

# Sophos Intercept X



## Intercept X Advanced, Intercept X Advanced with EDR, Intercept X Advanced with XDR, Intercept X Advanced with MTR

Sophos Intercept X ist die beste Endpoint Protection am Markt. Die Lösung stoppt neueste Cybersecurity-Bedrohungen mit einer Kombination aus Deep-Learning-KI, Anti-Ransomware-Funktionen, Exploit Prevention und anderen Techniken.

Sophos Intercept X nutzt einen umfassenden Ansatz zum Schutz Ihrer Endpoints und verlässt sich nicht auf eine einzelne Sicherheitstechnik. Dieser mehrschichtige Ansatz kombiniert moderne und traditionelle Techniken, um unterschiedlichste Bedrohungen zu stoppen.

### Stoppt unbekannte Bedrohungen

Die Deep-Learning-KI in Intercept X erkennt und blockiert neue und unbekannte Malware besonders zuverlässig. Um Bedrohungen ohne Signaturen zu erkennen, werden Dateiattribute aus Millionen von Samples untersucht.

### Blockiert Ransomware

Die modernen Anti-Ransomware-Funktionen von Intercept X erkennen und blockieren die bei Ransomware-Angriffen genutzten schädlichen Verschlüsselungsprozesse. Verschlüsselte Dateien werden wieder in ihren sicheren Zustand versetzt, wodurch Betriebsstörungen auf ein Minimum reduziert werden.

### Verhindert Exploits

Anti-Exploit-Technologie stoppt die Exploit-Techniken, mit denen Angreifer Geräte kompromittieren, Zugangsdaten stehlen und Malware in Umlauf bringen. Intercept X stoppt diese Techniken entlang der gesamten Angriffskette und schützt Ihr Unternehmen so vor dateilosen Angriffen und Zero-Day-Exploits.

### Mehrschichtige Abwehr

Neben leistungsstarken, modernsten Funktionen nutzt Intercept X auch bewährte traditionelle Verfahren. Diese Kombination aus modernen und traditionellen Techniken reduziert die Angriffsfläche und sorgt für eine einzigartig starke Cyberabwehr.

### Synchronized Security

Sophos-Lösungen arbeiten optimal zusammen und sind dadurch noch stärker. Intercept X und die Sophos Firewall tauschen beispielsweise Daten aus, um gefährdete Geräte während der Bereinigung automatisch zu isolieren. Sobald die Bedrohung beseitigt ist, wird der Netzwerkzugriff wiederhergestellt. Es ist keinerlei Eingreifen eines Administrators notwendig.

### Highlights

- ▶ Stoppt neue und unbekannte Bedrohungen mit Deep-Learning-KI
- ▶ Blockiert Ransomware und versetzt Dateien zurück in ihren sicheren Zustand
- ▶ Stoppt über die gesamte Angriffskette hinweg gezielt Exploit-Techniken
- ▶ Beantwortet wichtige IT-Operations- und Threat-Hunting-Fragen mit EDR
- ▶ Bietet 24/7/365-Sicherheit als Fully-Managed-Service
- ▶ Zeigt und nutzt Firewall-, E-Mail- und andere Datenquellen\* mit XDR
- ▶ Lässt sich einfach bereitstellen, konfigurieren und verwalten – selbst in Remote-Arbeitsumgebungen

*\* Cloud Optix und Sophos Mobile in Kürze verfügbar*

## Endpoint Detection and Response (EDR)

Sophos EDR wurde speziell für IT-Administratoren und Cybersecurity-Experten entwickelt und beantwortet wichtige IT-Operations- und Threat-Hunting-Fragen. Erkennen Sie beispielsweise Geräte mit Performance-Problemen oder verdächtigen Prozessen, die versuchen, eine Verbindung über Nicht-Standardports herzustellen, und greifen Sie remote auf die betroffenen Geräte zu, um Maßnahmen zur Bereinigung zu ergreifen.

## Extended Detection and Response (XDR)

Gehen Sie über Endpoints und Server hinaus und erfassen Sie auch Firewall-, E-Mail- und weitere Datenquellen\*. So erhalten Sie einen ganzheitlichen Überblick über die Cybersicherheit Ihres Unternehmens und haben die Möglichkeit, bei Bedarf jederzeit Detailinformationen abzurufen. Gehen Sie beispielsweise Problemen mit dem Büronetzwerk auf den Grund und ermitteln Sie, welche Anwendung diese verursacht.

*\*Integration von Sophos Cloud Optix und Sophos Mobile XDR erfolgt in Kürze*

## Managed Threat Response (MTR)

Unser 24/7/365 Threat Hunting Detection and Response Service „Sophos MTR“ wird durch ein Sophos-Expertenteam bereitgestellt. Sophos-Analysten reagieren auf potenzielle Bedrohungen, suchen nach „Indicators of Compromise“ und liefern detaillierte Analysen der Ereignisse – was ist wo, wann, wie und warum passiert?

## Einfache Verwaltung

Intercept X wird über Sophos Central verwaltet, die Cloud-Management-Plattform für alle Sophos-Lösungen. In dieser zentralen Konsole sehen Sie alle Geräte und Produkte und können Ihre Umgebung einfach bereitstellen, konfigurieren und verwalten – selbst wenn Ihre Belegschaft an verschiedensten Standorten und im Homeoffice arbeitet.

## Technische Spezifikationen

Intercept X unterstützt Windows- und macOS-Bereitstellungen. Aktuelle Informationen entnehmen Sie bitte den [Windows-Systemvoraussetzungen](#) und dem [Datenblatt „Intercept X for Mac“](#).

## Lizenzierungsübersicht

Funktionen	Intercept X Advanced	Intercept X Advanced with EDR	Intercept X Advanced with XDR	Intercept X Advanced with MTR Standard	Intercept X Advanced with MTR Advanced
<b>Basis-Schutz</b> (u. a. Application Control und Verhaltenserkennung)	✓	✓	✓	✓	✓
<b>Next-Gen-Schutz</b> (u. a. Deep Learning, Anti-Ransomware und Schutz vor dateilosen Angriffen)	✓	✓	✓	✓	✓
<b>EDR</b> (Endpoint Detection and Response)		✓	✓	✓	✓
<b>XDR</b> (Extended Detection and Response)			✓		siehe Fußnote*
<b>MTR</b> (Managed Threat Response – 24/7/365 Threat Hunting and Response Service)				✓	✓
<b>MTR Advanced</b> (indizienloses Threat Hunting, dedizierter Ansprechpartner und weitere Leistungen)					✓

**\*Bitte beachten:** Das MTR-Team kann bei Kunden von MTR Advanced auf XDR-Daten und -Funktionen zurückgreifen. MTR-Kunden sind in ihrer Sophos-Central-Konsole jedoch auf EDR-Funktionen beschränkt und müssen für XDR-Funktionen eine XDR-Lizenz erwerben.

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion  
unter [www.sophos.de/intercept-x](http://www.sophos.de/intercept-x)

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