SOPHOS
Cybersecurity evolved.

IT-Sicherheit in Zeiten von Homeoffice & Co

So schützen Sie alle Standorte, Geräte und Ressourcen

Sophos-Whitepaper Februar 2021

Homeoffice ist längst zur Norm geworden: Einer Umfrage von Gartner zufolge gehen 74 % der Unternehmen weltweit davon aus, dass viele Mitarbeiter selbst nach der Pandemie weiter von zu Hause aus arbeiten werden[1]. Gleichzeitig befinden sich auch die Ressourcen, die Mitarbeiter für ihre Arbeit benötigen, an mehreren Standorten: auf Servern im Büro, in cloudbasierten Anwendungen wie Office 365 oder Salesforce sowie in privaten oder öffentlichen Cloud-Umgebungen auf Amazon Web Services (AWS) und Microsoft Azure.

IT-Teams kommt dabei die schwierige Aufgabe zu, alle Mitarbeiter, Geräte und Ressourcen zu schützen – unabhängig davon, wo sich diese befinden. Unterdessen entwickeln Hacker immer bessere und perfidere Methoden, um Schlupflöcher in der Abwehr zunehmend virtueller Unternehmen zu finden.

Doch wie sieht ein umfassender Schutz für Unternehmen aus, deren Mitarbeiter und Ressourcen auf verschiedenste Orte verteilt sind? Die folgenden Punkte müssen gewährleistet sein:

- Sichere Konnektivität, damit Benutzer von überall aus auf Ressourcen zugreifen können: im Büro, zu Hause, beim Kunden, unterwegs, etc.
- Schutz für Geräte, über die Verbindungen hergestellt werden, wie Desktops, Laptops, Mobiltelefone oder Tablets
- Schutz für Daten und Workloads, auf die Benutzer Zugriff benötigen – unabhängig davon, ob sie sich in der Cloud oder in Ihrem lokalen Netzwerk befinden
- Einfache Verwaltung, damit IT-Teams mühelos dezentrale Strukturen von überall aus betreuen können

Sophos bietet ein komplettes Portfolio von Next-Gen-Security-Produkten mit modernsten Schutzfunktionen, die das o. g. Anforderungsspektrum abdecken. Alles wird über eine zentrale, webbasierte Security-Plattform gesteuert, die den täglichen Verwaltungsaufwand auf ein Minimum reduziert und IT-Abteilungen ermöglicht, die Sicherheit ihres Unternehmens von jedem beliebigen Ort aus zu verwalten.

In diesem Solution Brief beleuchten wir die jeweiligen Anforderungskriterien und stellen entsprechende Lösungen zum Schutz Ihrer zunehmend mobilen Arbeitsumgebungen vor. Zudem erfahren Sie, wie Sie mithilfe eines Cybersecurity-Systems von Sophos für höchste Sicherheit und maximale Produktivität sorgen.

Sichere Konnektivität

Die Corona-Pandemie hat zweifellos zu einer enormen Ausweitung der Remote-Arbeit, inklusive Videokonferenzen, geführt. Seit Beginn der Pandemie haben so viele Arbeitnehmer wie nie zuvor zumindest teilweise oder sogar komplett von zu Hause gearbeitet. Remote-Arbeit ist jedoch nicht erst seit Corona ein Trend: Viele Mitarbeiter wechselten schon vor der Pandemie flexibel tageweise zwischen Büro und Homeoffice.

Von der Arbeit im Homeoffice profitieren Unternehmen und Mitarbeiter gleichermaßen: Mitarbeiter sparen sich den Weg zur Arbeit. Das Ergebnis: mehr Zeit, weniger Fahrtkosten, zusätzliche Flexibilität und höhere Produktivität. Und Unternehmen profitieren von geringeren Kosten und niedrigeren Fluktuationsraten. Für IT-Abteilungen ist der Trend zu mobilen Arbeitskonzepten jedoch auch mit zusätzlichen Sicherheitsrisiken verknüpft. Ganz gleich, ob Ihre Mitarbeiter sich vom heimischen Wohnzimmer, vom Büro eines Kunden oder über den WLAN-Hotspot eines Cafés am anderen Ende der Welt einwählen: Ihr Netzwerk und Ihre Daten müssen jederzeit geschützt bleiben.

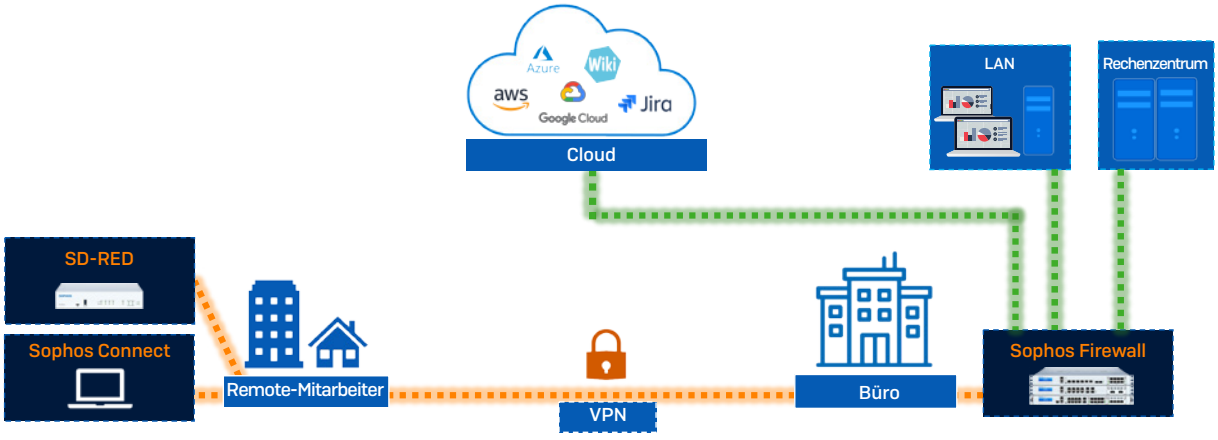
Mit den Lösungen von Sophos können Ihre Mitarbeiter schnell, effizient und sicher von überall aus eine Verbindung herstellen und arbeiten. Sophos bietet sowohl klassische VPN-basierte als auch „Zero Trust Network Access (ZTNA)"-Optionen an.

VPN

Der **Sophos Connect VPN Client** ist kostenlos verfügbar und lässt sich einfach anwenden. In Kombination mit der **Sophos Firewall** können Sie Ihre Remote-Mitarbeiter an die Zentrale anbinden, sodass sie problemlos sämtliche cloudbasierten Ressourcen nutzen können. Mit über 1,4 Mio. Anwendern weltweit bietet Sophos Connect Ihren Mitarbeitern, die Windows- und macOS-Geräte mobil nutzen, sicheren Zugriff auf Ressourcen im Unternehmensnetzwerk oder in der Public Cloud.

Sophos SD-RED (Remote Ethernet Device) ist ein einfaches Plug-and-Play-Gerät, das gemeinsam mit der **Sophos Firewall** zur Anbindung von Filialen, Remote-Standorten und Einzelpersonen mit Ihrem Hauptnetzwerk (physisch oder in der Cloud) genutzt werden kann.

SD-RED bietet ein immer aktives dediziertes oder Split-Tunnel-VPN und lässt sich dank flexibler Optionen einfach bereitstellen und verwalten. Das kleine, tragbare Gerät eignet sich ideal für Anwender, die jederzeit und von jedem Ort aus eine sichere Anbindung benötigen.



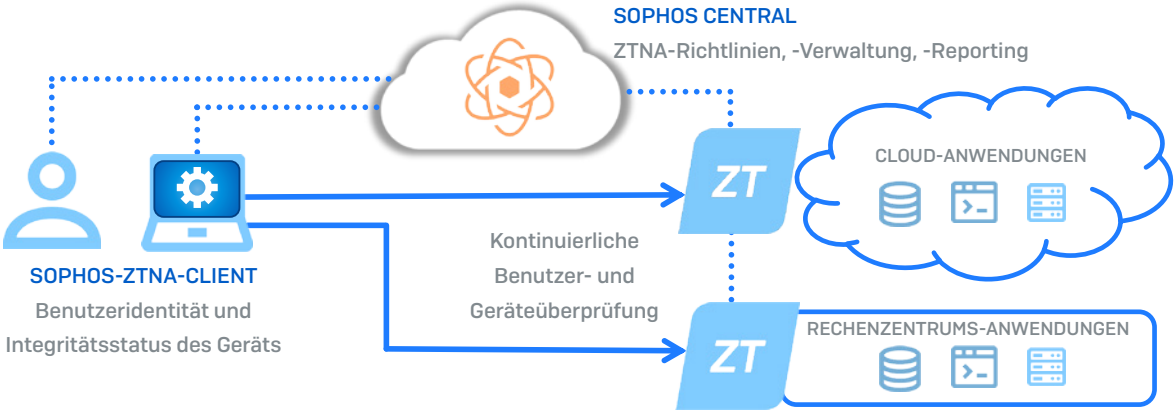
Sichere Remote-Konnektivität mit der Sophos Firewall und Sophos Connect VPN und SD-RED

ZTNA

VPN-Technologie hat Mitarbeitern über viele Jahre hinweg einen zuverlässigen Remote-Zugriff auf Unternehmensressourcen ermöglicht. Zu Beginn der Pandemie war VPN außerdem der Retter in der Not, der Unternehmen in nur wenigen Tagen ermöglichte, sicher auf Remote-Arbeit umzustellen. Die Anforderungen vieler Unternehmen gehen jedoch mittlerweile über das Leistungsspektrum von VPN hinaus.

Sophos Zero Trust Network Access (ZTNA) ist eine erstklassige Alternative zu Remote Access VPN und ermöglicht Benutzern, von jedem Ort aus einfach und transparent auf Unternehmensressourcen zuzugreifen. Gleichzeitig erhöht ZTNA auch Ihre Sicherheit, da die Benutzer ständig überprüft werden – in der Regel mit mehrstufiger Authentifizierung und einem Identitätsanbieter. Auch der Sicherheitsstatus und die Compliance des Geräts werden fortlaufend kontrolliert.

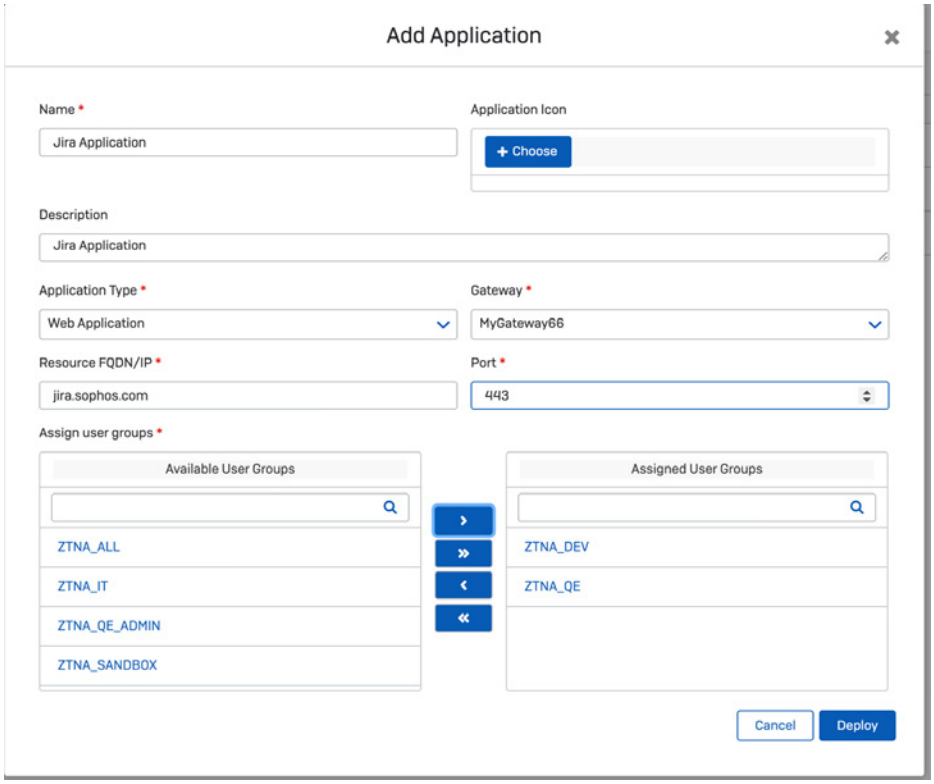
Sophos ZTNA stellt sicher, dass das Gerät registriert und ordnungsgemäß geschützt und die Verschlüsselung aktiviert ist. Anhand dieser Informationen werden auf Basis anpassbarer Richtlinien Benutzerrechte und -zugriff auf wichtige Anwendungen im Netzwerk gesteuert.



Das Prinzip von Sophos ZTNA

Mit Sophos ZTNA können Sie:

- Ihre Cyber-Abwehr optimieren: Sophos ZTNA bietet Ihnen sehr feinstufige Kontrollen. Sie können jeden Benutzer, jedes Gerät und jede Anwendung auf Basis Ihrer spezifischen Unternehmensrichtlinien und der für Sie akzeptablen Risikostufe individuell steuern. Zudem prüft ZTNA kontinuierlich die Benutzeridentität und den Gerätestatus, bevor Zugriff gewährt wird. So wird das Risiko lateraler Bewegungen innerhalb des Netzwerks minimiert.
- Die Effizienz steigern: Da Sophos ZTNA über die Plattform Sophos Central verwaltet wird, können IT-Abteilungen neue Benutzer einfach registrieren und flexibel auf Änderungen der Arbeitsumgebung reagieren. Auch für die Enduser ist diese Lösung transparenter, da sie im Gegensatz zum klassischen VPN reibungslos funktioniert, ohne dass die Benutzer sich erneut authentifizieren müssen.



Einfaches Hinzufügen von Anwendungen mit Sophos ZTNA

Egal, für welche Methode Sie sich entscheiden: Mit den vielfach ausgezeichneten Security-Produkten von Sophos schützen Sie Ihre Mitarbeiter auf jedem Gerät, an jedem Ort.

Schutz für Geräte

51 % der Unternehmen wurden im letzten Jahr von Ransomware getroffen. Bei 73 % dieser Vorfälle gelang es Angreifern, Daten zu verschlüsseln[2].

Wenn man sich neben diesen alarmierenden Zahlen vor Augen führt, dass Unternehmen unterschiedlichste Geräte – Desktops, Laptops, firmeneigene und Privatgeräte – sowie ein ganzes Arsenal an Betriebssystemen (Windows, macOS, Linux, Android, Chromebook, iOS usw.) schützen müssen, ist es kaum verwunderlich, dass die meisten IT-Abteilungen an ihre Grenzen stoßen.

Sophos Intercept X bietet Ihnen branchenführenden Schutz für alle diese Geräte und Plattformen. Sie profitieren von mehreren Technologieschichten, die Angreifer an zahlreichen Punkten in der Kill Chain stoppen. Enthalten sind u.a.:

- Anti-Ransomware-Schutz, der die unbefugte Verschlüsselung von Dateien, Festplatten und Boot Records blockiert und sie in ihren sicheren Ursprungszustand zurückversetzt
- Deep-Learning-KI, die Bedrohungen anhand von Millionen von Dateiattributen analysiert und bekannte und unbekannte Malware stoppt, bevor diese ausgeführt werden kann
- Anti-Exploit-Technologie zum Blockieren von Exploits, Techniken aktiver Angreifer sowie dateilosen und skriptbasierten Angriffen
- Signaturbasierter Basisschutz, der bekannte Bedrohungen stoppt

Darüber hinaus schützt Sophos Intercept X jedes Gerät auf jeder Plattform, sodass Ihre Mitarbeiter auf jedem Gerät ihrer Wahl sicher arbeiten können:

- Windows- und macOS-Desktops und -Laptops
- Windows- und Linux-Server
- Virtuelle Desktop-Umgebungen, die von Cloud-Anbietern gehostet werden
- Android- und iOS-Mobilgeräte oder Chromebooks

Endpoint Detection and Response (EDR)

Die verheerendsten Cyber-Bedrohungen sind von Hackern manuell durchgeführte Angriffe, bei denen häufig legitime Tools und Prozesse wie PowerShell ausgenutzt werden. Bei diesem interaktiven Live-Hacking wenden die Hacker immer neue Taktiken, Techniken und Prozesse (TTPs) an, die es ihnen ermöglichen, Sicherheitssysteme und Protokolle zu umgehen. Sobald die Angreifer in Ihr Netzwerk gelangt sind, können sie sich lateral fortbewegen und so Daten exfiltrieren, Ransomware bereitstellen und Malware oder Backdoors für zukünftige Angriffe installieren.

Um solche manuellen Hacker-Angriffe zu stoppen, ist manuelles Threat Hunting durch Bedrohungsexperten erforderlich. Mit **Intercept X with EDR** (Endpoint Detection and Response) können Sie Threat Hunts über dieselbe Konsole durchführen, über die Sie auch Ihre Intercept X Endpoint Protection verwalten.

Intercept X with EDR ist die erste speziell für Sicherheitsanalysten und IT-Administratoren entwickelte EDR-Lösung. Während bei anderen EDR-Tools nicht selten ein Spezialteam oder ein internes Security Operations Center (SOC) erforderlich ist, bleibt Sophos EDR trotz umfassender Analyse-Funktionen einfach und benutzerfreundlich.

Mit den leistungsstarken, individuell anpassbaren SQL-Abfragen von Intercept X with EDR können Sie verdächtige Signale und Bedrohungen untersuchen und dafür sorgen, dass Sicherheitsvorgaben eingehalten werden. Typische Anwendungsbeispiele:

- Chrome läuft langsam: Ermitteln, welche nicht autorisierten Chrome-Erweiterungen installiert wurden
- Netzwerkaktivitäten überprüfen: Nach fehlgeschlagenen Anmeldeversuchen und aktiver Kommunikation von PowerShell suchen
- Software-Abfragen: Überprüfen, ob vertrauliche Dateien von Geräten entfernt wurden und/oder ob Sie die Softwarelizenznutzung überschritten haben
- Phishing-Analyse: Benutzer identifizieren, die auf einen verdächtigen Link geklickt haben, und ermitteln, ob sie Dateien heruntergeladen haben

Außerdem können Sie über ein Befehlszeilentool remote auf Geräte zugreifen, um Probleme zu beheben. So lassen sich beispielsweise Geräte neu starten, aktive Prozesse beenden, Skripts oder Programme ausführen, Konfigurationsdateien bearbeiten, forensische Tools ausführen und Software installieren/deinstallieren.

Managed Detection and Response (MDR)

Wenn Sie nicht über die Zeit, Kapazitäten oder Expertise verfügen, um Ihre eigenen Threat Hunts und Analysen durchzuführen, sollten Sie auf Services wie **Sophos Managed Threat Response** (MTR) zurückgreifen.

Mit Sophos MTR steht Ihnen ein Expertenteam zur Seite, das 24/7 Managed Detection and Response mit Threat Hunting als Fully-Managed-Service anbietet. Das Team spürt Bedrohungen aktiv auf und prüft potenzielle Vorfälle – so können frühzeitig wirksame Gegenmaßnahmen getroffen werden.

Außerdem korreliert Sophos MTR Daten-Feeds von Ihren Sophos-Schutzlösungen, um Indikatoren einer Kompromittierung („Indicators of Compromise") zu identifizieren. Im Gegensatz zu anderen Managed Detection und Response Services benachrichtigt das Sophos MTR-Team Sie bei Problemen nicht bloß, sondern ergreift konkrete Maßnahmen, um die Bedrohung im Keim zu ersticken.

Mobile Endpoints verwalten und schützen

Wenn Mitarbeiter private Endgeräte beruflich nutzen, stehen IT-Abteilungen vor der Herausforderung, Unternehmensdaten zu schützen, ohne die Privatsphäre der Benutzer zu verletzen. **Sophos Mobile** schützt iOS-, Android-, Chrome-OS-, Windows-10- und macOS-Geräte. Diese Unified-Endpoint-Management-Lösung ermöglicht Ihnen, jede beliebige Kombination privater und firmeneigener Geräte mit minimalem Aufwand zu schützen. Sie ist somit ideal für BYOD-Szenarien (Bring Your Own Device) geeignet.

Mit Sophos Mobile können Sie:

- Bedrohungen für Mobilgeräte stoppen: Sophos Mobile basiert auf den leistungsstarken Funktionen von Intercept X und bietet branchenführenden Schutz vor Malware, Phishing, Man-in-the-Middle-Angriffen und weiteren Bedrohungen.
- Unternehmensdaten schützen: Ob Verwaltung des kompletten Geräts oder reine Container-Verwaltung – wählen Sie einfach die für Sie passende Kontrolle Ihrer Daten.
- Verwaltungsaufwand reduzieren: Über das flexible Self-Service-Portal können Benutzer in Eigenregie ihre privaten macOS-, Windows-10- oder Mobilgeräte registrieren, Passwörter zurücksetzen und Hilfestellung erhalten, ganz ohne Support der IT-Abteilung.

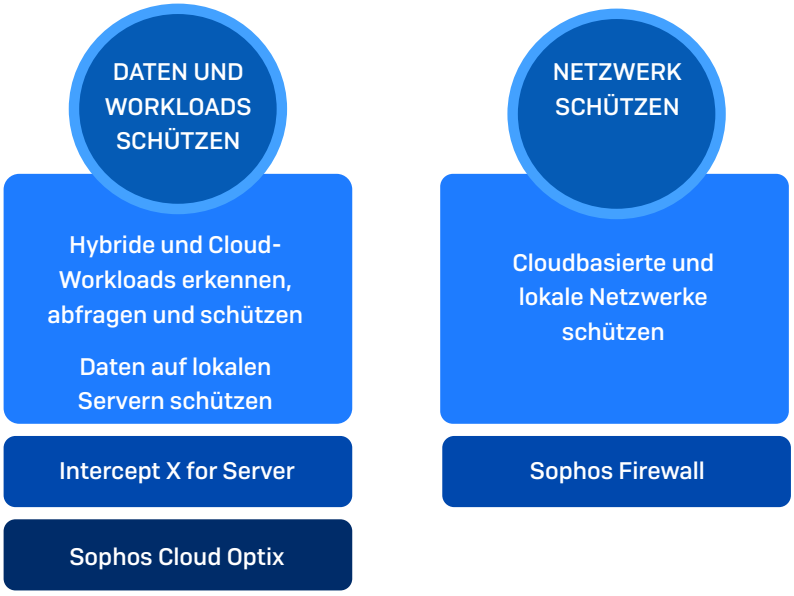
Schutz für Ressourcen

Sie führen Server vor Ort aus, nutzen cloudbasierte Anwendungen oder hosten Ressourcen in privaten und öffentlichen Cloud-Umgebungen auf AWS, Azure oder GCP? Je nach den Anforderungen Ihres Unternehmens nutzen Sie vermutlich einige oder evtl. sogar alle diese Möglichkeiten.

Denn die Cloud spielt im Alltag der meisten Unternehmen eine immer größere Rolle. Diese Entwicklung ist auch Cyberkriminellen nicht verborgen geblieben – so verzeichneten 70 % der Unternehmen, die die Public Cloud nutzen, in den letzten 12 Monaten[3] einen Sicherheitsvorfall in der Cloud.

Beim Schutz Ihrer Ressourcen – unabhängig davon, wo diese sich befinden – sind zwei Dinge wichtig:

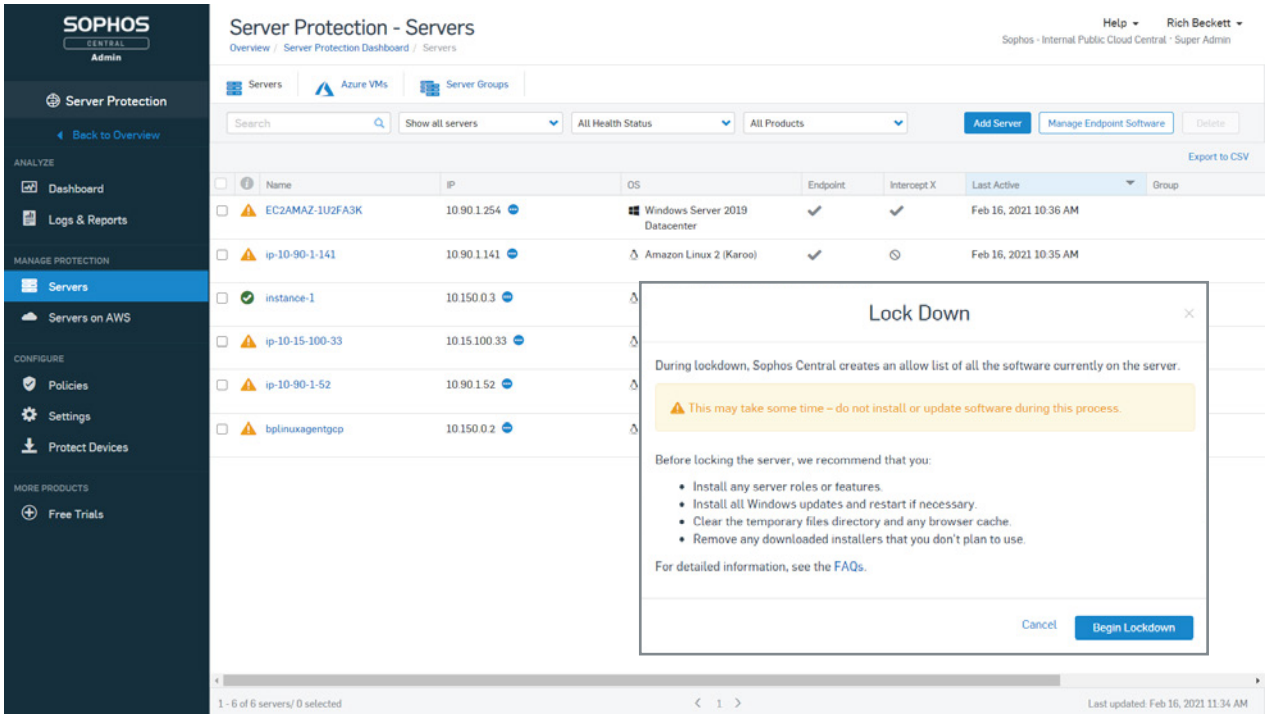
1. Sie müssen die Daten und Workloads schützen
2. Sie müssen das Netzwerk schützen, damit Angreifer sich keinen Zugriff verschaffen können



Daten und Workloads schützen

Daten und Workloads gehören zu Ihren wichtigsten Assets. **Sophos Intercept X for Server** sichert lokale, Cloud- oder Hybrid-Workload-Umgebungen und schützt virtuelle Windows- und Linux-Maschinen und -Desktops vor den neuesten Bedrohungen.

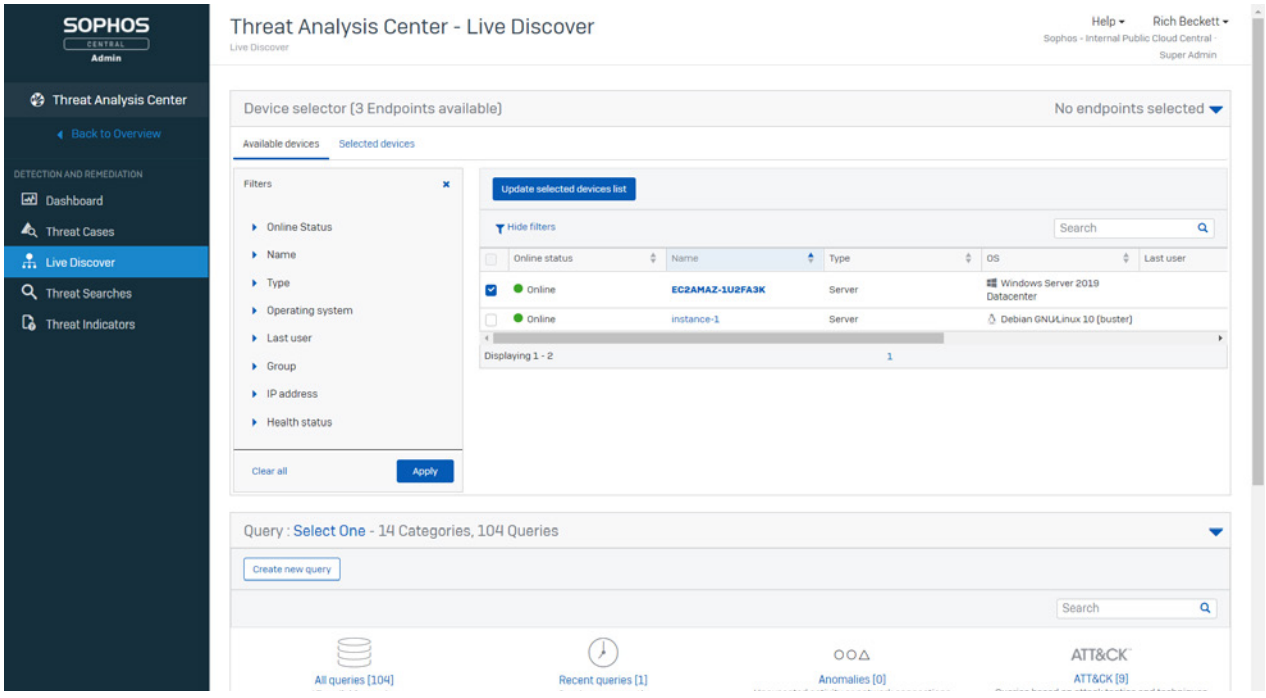
- Komplexe Angriffe stoppen: Wehren Sie Bedrohungen wie Ransomware, Exploit-basierte Angriffe und neuartige Malware ab
- Server-Workloads sperren (Lockdown): Kontrollieren Sie genau, was ausgeführt werden darf, und lassen Sie sich benachrichtigen, wenn versucht wird, nicht autorisierte Änderungen vorzunehmen
- Alles zentral verwalten: Installieren und verwalten Sie Ihre gesamte Infrastruktur über eine zentrale Konsole – selbst in gemischten Umgebungen mit Cloud-Workloads und lokalen Servern



Intercept X for Server

Mit **Intercept X for Server with EDR** lassen sich Ihre EDR-Analysen auch auf Ihre lokalen und Cloud-Server ausweiten. So können Sie:

- Wichtige IT-Operations- und Threat-Hunting-Aufgaben erledigen, wie: Performance-Probleme erkennen, sich einen Überblick über Installationen verschaffen und verdächtigen Aktivitäten auf den Grund gehen.
- Cloud-Workloads automatisch erkennen: Sie behalten wichtige Cloud-Services im Blick, einschließlich S3 Buckets, Datenbanken und serverlosen Funktionen
- Unsichere Bereitstellungen erkennen: Ihre Cloud-Umgebungen werden per KI-Monitoring konstant überwacht, Unregelmäßigkeiten werden sofort gemeldet

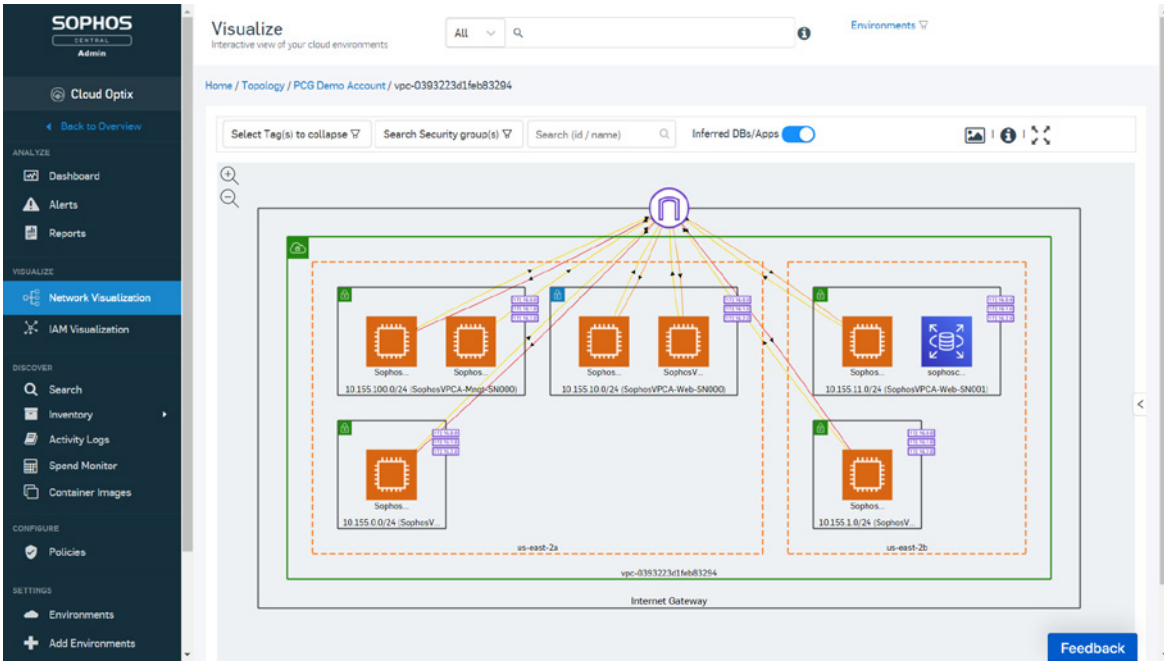


Ihre EDR-Analysen auf Ihren Server ausweiten

Neben dem Schutz Ihrer Daten und Workloads ist Transparenz von ebenso großer Bedeutung. So benötigen Sie stets einen klaren Einblick in ausgeführte Elemente und sollten in der Lage sein, Cloud-Provider-Services zu konfigurieren, um mögliche Sicherheitslücken zu schließen.

Sophos Cloud Optix ist eine „Cloud Security Posture Management"-Lösung, die Ihnen diese Informationen liefert, einschließlich:

- Multi-Cloud-Transparenz: Sie erhalten ein detailliertes Inventory aller Cloud-Ressourcen – Server, Container, Speicher, Netzwerk und IAM für AWS, Azure und GCP
- Risikobasierte Priorisierung: Sie analysieren fortlaufend Konfigurationen auf Sicherheitsrisiken und überprivilegierten IAM-Zugriff
- Compliance-Verwaltung: Sie überwachen kontinuierlich die Compliance mithilfe unterschiedlicher Vorlagen, benutzerdefinierter Richtlinien und Collaboration-Tools
- Integrierte Sicherheit: Sie identifizieren Sophos Firewalls und Workload-Schutz auf AWS
- Cloud-Kostenoptimierung: Sie verwalten AWS- und Azure-Ausgaben gemeinsam auf einem Bildschirm



Sophos Cloud Optix

Sicherheits-Warnmeldungen für Ihre Cloud-Umgebungen haben durchaus ihren Nutzen. Auch Dienste wie Amazon GuardDuty bieten erstklassigen Service. Allerdings kann die schiere Menge an Warnmeldungen Sicherheitsteams schnell überfordern. Denn oft ist es praktisch unmöglich, schnell zu erkennen, welche Benachrichtigungen tatsächlich relevant sind.

Die Amazon-Web-Services-Umgebungen, in denen unsere Cybersecurity-Plattform Sophos Central gehostet wird, schützen wir mit Sophos Cloud Optix. Dies ermöglicht unserem eigenen Sicherheitsteam, sich auf die wirklich wichtigen Informationen zu konzentrieren.

„Mit Sophos Cloud Optix minimieren wir die Flut irrelevanter Warnmeldungen erheblich. Die leistungsstarke künstliche Intelligenz in Sophos Cloud Optix korreliert die Daten und zeigt uns nur wirklich wichtige Warnungen, auf die wir reagieren müssen."

Ross McKerchar, VP und CISO, Sophos

Netzwerke schützen

Um Ihre Ressourcen zu schützen, müssen Sie auch die Netzwerke schützen, in denen die Ressourcen ausgeführt werden. Hier hilft die **Sophos Firewall**: Sie bietet einzigartige Sicherheit und Transparenz für lokale, AWS- und Azure-Umgebungen.

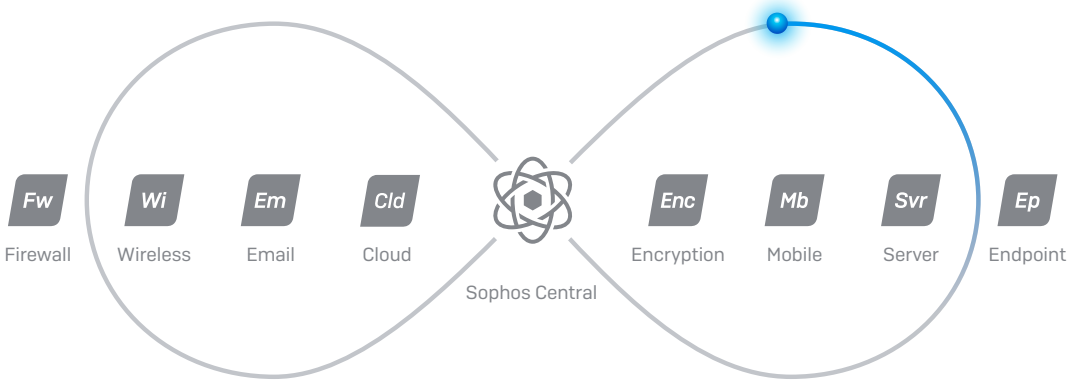
- Integrierter, mehrschichtiger Schutz, der selbst hochkomplexe Bedrohungen stoppt
- Leistungsstarke All-in-One-Lösung für WAF, IPS, ATP, URL-Filterung, pfadbasiertes Routing und länderbasierte Blockierung mit umfangreichen Reports, die einen umfassenden Einblick in Benutzer- und Netzwerkaktivitäten ermöglichen
- Cloud-Transparenz, Einblicke in Schatten-IT und automatische Reaktion auf Bedrohungen
- Härten Ihrer Cloud-Workloads gegen Hacking-Versuche wie SQL Injection und Cross-Site Scripting und Bereitstellen eines sicheren Benutzerzugriffs mittels Reverseproxy-Authentifizierung
- Flexible Ausführung als eigenständige und hochverfügbare Lösung

Um die cloudbasierte Bereitstellung zu erleichtern, ist die komplette Software in einem einzigen, vorkonfigurierten virtuellen Maschinen-Image erhältlich.

Einfache Verwaltung

Mit Sophos können Sie Ihre gesamte IT-Sicherheit über eine einzige Web-Plattform verwalten: Sophos Central. Sie müssen nicht mehr zwischen verschiedenen Konsolen jonglieren, um Ihr Unternehmen zu schützen. Sie finden alle Funktionen an einem zentralen Ort. Außerdem können Sie problemlos produktübergreifende Analysen durchführen und Daten von mehreren Services einfach korrelieren.

Da Sophos Central in der Cloud gehostet wird, ist die Lösung optimal für dezentrale IT-Teams geeignet. Mit mehr als 400.000 Benutzern weltweit entscheiden Sie sich mit Sophos Central für die Cloud-Security-Plattform, der weltweit die meisten Kunden vertrauen und die sich in der Praxis bewährt hat.



Zudem können Sophos-Produkte mittels Sophos Central bedrohungs- und sicherheitsbezogene Informationen in Echtzeit austauschen und gemeinsam auf Bedrohungen reagieren – wir nennen diese Technologie Synchronized Security. Die Vorteile:

- Automatische Reaktion auf Vorfälle: Wenn ein Sophos-Produkt verdächtige Aktivitäten erkennt – beispielsweise eine Malware-Infektion oder ein Gerät, das die Compliance nicht einhält – tauscht es diese Informationen mit dem gesamten Cybersecurity-System aus. Die anderen Produkte reagieren dann in Sekundenschnelle automatisch auf den Vorfall. Beispielsweise:
  - Die Sophos Firewall isoliert infizierte Geräte sofort und verhindert die Ausbreitung der Bedrohung sowie laterale Bewegungen.
  - Intercept X scannt Endpoints automatisch, wenn kompromittierte Posteingänge erkannt werden. Damit lässt sich das Risiko durch E-Mail-Bedrohungen wirksam eindämmen.
  - Sophos Wi-Fi schränkt den Netzwerkzugriff von Geräten ein, die nicht den Richtlinien entsprechen, sodass nicht autorisierte und unsichere Geräte nicht in Ihr WLAN gelangen.
- Einzigartige Transparenz: IT-Abteilungen profitieren von mehr Transparenz und Kontrolle über ihr Netzwerk und haben die Möglichkeit:
  - Infizierte Geräte anhand des Namens und nicht anhand der IP-Adresse zu erkennen, wodurch Sicherheitsanalysen beschleunigt werden.
  - Alle Anwendungen im Netzwerk zu identifizieren: Durchschnittlich passieren 43 % des Netzwerkverkehrs Ihre Umgebung als „nicht klassifiziert". Ihre IT-Abteilung hat also keinerlei Kontrolle darüber, ob dieser Traffic unbedenklich, schädlich oder gar bösartig ist. Mit Synchronized Security erhalten Sie ein leistungsstarkes Cybersecurity-System, in dem Sophos Firewall und Intercept X koordiniert zusammenarbeiten, um automatisch ALLE Anwendungen im Netzwerk zu identifizieren und zu klassifizieren.

Branchenführend in puncto Schutz und Effizienz

Mit einem Sophos-Cybersecurity-System erhalten Sie Next-Gen-Schutz, eine zentrale Verwaltungsplattform, produktübergreifenden Austausch von Bedrohungsdaten und automatisierte Incident Response. Gemeinsam sorgen diese Funktionen bei Ihrem IT-Team für deutlich mehr Effizienz und Produktivität.

Kunden, die Sophos Intercept X und die Sophos Firewall nutzen und über Sophos Central verwalten, berichten uns immer wieder, dass sich die **Effizienz ihrer IT-Abteilung verdoppelt hat** und gleichzeitig **85 % weniger Sicherheitsvorfälle zu verzeichnen sind**.

„Da die Tools die meisten Sicherheitsereignisse automatisch erkennen und beheben, bleibt unserer kleinen IT-Abteilung genügend Zeit, die Sicherheit des Unternehmens zu verwalten und Kompromittierungen zu unterbinden."

Chief Technology Officer, Software Services Provider

Schutz für alle Standorte, Geräte und Ressourcen

Flexibles Arbeiten von verschiedenen Orten und Geräten aus ist unaufhaltsam auf dem Vormarsch. Auch die Nutzung cloudbasierter Anwendungen lässt sich nicht mehr zurückdrehen. Denn diese flexiblen Arbeitsformen erleichtern uns den Alltag. Doch sie stellen IT-Abteilungen auch vor ungeahnte Herausforderungen und bieten Cyberkriminellen neue Angriffsflächen. Um die heutigen Arbeitsumgebungen wirksam zu schützen, sind – unabhängig vom Standort – sichere Verbindungen, Ressourcen und Geräte erforderlich – und zwar ohne zusätzliche IT-Budgets.

Die leistungsstarken Lösungen von Sophos unterstützen Sie dabei, diese neuen Herausforderungen zu meistern. Wenden Sie sich an Ihren Sophos-Ansprechpartner, um Ihre spezifischen Anforderungen persönlich zu besprechen, oder testen Sie unsere Produkte unverbindlich mit einer kostenlosen Testversion.

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

2 The State of Ransomware 2020, Sophos

3 The State of Cloud Security 2020, Sophos

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

210215 WPDE (MP)

SOPHOS