LÖSUNGSBROSCHÜRE

Sophos MDR

Erkennung und Reaktion, mit der Sie Angreifern einen Schritt voraus bleiben und wichtige Sicherheitsprobleme lösen

Egal wie Ihr aktueller Cybersecurity-Status ist: Sophos Managed Detection and Response (MDR) Services bieten umfassende MDR-Optionen, die Ihr Risiko reduzieren, Ihr Sicherheitskonzept vereinfachen, Ihre Technologie-Investitionen optimal ausschöpfen und Ihre Abwehr stärken.

Die Lösung für heutige Sicherheitsprobleme

Bedrohungen einen Schritt voraus zu bleiben, wird immer schwieriger: Die Bedrohungslandschaft ändert sich rasant, mit ständig neuen Angriffstaktiken und Ransomware-Typen. Unternehmen und Organisationen bemühen sich, mehr interne Sicherheitsexperten einzustellen, auszubilden und langfristig zu binden, aber die Fluktuation und Burnout-Raten sind hoch. Die zur Verfügung stehenden Mitarbeitenden tun sich schwer, die Informationsflut verschiedener Sicherheitstools zu verarbeiten und die Schutzlücken zu schließen, die durch die fehlende Verknüpfung der Tools entstehen.

Die Probleme in Zahlen

Ransomware-Angriffe, die außerhalb der normalen Geschäftszeiten beginnen[1]

Ransomware-Angriffe mit Missbrauch von Zugangsdaten oder Ausnutzung einer unbekannten Schwachstelle[2]

Weltweiter Mangel an qualifizierten Cybersecurity-Experten[3]

Ransomware-Opfer, die nicht genug Fachkräfte oder Expertise hatten, um den Angriff zu stoppen[4]

IT-/Sicherheitsexperten, die im letzten Jahr unter Cybersecurity-Erschöpfung und -Burnout litten[5]

Sophos MDR Services

In unserem Angebot finden Sie den optimalen MDR-Service für Ihre Anforderungen – passend zu Unternehmensgröße, Branche, Budget und Cybersecurity-Reifegrad. Falls sich Ihre Anforderungen ändern, können Sie den Service mit zusätzlichen Optionen anpassen. Unsere MDR-Services sind eine Kombination aus benutzerfreundlichen, KI-basierten Technologien und hochspezialisierten Sicherheitsexperten, die Bedrohungen rund um die Uhr überwachen, abwehren, erkennen und auf sie reagieren.

Vorteile

- **Weniger Risiko:** Starker Schutz, basierend auf neuesten Erkenntnissen zu Angreifer-Trends und -Techniken, der Expertise erfahrener Bedrohungsforscher sowie Ergebnissen aus Sicherheitstests und Threat Hunts
- **Konsolidiertes Sicherheitskonzept:** Daten verschiedener Sicherheitsprodukte in einer zentralen Plattform – zur Korrelierung, Bewertung und Entscheidungsfindung
- **Optimale Nutzung Ihrer Technologie-Investitionen:** Hunderte führender Sicherheitsprodukte integriert in einen einzigen Service – Endpoint, Cloud, Identity, Netzwerk, Backup, E-Mail. Weitere Integrationen in Planung
- **Stärkere Abwehr:** Detaillierte Analysen verdächtiger Aktivitäten, schnelle Reaktion auf bestätigte Bedrohungen und 24/7 Zugriff auf Sicherheitsanalysten und interdisziplinäre Experten

Leistungen von Sophos MDR

Sie erhalten ein sofort einsatzbereites, KI-beschleunigtes Security Operations Center (SOC).

Unser Team globaler Cybersecurity-Experten überwacht Ihre Umgebung 24/7 auf Bedrohungen.

Branchenführende Bedrohungsforscher entdecken kontinuierlich neue Bedrohungsgruppen und Angriffstechniken.

Proaktives Threat Hunting findet verborgene Bedrohungen, die von Sicherheitstools übersehen werden.

Mit umfassender Incident Response beseitigen Sie Angreifer vollständig. Ohne Obergrenze oder zusätzliche Gebühren.

Kontinuierliche Updates der Regeln zur Bedrohungserkennung und Technologie-Integrationen sorgen dafür, dass Sie geschützt bleiben.

Dank Optionen zur Datenspeicherung vermeiden Sie hohe Protokollspeicherkosten.

Über verschiedene Service-Level und Reaktions-Optionen passen Sie Sophos MDR individuell an Ihre Anforderungen an.

Sie erhalten Schnellzugriff auf fachübergreifende Cybersecurity-Expertise.

Funktionen

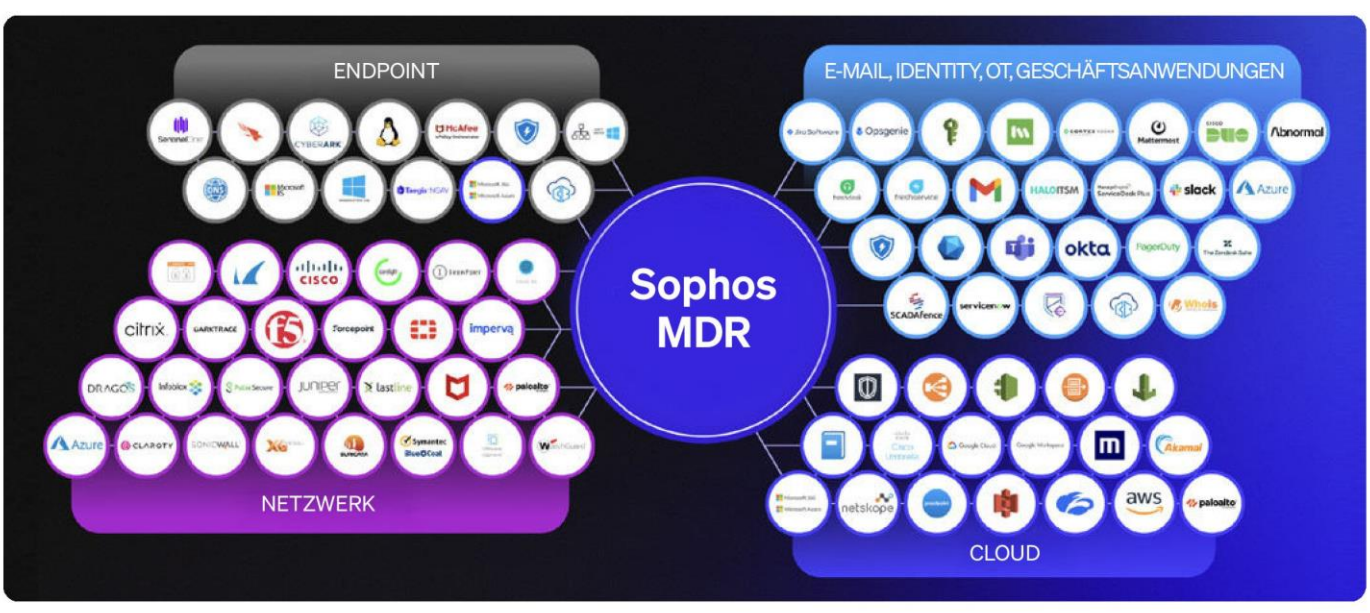
- 24/7 Bedrohungsüberwachung, -erkennung, -analyse und -reaktion
- Umfangreiche Integrationen ohne Extrakosten für Endpoint, Netzwerk, Cloud, Identity, E-Mail, OT und mehr.
- Schneller Zugriff auf interdisziplinäre Sicherheitsexperten
- Threat Hunting durch Experten
- Ursachenanalyse
- Breach Protection Warranty

Reduzieren Sie Ihr Risiko

Angriffsflächen werden immer größer, und Sie müssen eine stetig wachsende Technologielandschaft schützen. Sophos MDR nutzt die Vorteile von Automatisierung und einer KI-nativen Plattform – kombiniert mit umfassender Threat Intelligence, Forschung und Erkenntnissen aus Threat Hunts und Sicherheitstests –, um aus der Vielzahl von Datenmeldungen echte Bedrohungen herauszufiltern und schnellstmöglich zu beseitigen. So können wir schnell die größten Bedrohungen für Ihr Unternehmen priorisieren.

Nutzen Sie vorhandene Technologien

Schöpfen Sie bereits getätigte Investitionen in Cybersecurity-Produkte optimal aus, ohne Ihre bisherige IT-Infrastruktur auszutauschen. Mit mehr als 350 Technologie-Integrationen können wir Telemetriedaten von führenden Drittanbieter-Produkten erfassen, um die Bedrohungserkennung und -reaktion zu beschleunigen. So erhalten Sie mehr Flexibilität, wenn sich Ihr Produkt-Footprint in Zukunft ändern sollte.



Das Bild zeigt eine repräsentative Auswahl unserer über 350 Technologie-Integrationen.

Ein umfassendes Team von Sicherheitsexperten

Sicherheitsexperten sind schwer zu finden. Und sie langfristig zu binden, ist noch schwieriger. Sophos MDR löst diesen Problem mit einem Team von interdisziplinären Sicherheitsexperten, die Ihnen bei jedem Schritt auf Ihrem Weg zu besserer Cybersecurity zur Seite stehen.

- **Sicherheitsanalysten:** Dienen als erste Verteidigungslinie und bieten Bedrohungsüberwachung, -analyse und Vorfallsreaktion 24/7.
- **Bedrohungsforscher:** Erforschen proaktiv Bedrohungsakteure, Angriffsaktivitäten und neuen Taktiken, Techniken und Prozesse.
- **Threat Hunter:** Führen indizien- und hypothesengesteuerte Suchen nach Angreiferaktivitäten durch, um versteckte Bedrohungen zu finden.
- **Incident Responder:** Führen Aktivitäten zur Abwehr, Eindämmung und Beseitigung komplexer Cybervorfälle durch, um Angreifer vollständig zu eliminieren und der Ursache auf den Grund zu gehen.
- **Detection Engineers:** Entwickeln und implementieren kontinuierlich neue Erkennungen, die auf Grundlage von Bedrohungsforschung, Incident Response, Threat Hunting und Sicherheitstests ermittelt werden.
- **Security Automation Engineers:** Optimieren und skalieren Betriebsabläufe, um irrelevante Informationen herauszufiltern und die Reaktion auf akute Bedrohungen zu beschleunigen.
- **Customer Success Team:** Fungiert als Ihr Fürsprecher und erste Anlaufstelle für alle Sophos-Anliegen.

WÜST-IT

Kontaktieren Sie uns.
Wir freuen uns auf Sie!

WÜST Datentechnik GmbH
Mühlstraße 1a
65582 Aull

06432/8005-0
info@wuest-it.de
www.wuest-it.de