Ereignisse. Je höher der Integrationsgrad des Systems, desto effektiver ist es.

Zentrale Verwaltung, integrierte Komponenten, automatisierte Aktionen und Erweiterbarkeit sind essenziell in einem Cybersecurity-System



Mehrwert für Ihr Unternehmen

Ein Cybersecurity-System sollte sowohl dem gesamten Unternehmen als auch der IT-Abteilung einen Mehrwert bieten. Eine effektive Lösung bietet Ihnen folgende Vorteile:

- **Cyber-Risiken werden eingedämmt.** Ihre Anfälligkeit für Angriffe wird verringert und Sie können bei einer Infektion deutlich schneller reagieren.
- **Mehr Transparenz.** Sie erhalten deutlich mehr Einblick in Ihre Sicherheit und Ihre gesamte IT-Infrastruktur. Dadurch können Sie fundierte, richtige Entscheidungen treffen.
- **Höhere Produktivität.** Sie verringern die Auswirkungen der Cybersicherheit auf die IT-Abteilung und alle Mitarbeiter.
- **Sie sparen Geld.** Durch den Wechsel von Insellösungen zu einem Cybersecurity-System verringern sich Ihre Onboarding-, Integrations- sowie Trainingskosten. Zudem wird der finanzielle Aufwand für die Systemverwaltung reduziert. Auch andere Abteilungen, wie etwa der Einkauf oder die Rechtsabteilung, profitieren von einer Konsolidierung der Anbieter.
- **Sie demonstrieren den Nutzen der IT-Security.** Da IT-Abteilungen weniger Zeit für das Beheben tagtäglicher Probleme aufwenden müssen, können sie sich auf geschäftsrelevante Projekte konzentrieren. Der bessere Schutz führt zu weniger Ausfallzeiten bei den Benutzern, wodurch allen Mitarbeitern im Unternehmen der Mehrwert der IT-Sicherheit bewusst wird.

Worauf es bei einem Cybersecurity-System ankommt

Zur optimalen Nutzung eines Cybersecurity-Systems gilt es, die folgenden vier Hauptaspekte zu beachten.

1. **Produktumfang**
   Sie müssen nicht direkt zu Beginn ein komplettes All-in-One-System einführen. Achten Sie jedoch darauf, dass sich das System bei Bedarf zu einem späteren Zeitpunkt erweitern lässt. Unternehmen starten häufig mit einem kleineren System (beispielsweise zwei Sicherheitskomponenten, die zusammenarbeiten) und erweitern dieses später um weitere Lösungen. Eine zukunftssichere Lösung muss mit Ihrem Unternehmen mitwachsen können.
   - **Bandbreite der Sicherheitsservices.** Wie umfangreich ist das Cybersecurity-System? Welche Produkte sind im Bedarfsfall verfügbar? Erfüllt das System Ihre gesamten Cybersecurity-Anforderungen oder konzentriert es sich nur auf einen Bereich?
   - **Kommunikation zwischen den Komponenten.** Wie tauschen die Produkte Informationen aus? Produkte, die nur in eine Richtung kommunizieren, können als Teil eines Systems nur begrenzt zusätzliche Vorteile bieten. Produkte, die kontinuierlich Informationen im gesamten System austauschen, bieten dagegen wesentlich mehr Vorteile in Bezug auf Sicherheit und Ressourcen.
   - **Einfache Erweiterbarkeit.** Wie leicht lassen sich neue Produkte in das Cybersecurity-System hinzufügen? Und wie einfach lassen sich diese neuen Technologien bereitstellen und nutzen?
   - **Zusatzkosten.** Müssen Sie zusätzlich zu den Einzellösungen weitere Produkte oder Subscriptions erwerben, um die Vorteile eines Cybersecurity-Systems nutzen zu können? Bei der Planung der Kosten sollten Sie sowohl die Kosten der Security-Produkte als auch die Kosten für Training und Onboarding beachten.

2. **Produktintegration**
   Sinn und Zweck eines Security-Systems ist, dass es mehr bietet als die Summe seiner einzelnen Bestandteile. Das bedeutet, die einzelnen Produkte erreichen durch ihre Zusammenarbeit Vorteile, die sie nicht bieten können, wenn sie getrennt voneinander arbeiten. Die Hauptvorteile eines Sicherheitssystems lassen sich in zwei Kategorien einteilen: Automatisierung und Transparenz. Dabei gilt es, vor allem die folgenden Fragen zu beachten:

   - **Zero-Touch, automatisierte Reaktion.** Wie arbeiten die Produkte zusammen, um bisherige manuelle Aufgaben zu automatisieren? In welchem Umfang bietet das System eine automatisierte Reaktion auf Vorfälle? Meldet das System Infektionen z.B. lediglich an den Administrator, der dann selbst tätig werden muss? Oder schützt das System das infizierte Gerät automatisch, bereinigt die Infektion und schaltet es nach Wiederherstellung der Systemintegrität wieder online?
   - **Netzwerkweite Transparenz.** Inwiefern verschafft Ihnen die Produktintegration mehr Transparenz im gesamten Unternehmen? Bietet das System durch Echtzeitanalysen von Vorfällen und Reports für die gesamte Umgebung sofort Informationen, auf Basis derer Sie reagieren können? Erkennt das System unbekannte Bedrohungen?

Cybersecurity-Systeme sollten Zero-Touch-Reaktionen und Transparenz im gesamten Netzwerk gewährleisten.

Überlegen Sie bei Produktintegrationen genau, was den meisten Nutzen für Ihr Unternehmen bringt. Was sind Ihre Herausforderungen? Welche Systemfunktionen bringen Ihnen die meisten Vorteile?

3. **Effizienter Betrieb**
   Je einfacher das System zu bedienen ist, desto mehr können Sie von seinen Funktionen profitieren. Komplexe Lösungen, die schwierig zu bedienen sind, bieten nur eingeschränkt Vorteile und erhöhen oft noch den Verwaltungsaufwand der IT-Abteilung. Achten Sie deshalb besonders auf folgende Punkte:

   - **Benutzerfreundlichkeit.** Wie schnell und einfach lässt sich das System bereitstellen, überwachen und verwalten? Wie viele Management-Konsolen benötigen Sie? Je mehr Aufgaben Sie an einer zentralen Stelle erledigen können, desto besser.
   - **Kosten.** Handelt es sich um ein cloudbasiertes System oder müssen Sie lokale Server finanzieren und warten?
   - **Konsistenz.** Sind Dialoge, Anzeigen und Layout im gesamten System einheitlich? Wenn Sie sich mit einer Anzeige vertraut gemacht haben, können Sie dann auch die anderen einfach verstehen oder sehen alle unterschiedlich aus?

4. **Produktführerschaft**
   Der Umstieg auf ein synchronisiertes Sicherheits-System sollte nicht dazu führen, dass Sie Kompromisse beim Schutz eingehen. Achten Sie deshalb sowohl auf die Qualität des Systems als auch auf die Schutzfunktionen der einzelnen Produkte. Beginnen Sie mit Produkten, die eigenständig bereits sehr gut sind und im System noch mehr Vorteile bieten.

   - **Testergebnisse und Bewertungen.** Achten Sie bei der Auswahl darauf, dass die Produkte gut in Effizienztests (wie etwa SE Labs, AV-Test) und Marktanalysen (z. B. Gartner Magic Quadrant) abschneiden.

- **Kunden-Feedback.** Wie bewerten Kunden das Cybersecurity-System? Welche Vorteile haben sie überzeugt? Wurde das System den Verkaufsversprechen gerecht?
- **Anerkannte Marktführer.** Wählen Sie Produkte, die von Branchenexperten als marktführend eingestuft werden.

Anbieter im direkten Vergleich

Produktumfang

Security-Produkte	Sophos Synchronized Security	Fortinet Fortinet Security Fabric	Microsoft Intelligent Security Graph	SonicWall Capture Cloud	Cisco Stealthwatch and Identity Services Engine (ISE)	Palo Alto Application Framework
Endpoint	✓	✓	✓	✓ (SentinelOne)	✓	✓ (Traps)
Endpoint Detection and Response (EDR)	✓	✓	✓	✓	✓	✓
Server	✓	✓	✓	✓	✓	✓
Firewall	✓	✓		✓	✓	✓
E-Mail	✓	✓		✓	✓	
Mobile	✓		✓		✓	
WLAN	✓	✓		✓	✓	
Festplattenverschlüsselung	✓		✓			
Security-Awareness-Training	✓					
Cloudbasierte Workloads	✓	✓	✓		✓	✓
Für die Produktintegration sind weitere Subscriptions erforderlich		✓[1]			✓[2]	✓[3]

1. Zur Integration von FortiClient in Security Fabric ist eine „FortiGate Endpoint Telemetry and Compliance"-Lizenz erforderlich. IOC Service auf FortiAnalyzer erforderlich, um kompromittierte Hosts einzusehen.
2. Cisco Network Orchestrator Trusted Access erforderlich.
3. Threat Prevention-/WildFire-Subscription erforderlich.

Produktintegration

	Automatisierte Zero-Touch-Reaktion	Netzwerkweite Transparenz
Sophos Synchronized Security	‣ Kontinuierliche Überwachung des Sicherheitszustands von Geräten mittels Security Heartbeat™, ermöglicht eine automatische Reaktion auf Vorfälle ‣ Automatische Isolation kompromittierter Endpoints unabhängig vom Infektionsort: Endpoint oder Netzwerk ‣ Lateral Movement Prevention verhindert, dass sich Bedrohungen im Netzwerk ausbreiten ‣ Automatische Beschränkung des WLAN-Zugriffs für kompromittierte Endpoints ‣ Automatische Beschränkung des WLAN-Zugriffs für Mobilgeräte, die nicht den Compliance-Vorgaben entsprechen ‣ Automatischer Scan von Endpoint-Geräten bei Erkennen von schädlichen E-Mails ‣ Automatischer Widerruf von Verschlüsselungsschlüsseln bei Erkennen von Malware oder Eindringlingen	‣ Synchronized App Control identifiziert alle Anwendungen im Netzwerk, einschließlich bisher unbekannter Netzwerk- und Cloud-Anwendungen ‣ Threat Cases liefert vollständige Transparenz über sämtliche Ereignisse eines Vorfalls mit Angabe aller betroffenen Dateien und URLs/IPs ‣ Korrelation des Netzwerkverkehrs zu einzelnen Anwendungen auf einzelnen Computern
Fortinet Fortinet Security Fabric	‣ Automatische Isolation von kompromittierten Endpoints, wenn die Firewall eine Infektion erkennt	‣ Anzeige einer grafischen Übersicht über alle verbundenen Security Fabric-Geräte ‣ Endpoint-Status-Überwachung erkennt, ob FortiClient installiert ist ‣ Security Rating zeigt den Sicherheitsstatus des Unternehmens (separat lizenziert)
Microsoft Intelligent Security Graph	‣ Endpoint-Analyse kann in Defender ATP automatisch ausgelöst werden	‣ CASB identifiziert unbekannte Cloud-Anwendungen über den Windows Defender ATP-Client ‣ Windows Defender ATP und Office 365 ATP tauschen Daten aus, um die Nachverfolgung von Bedrohungen von der E-Mail-Zustellung bis zur Ausführung auf dem Endpoint zu gewährleisten
SonicWall Capture Cloud	‣ Automatisierung der komplexen Firewall-Bereitstellung sowie von Verwaltungs-Aufgaben ‣ Endpoint Protection-Client erleichtert die Bereitstellung und Verwaltung von TLS/SSL-Zertifikaten	‣ Cloud App Security (CAS) liefert Transparenz über Cloud Apps (in Analytics-Lizenz)
Cisco Stealthwatch and Identity Services Engine (ISE)	‣ Netzwerkzugriffskontrolle durch ISE auf der Basis von Compliance und anderen Faktoren ‣ Cisco Threat Response ermöglicht der IT-Security-Abteilung die manuelle Nachforschung und Reaktion auf Bedrohungen	‣ Cisco AMP verfolgt Bedrohungen auf E-Mail-, Firewall- und Endpoint-Ebene nach
Palo Alto Application Framework	‣ Reaktionsfunktionen hängen von der verwendeten Anwendung ab. Behebung wird in der Regel auf Netzwerkebene eingeleitet, z. B. Blockieren von URLs oder IP-Adressen	‣ Anwendungen haben Zugriff auf Sicherheitsinformationen von Netzwerk und Endpoints

Betriebliche Effizienz

Effizienz bei der Verwaltung	Sophos Synchronized Security	Fortinet Fortinet Security Fabric	Microsoft Intelligent Security Graph	SonicWall Capture Cloud	Cisco Stealthwatch and Identity Services Engine (ISE)	Palo Alto Application Framework
In der Cloud gehostete Verwaltung	✓		✓	✓	✓	
Eine Management-Konsole	✓	✓		✓		
Einheitliche Oberfläche aller Produkte	✓	✓		✓		

Produktführerschaft

Produktführerschaft	Sophos Synchronized Security	Fortinet Fortinet Security Fabric	Microsoft Intelligent Security Graph	SonicWall Capture Cloud	Cisco Stealthwatch and Identity Services Engine (ISE)	Palo Alto Application Framework
Gartner Magic Quadrant für Endpoint Protection-Plattformen (2018)	Leader	Niche Player	Visionary	Visionary	Visionary	Niche Player
Gartner Magic Quadrant für UTM/Enterprise Firewalls (2018)	Leader	Leader	n.v.	Challenger	Leader	Leader

Synchronized Security von Sophos

Seit der Veröffentlichung im Jahr 2015 vereint Synchronized Security die branchenführenden Endpoint- und Netzwerk-Lösungen von Sophos in einem leistungsstarken, vollständig integrierten Cybersecurity-System. Das Herzstück von Synchronized Security ist Sophos Central, eine intuitive Security-Plattform, mit der die IT alle Elemente über eine zentrale webbasierte Benutzeroberfläche verwalten kann. Über den Security Heartbeat™ tauschen die Produkte in Echtzeit Informationen aus. Dadurch können sie automatisch auf Bedrohungen reagieren und bieten eine einmalige Transparenz über Cyberrisiken im gesamten Netzwerk.

Unsere Kunden bestätigen, dass Synchronized Security die Cybersecurity revolutioniert hat.

90% der Kunden geben an, dass sie ihren Netzwerkverkehr mit Synchronized Security besser kontrollieren können

85% der Kunden geben an, dass sie durch Sophos Synchronized Security in Sachen Sicherheit jetzt viel besser aufgestellt sind

84% der Kunden geben an, dass Synchronized Security erheblich zur Entlastung der IT-Abteilung beiträgt

Mehr Informationen zu Synchronized Security finden Sie unter www.sophos.de/synchronized.

Mehr Informationen unter www.sophos.de/synchronized

Die im vorliegenden Dokument enthaltenen Informationen basieren auf der Auslegung zum Zeitpunkt der Verfassung des Dokuments öffentlich verfügbarer Daten durch Sophos. Dieses Dokument wurde von Sophos und nicht von den anderen aufgeführten Anbietern erstellt. Änderungen der Eigenschaften und Funktionen der verglichenen Produkte, die direkten Einfluss auf die Richtigkeit oder Gültigkeit dieses Vergleichs haben können, sind vorbehalten. Die in diesem Dokument enthaltenen Informationen sollen ein allgemeines Verständnis sachlicher Informationen zu verschiedenen Produkten vermitteln und sind möglicherweise nicht vollständig. Alle dieses Dokument verwendenden Personen sollten auf Basis ihrer Anforderungen ihre eigenen Kaufentscheidungen treffen und sollten auch Original-Informationsquellen zu Rate ziehen und sich bei der Wahl eines Produkts nicht nur auf dieses Dokument verlassen. Sophos gibt keine Garantie für die Zuverlässigkeit, Richtigkeit, Zweckmäßigkeit oder Vollständigkeit der in diesem Dokument enthaltenen Informationen. **Die Informationen in diesem Dokument werden in der vorliegenden Form und ohne jegliche Garantie bereitgestellt.** Sophos behält sich das Recht vor, dieses Dokument jederzeit zu ändern oder zurückzuziehen.

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

SOPHOS