



## Bedrohungslage

Die Bedrohung durch Cyberkriminalität wächst kontinuierlich. Erst kürzlich warnte BKA-Präsident Münch vor einer Zunahme von Cyberangriffen auf öffentliche Verwaltungen und Hochschulen.

## Maßnahmen zur Optimierung der Cybersicherheit

Zum Schutz sensibler Daten, zur Sicherung von Forschungsergebnissen und Immaterialgütern und letztlich zur Erhaltung unserer Arbeitsfähigkeit ergreift das ITS (IT-Servicezentrum der Universität Kassel) in Abstimmung mit der Hochschulleitung vielfältige Maßnahmen, um die Erfolgsaussicht potentieller Angreifer zu verringern. Dazu zählen u.a. die physische Absicherung wichtiger Server und Netzwerkkomponenten, die Netzwerksegmentierung, laufende Software- und System-Updates, regelmäßige Backups, Mailscanner, gut konfigurierte Firewalls, eine leistungsfähige Kombination aus IDS (Intrusion Detection System) und IPS (Intrusion Prevention System) ebenso wie das Angebot zentral gemanagter Endgeräte (UKCaaS – Uni Kassel Client as a Service).

## Virenschutz-Software

Von zentraler Bedeutung für die Sicherheit von Rechnern war und ist Antivirus-Software, die Endgeräte u.a. anhand laufend aktualisierter Signaturen bekannter Schad-Software und heuristischer Analysen vor dem (meist durch E-Mail-Anhänge oder Links auf manipulierte Websites bewerkstelligten) Befall mit Viren, Würmern, Trojanern o.ä. Bedrohungen schützen kann.

## Notwendigkeit eines umfassenderen Schutzes

Was für einen privaten Rechner schon einen guten Basischutz bieten mag, genügt jedoch für eine komplexe Organisation wie eine Hochschule längst nicht mehr. So dürfen nach den Vorgaben für den sog. „Grundschutz“ des BSI (Bundesamt für Sicherheit in der Informationstechnik), an denen sich auch die Informationssicherheitsleitlinie für die hessische Landesverwaltung orientiert, nur zentral administrierte, auf die Bedarfe der jeweiligen Institution zugeschnittenen Service- und Supportleistungen verwendet werden. Produkte für die reine Heimnutzung oder Produkte ohne Support sind dagegen im professionellen Wirkbetrieb explizit nicht einzusetzen (vgl. BSI, OPS.1.1.4 Schutz vor Schadprogrammen [Edition 2022]).

## Upgrade auf die aktuellen Versionen von Sophos

Auch die Hersteller von Antivirus-Software haben auf die neuen Herausforderungen reagiert. So forciert der bekannte Sicherheits-Software-Hersteller Sophos seine nunmehr auch vom ITS bereitgestellte Cloud-Anwendung Intercept X Advanced mit XDR (Extended Detection and Response), die sowohl

traditionelle als auch neuartige Bedrohungen für Computernetzwerke erkennt und bekämpft. Dagegen hat er die On-Premise Varianten seines bisherigen Virenschanners sowie der „Sophos Enterprise Console“ zum 20. Juli 2023 abgekündigt. Danach werden diese Produkte nicht mehr mit Updates durch den Hersteller versorgt. Die bestehenden Installationen von „Sophos Antivirus“ und der „Sophos Enterprise Console“ müssen daher bis spätestens zum 20. Juli 2023 durch die entsprechenden Nachfolgeprodukte ersetzt werden, um keine gefährliche Sicherheitslücke entstehen zu lassen.

## Änderungen im Betrieb von Sophos

Um den Anforderungen des BSI hinsichtlich des Schutzes vor Schadprogrammen zu genügen, setzt das ITS im Gleichklang mit den Rechenzentren der übrigen hessischen Universitäten bei zentral gemanagten Rechnern auf die langjährig bewährte Software von Sophos in ihrer neuesten Generation, die mit dem Ziel einer effizienten Einstellbarkeit unter Berücksichtigung der jeweiligen Sicherheitsanforderungen via Cloud über eine zentrale Konsole administriert wird.

Im Februar 2023 hat das ITS darüber informiert, dass aus dem notwendigen Wechsel auf die aktuellen Versionen von Sophos auch Änderungen im Betrieb resultieren werden. So verwalten die beteiligten Fachbereiche die Verteilung der vom ITS zur Verfügung gestellten Sicherheits-Software von Sophos nunmehr über ein eigenes Benutzerkonto (sog. „Tenant“) selbständig. Wenden Sie sich daher für die Installation der aktuellen Sophos-Variante auf einem nicht zentral gemanagten Rechner (unter Windows, Mac oder Linux) an den oder die Sophos-Admins Ihres Fachbereichs.

Die aktuelle Sophos-Lizenz erstreckt sich nicht auf privat genutzte Endgeräte und auch nicht mehr auf Endgeräte von Studierenden. Sophos-Installationen auf solchen Geräten verlieren ihre Schutzwirkung und müssen daher ggf. bis zum 20. Juli 2023 deinstalliert werden. Für einen einigermaßen adäquaten Schutz vor Viren sollte sodann durch die Installation oder Aktivierung aktueller Virenschutz-Software wie dem Microsoft Defender gesorgt werden.

## Neues Sicherheitsniveau

Mit Sophos Intercept X Advanced mit XDR erreicht die IT-Sicherheit für Endgeräte ein deutlich höheres Niveau. Während sich klassischer Virenschutz in erster Linie auf die Erkennung und Beseitigung von Viren und Malware konzentriert, wird mit der nunmehrigen EPPS (Endpoint-Protection-Software) ein breiterer und komplexerer Ansatz verfolgt. Er umfasst neben der Antivirenfunktionalität auch Deep-Learning-KI-gestützten Schutz vor „modernen“ Bedrohungsvarianten.

## Preis der Sicherheit

Freilich ist das deutlich erhöhte und angesichts der Bedrohungslage höchst willkommene Sicherheitsniveau nicht „kostenlos“ zu haben:

- So sind die Lizenzgebühren für EPPS deutlich höher als für klassischen Virenschutz.
- Auch im Betrieb verbraucht derartige Software mehr Ressourcen, was sich auf die Systemleistung auswirken und in einigen Fällen zur Verlangsamung oder Unterbrechung der Arbeit mit dem Endgerät führen kann.
- Wie jede Sicherheits-Software stuft EPPS in seltenen Fällen legitime Aktivitäten oder Programme außerhalb üblicher Büro-Anwendungen als schädlich ein („False Positives“) und blockiert diese, was zu vorübergehenden Störungen und Unannehmlichkeiten für die Nutzenden führen kann.
- Bisweilen kommt es zu Kompatibilitätsproblemen zwischen der EPPS und anderen Anwendungen oder Systemen, die im Netzwerk eingesetzt werden.
- Vor allem aber wird der Gewinn an Sicherheit durch einen Verlust an Freiheit erkaufte. Letzterer resultiert zunächst daraus, dass die einmal installierte EPPS von einem Endgerät nur wieder deinstalliert werden kann, wenn ein Sophos-Admin dies technisch freischaltet. Außerdem kann die EPPS potenziell gefährliche Aktivitäten blockieren und bei einem erkannten Angriff das davon betroffene Gerät vom Netz nehmen. Am schwersten wiegt aber, dass Sicherheits-Systeme wie EPPS zur Aufrechterhaltung des von ihnen gebotenen Sicherheitsniveaus u.a. aufgerufene Anwendungen, Websites und Datentransfers überwachen und über Geräte und Nutzende gesammelte Daten speichern müssen. Im Fall von Sophos geschieht dies (bis zu 90 Tage lang) zum überwiegenden Teil lokal auf dem Endgerät. Um die Wirksamkeit der EPPS zu erhöhen und u.a. Trainingsdaten für die KI zur Verfügung zu stellen, wird jedoch ein Teil der erhobenen Daten auch in einen „Data Lake“ in der Cloud übertragen (Details unter <https://www.sophos.com/de-de/legal/sophos-data-lake>). Admins mit entsprechenden Zugangsrechten haben über „Sophos Central“, das einheitliche Benutzer-Interface von Sophos, Zugriff auf diese Daten und können überdies „remote“ reagieren. Das rückt EPPS in die Nähe von Spyware, wobei der gravierende Unterschied darin besteht, dass Spyware den primären Zweck hat, Nutzende auszuspionieren, während EPPS, mit der ja hehre Ziele verfolgt werden, lediglich (aber immerhin) eine dahingehende Missbrauchsmöglichkeit eröffnet.

## Balance zwischen Sicherheit und Freiheit

Sophos Intercept X Advanced mit XDR bietet bis zu einem gewissen Grad die Möglichkeit, das Sicherheitsniveau und damit die Überwachung von Aktivitäten der zu schützenden Endgeräte und Nutzenden an rechtliche Rahmenbedingungen, konkrete Sicherheitsbedarfe und die jeweilige Unternehmenskultur anzupassen.

So werden sog. „Super-Admins“ am ITS aus der Sicht unserer Universität überbordende Sophos-Funktionalitäten zentral deaktivieren. Diesbezüglich ggf. künftig erforderliche Optimierungen wird das ITS mit dem Personalrat abstimmen.

Es gibt jedoch Funktionen, die von den „Tenants“ (den Sophos-Admins der Fachbereiche) entgegen der defaultmäßigen Deaktivierung wieder aktiviert werden und zu unlauteren Zwecken dienenden Überwachung von Aktivitäten auf Endgeräten missbraucht werden könnten. Dies lässt sich wegen der von Sophos gewählten Rechtsstruktur technisch nicht anders lösen.

Um einem potenziellen Missbrauch zumindest einen rechtlichen Riegel vorzuschieben, wird der Kanzler unserer Universität eine entsprechende Dienstanweisung erlassen, die es Admins (von den „Super-Admins“ am ITS bis zu den Sophos-Admins der Fachbereiche, die auf einer internen Website des ITS eingesehen werden können) untersagt, defaultmäßig abgeschaltete Funktionen zu aktivieren sowie und vor allem durch aktivierte Funktionen gegebenen Möglichkeiten für Überwachungszwecke zu missbrauchen oder im Zuge der Administration der EPPS wahrgenommene Informationen Dritten zu offenbaren. Ein Verstoß gegen eine Dienstanweisung kann gravierende arbeitsrechtliche Folgen haben, die – je nach Schwere des Verstoßes – bis hin zur verhaltensbedingten Kündigung reichen.

Einen Überblick über die Funktionen von Sophos Central - Intercept X Advanced mit XDR bietet eine vom ITS bearbeitete und hier als Anhang 1 angefügte Tabelle. (Eine Erläuterung der in Anhang 1 nur schlagwortartig bezeichneten Funktionsgruppen findet sich in Anhang 2.) Aus den Spalten lassen sich die Funktionen wie folgt ablesen:

- Herstellerseits vorgesehene Funktionen (die grundsätzliche „Mächtigkeit“ der Software) sowie davon auf Basis unserer Lizenz verfügbare Funktionen;
- Jene eingeschränkte Menge an Funktionen, deren Nutzung vom ITS vorgeschlagen wird;
- Vom ITS technisch in einer Weise gesperrte Funktionen, welche die Nutzung durch einen dezentralen Admin zuverlässig unterbindet;
- Jene Funktionen, die vom ITS zwar defaultmäßig deaktiviert werden, von einem dezentralen Admin aber wieder aktiviert werden könnten, der dies allerdings wegen einer entsprechenden Dienstanweisung nicht darf.

Die Prüfung der datenschutzrechtlichen Zulässigkeit des Einsatzes von Sophos Intercept X Advanced mit XDR wurde von der Datenschutzbeauftragten bereits mit positivem Ergebnis vorgenommen.

Auf dieser Grundlage werden zwischen dem Personalrat und der Dienststellenleitung unserer Universität zunächst eine Regelungsabrede und in der Folge eine Dienstvereinbarung getroffen, welche die Bedingungen für den zulässigen Einsatz von Sophos Intercept X Advanced mit XDR festlegt.

## Haftung für den Einsatz nicht oder nicht ausreichend geschützter Endgeräte

Die Frage nach der Haftung für Schäden, die auf den Einsatz nicht oder nicht ausreichend geschützter Endgeräte zurückzuführen sind, ist nicht einfach zu beantworten. Grundsätzlich hat es die Dienststelle (ggf. auf Basis einer Dienstvereinbarung) in der Hand, den Einsatz privater Rechner entweder zu verbieten oder nur für den Fall der Einhaltung von Richtlinien zur entsprechenden Konfiguration von Sicherheitsmaßnahmen (z.B. einer Nutzungsvereinbarung für „Bring Your Own Device“ – BOYD) zuzulassen. Ebenso wäre es möglich, die private Nutzung von

Dienstgeräten zu untersagen. Und schließlich könnte für die Nutzung von Dienstgeräten der Einsatz bestimmter Sicherheitsmaßnahmen vorgeschrieben werden. Wegen der Möglichkeit, Sicherheitsmaßnahmen zur Überwachung der Mitarbeitenden einzusetzen, wäre auch hierfür eine entsprechende Dienstvereinbarung erforderlich. Diese gibt es an unserer Universität bislang nicht.

Solange aber diesbezüglich keine strikten Regeln existieren, ist die Gefahr einer persönlichen Haftung von Mitarbeitenden eher gering: Im Innenverhältnis haften Beschäftigte des öffentlichen Dienstes nämlich nur für Vorsatz und grobe Fahrlässigkeit. Diese Haftungsbeschränkung gilt kraft Gesetzes (§ 48 BeamStG) für Beamte. Für tariflich Beschäftigte verweisen die tarifvertraglichen Vorschriften (§ 7 Abs. 3 TV-H) auf die beamtenrechtlichen Regelungen. Allerdings ist nicht auszuschließen, dass der Verzicht auf jegliche Sicherheitsmaßnahmen auf einem im Netzwerk der Universität verwendeten Endgerät als grobe Fahrlässigkeit beurteilt würde.

### **Grundlagen für Ihre Entscheidung für oder gegen den Einsatz von Sophos Intercept X Advanced mit XDR**

Die beschriebene Regelungsabrede und in der Folge die Dienstvereinbarung des Personalrats mit der Dienststellenleitung unserer Universität eröffnen die Möglichkeit, Sophos Intercept X Advanced mit XDR auch auf nicht zentral gemanagten dienstlichen Endgeräten einzusetzen, verpflichtet jedoch nicht dazu.

Dies bedeutet, dass alle Mitarbeitenden die Entscheidung treffen können und müssen, ob sie im eigenen Interesse und in jenem der gesamten Universität für aus heutiger Sicht optimale Endgerätesicherheit durch den Einsatz der aktuellen Sophos-Produkte oder – im Rahmen ihrer Dienst- und Sorgfaltspflichten – lieber durch die Verwendung anderer geeigneter Produkte für einen hinlänglichen Schutz vor Schad-Software sorgen wollen.

Dabei können sie sich u.a. von Überlegungen wie den folgenden leiten lassen:

- Als wesentliche Maßnahme eines umfassenden ISMS (Informationssicherheitsmanagementsystem) strebt unsere Universität eine weitere Verbesserung der Informationssicherheit auf der Grundlage des BSI-Grundschutzes an. Dafür wird künftig die Nutzung von Schutz-Software für den Enterprise-Bereich (wie Sophos Intercept X Advanced mit XDR) ohnehin unumgänglich sein.
- Bei der Nutzung digitaler Dienste sind wir alle längst darauf angewiesen, Admins an der Universität (und darüber hinaus) zu vertrauen. Was die potenzielle missbräuchliche Überwachung von Kolleginnen und Kollegen unter Nutzung der von der EPPS gesammelten Daten anbelangt, erhält dieses Vertrauen durch die Regelungsabrede bzw. die Dienstvereinbarung und die Dienstanweisung eine zusätzliche Basis.
- Bitte bedenken Sie bei Ihrer Entscheidung, dass Sicherheit in allen Bereich vor allem von informierter Eigenverantwortung abhängt. Bedrohungsbilder aber auch Einsichten verändern sich im Laufe der Zeit. So gingen der Verpflichtung, beim Autofahren einen Sicherheitsgurt und beim Motorradfahren einen Helm zu tragen, jeweils langjährige Diskussionen voraus. Möglicherweise wird es künftig an unserer Universität die Verpflichtung zur Verwendung eines leistungsfähigen Schutzes vor Schad-Software geben.
- Noch können Sie aber (wenn Sie keinen zentral gemanagten Rechner verwenden) unter informierter Abwägung der Pro- und Contra-Argumente entscheiden, ob Sie Sophos Intercept X Advanced mit XDR einsetzen oder sich lieber auf eine „klassische“ Software zum Schutz vor Schad-Software verlassen wollen. Denken Sie dabei bitte auch an das Ziel, die gesamte Universität in optimaler Weise vor erfolgreichen Cyberangriffen zu bewahren.

Sollten Sie vor Ihrer Entscheidung noch Fragen haben, wenden Sie sich damit bitte zunächst an die oder den Sophos-Admin Ihres Fachbereichs, die oder der bei Bedarf weitere Informationen beim ITS anfordern wird.

# Anhang 1

## Vorläufiger Nutzungsvorschlag für Sophos Central - Intercept X Advanced with XDR an der Universität Kassel

11.07.2023

Als "Sophos Central" wird das einheitliche Benutzer-Interface von Sophos bezeichnet. Darüber haben wir Zugang zu unserem erworbenen Sophos-Produkt "Intercept X Advanced with XDR". Dabei handelt es sich um eine neue Generation der herkömmlichen "AntiViren-Software", für die oft auch die Bezeichnung "EndPointProtection" verwendet wird.

XDR steht dabei für "eXtended Detection and Response" - dieser Namenszusatz gibt etwas Aufschluss über die Funktionen der neuen Generation: **Erweiterte Erkennung und Reaktion**.

Nähere Informationen zu den Grundfunktionen des XDR: <https://doc.sophos.com/central/customer/help/de-de/ManageYourProducts/XDR/index.html>

Features	Gegenwärtig an der UKS zur Verfügung stehender Funktionsumfang	Davon zur Nutzung an der UKS aktuell vom ITS vorgeschlagen	Vom ITS technisch zentral gesperrt	Zentral untersagt und vom ITS als Default gesetzt
<b>ANGRIFFSFLÄCHE</b>				
Web Security	✓	✓		
Download Reputation	✓	✓		
Web Control/Kategoriebasierte URL-Filterung	✓			✗
Peripheriekontrolle	✓			✗
Application Control	✓			✗
<b>VOR AUSFÜHRUNG AUF DEM GERÄT</b>				
Deep-Learning-Malware-Erkennung	✓	✓		
Anti-Malware-Dateiscans	✓	✓		
Live Protection	✓	✓		
Verhaltensanalysen vor Ausführung (HIPS)	✓	✓		
Blockierung potenziell unerwünschter Anwendungen (PUAs)	✓	✓		
Intrusion Prevention System	✓	✓		
<b>STOPPEN VON BEDROHUNGEN BEI AUSFÜHRUNG</b>				
Data Loss Prevention	✓			✗
Laufzeit-Verhaltensanalyse (HIPS)	✓	✓		

Antimalware Scan Interface (AMSI)	✓	✓		
Malicious Traffic Detection (MTD)	✓	✓		
Exploit Prevention	✓	✓		
Active Adversary Mitigations	✓	✓		
Ransomware File Protection (CryptoGuard)	✓	✓		
Disk and Boot Record Protection (WipeGuard)	✓	✓		
Man-in-the-Browser Protection (Safe Browsing)	✓			✗
Enhanced Application Lockdown	✓			✗
<b>ERKENNUNG</b>				
Live Discover (umgebungsübergreifende SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben)	✓		✗	
SQL-Abfragen-Library (vorformulierte, individuell anpassbare Abfragen) Erkennung und Priorisierung verdächtiger Ereignisse	✓		✗	
Erkennung verdächtiger Ereignisse und Priorisierung	✓	✓		
Datenspeicherung auf Festplatte (bis zu 90 Tage) mit schnellem Datenzugriff	✓			✗
Produktübergreifende Datenquellen – z. B. Firewall, E-Mail (Sophos XDR)	✓	✓		
Produktübergreifende Abfragen (Sophos XDR)	✓	✓		
Sophos Data Lake Cloud-Speicher	✓ 30 Tage	✓ 30 Tage		
Geplante Abfragen	✓			✗
<b>ANALYSE</b>				
Bedrohungsfälle (Ursachenanalyse)	✓	✓		
Deep Learning-Malware-Analyse	✓	✓		
Erweiterte Bedrohungsdaten von Sophos X-Ops auf Abruf	✓		✗	
Export forensischer Daten	✓	✓		
<b>BEREINIGUNG</b>				

Automatisierte Malware-Entfernung	✓	✓		
Synchronized Security Heartbeat	✓	✓		
Sophos Clean	✓	✓		
Live Response (Remote-Analyse und -Reaktion)	✓		✗	
On-Demand-Endpoint-Isolation	✓	✓		
Mit einem Klick „Entfernen und blockieren“	✓	✓		
<b>THREAT HUNTING und REAKTION DURCH EXPERTEN</b>				
24/7 indizienbasiertes Threat Hunting	✗			
Security Health Checks	✗			
Datenspeicherung	✗			
Aktivitätsreports	✗			
Angriffserkennung	✗			
Beseitigung von Bedrohungen und ihren Folgen	✗			
Umfassende Reaktion auf Vorfälle: Bedrohungen werden vollständig eliminiert	✗			
Erfordert vollständigen Sophos XDR Agent (Schutz, Erkennung und Reaktion)				
Ursachenanalyse: um ein erneutes Auftreten in Zukunft zu verhindern	✗			
Dedizierter Ansprechpartner	✗			
<b>ZERO TRUST NETWORK ACCESS</b>				
Integrierter ZTNA-Agent	✗			
ZTNA-Zugriffsrichtlinien und -Kontrollen	✗			

**Quellen**

<https://www.sophos.com/de-de/products/endpoint-antivirus/tech-specs>

<https://doc.sophos.com/central/customer/help/de-de/ManageYourProducts/XDR/index.html>

# Anhang 2

## Gruppierung der Funktionsübersicht und Erklärung

Als "**Sophos Central**" wird das einheitliche Benutzer-Interface von Sophos bezeichnet. Darüber haben wir den Zugang zu unserem eigentlich erworbenen und genutzten Sophos Produkt "**Intercept X Advanced with XDR**". Dabei handelt es sich um eine neue Generation der herkömmlichen "AntiViren-Software". In dem Zusammenhang wird oft auch die Bezeichnung "EndPointProtection" verwendet, was ebenfalls eine generelle Vereinheitlichung der "AntiViren-Software" der neuen Generation darstellt.

XDR steht dabei für "eXtended Detection and Response" - dieser Namenszusatz gibt den wesentlichen Aufschluss über die Funktionen der neuen Generation. Nämlich: **erweiterte Erkennung und Reaktion**.

Nähere Informationen zu den Grundfunktionen des XDR: <https://doc.sophos.com/central/customer/help/de-de/ManageYourProducts/XDR/index.html>

## Vollständige Funktionsumfang (nach Angaben des Herstellers)

<b>Funktion:</b>	<b>Funktionsgruppe:</b>
<b>ANGRIFFSFLÄCHE</b>	
Web Security	Web Control
Download Reputation	Web Control
Web Control/Kategoriebasierte URL-Filterung	Web Control
Peripheriekontrolle	Peripheral Control
Application Control	Application Control
<b>VOR AUSFÜHRUNG AUF DEM GERÄT</b>	
Deep-Learning-Malware-Erkennung	Threat Protection
Anti-Malware-Dateiscans	Threat Protection
Live Protection	Threat Protection
Verhaltensanalysen vor Ausführung (HIPS)	Threat Protection
Blockierung potenziell unerwünschter Anwendungen (PUAs)	Threat Protection
Intrusion Prevention System	Threat Protection
<b>STOPPEN VON BEDROHUNGEN BEI AUSFÜHRUNG</b>	
Data Loss Prevention	Data Loss Prevention
Laufzeit-Verhaltensanalyse (HIPS)	Threat Protection
Antimalware Scan Interface (AMSI)	Threat Protection
Malicious Traffic Detection (MTD)	Threat Protection
Exploit Prevention	Threat Protection
Active Adversary Mitigations	Threat Protection

Ransomware File Protection (CryptoGuard)	Threat Protection
Disk and Boot Record Protection (WipeGuard)	Threat Protection
Man-in-the-Browser Protection (Safe Browsing)	Web Control
Enhanced Application Lockdown	Application Control
<b>ERKENNUNG</b>	
Live Discover (umgebungsübergreifende SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben)	Sophos Central Konsole
SQL-Abfragen-Library (vorformulierte, individuell anpassbare Abfragen) Erkennung und Priorisierung verdächtiger Ereignisse	Sophos Central Konsole
Erkennung verdächtiger Ereignisse und Priorisierung	Threat Protection
Datenspeicherung auf Festplatte (bis zu 90 Tage) mit schnellem Datenzugriff	Sophos Central Core
Produktübergreifende Datenquellen – z. B. Firewall, E-Mail (Sophos XDR)	Sophos Central Konsole
Produktübergreifende Abfragen (Sophos XDR)	Sophos Central Konsole
Sophos Data Lake Cloud-Speicher	Sophos Central Konsole
Geplante Abfragen	Sophos Central Konsole
<b>ANALYSE</b>	
Bedrohungsfälle (Ursachenanalyse)	Threat Protection
Deep Learning-Malware-Analyse	Threat Protection
Erweiterte Bedrohungsdaten von Sophos X-Ops auf Abruf	Sophos Central Konsole
Export forensischer Daten	Sophos Central Konsole
<b>BEREINIGUNG</b>	
Automatisierte Malware-Entfernung	Threat Protection
Synchronized Security Heartbeat	Sophos Central Core
Sophos Clean	Threat Protection
Live Response (Remote-Analyse und -Reaktion)	Sophos Central Konsole
On-Demand-Endpoint-Isolation	Sophos Central Core
Mit einem Klick „Entfernen und blockieren“	Sophos Central Konsole

Funktionsgruppe:	Beschreibung:
Web Control	Diese Funktion kann verwendet werden, um bestimmte Webseiten und/ oder Downloads zu sperren. Dabei bietet Sophos Kategorien an, die gesperrt werden können, zum Beispiel „Criminal Activity“, „Hacking“, „Illegal Drugs“. Es ist zudem möglich, eine eigene allow / deny-Liste zu führen, um gesperrte Webseiten dann wieder freizuschalten. Wenn ein:e Nutzer:in versucht, eine gesperrte Webseite aufzurufen wird dies an Sophos Central gemeldet. Die Web Control Funktion kann als Ergänzung zu der Threat Protection sehr nützlich sein, da man schädliche Daten schon abfangen kann, bevor diese überhaupt auf dem Gerät landen.
Peripheral Control	Mit dieser Funktion kann gesteuert werden, wie ein Rechner mit Peripherie (externen Speichermedien, Bluetooth, Wireless, etc.) umgeht. Dabei kann man entscheiden, ob man nur überwachen möchte, welche Peripherie an einen Rechner angesteckt wird, oder ob man diese auch nur auf bestimmte Peripherie einschränken möchte, die erlaubt wird.
Application Control	Diese Funktion kann verwendet werden, um das Ausführen von Programmen einzuschränken. Wenn ein:e Nutzer:in versucht, ein blockiertes Programm zu starten, wird dies verhindert und eine Information darüber an Sophos Central gemeldet.
Threat Protection	Diese Funktion überwacht den Rechner auf schädliche oder verdächtige Daten oder Software. Sollte etwas Problematisches gefunden werden, wird diese Information an Sophos Central gemeldet und die betroffene Datei gelöscht.
Data Loss Prevention	Mit dieser Funktion kann gesteuert werden, wie mit bestimmten Daten umgegangen wird. Sophos kann so zum Beispiel überprüfen, ob in einer Datei sensible Daten von Personen sind, oder ob Bank Account Informationen zu finden sind. Wenn der:ie Nutzer:in dann versucht, diese Datei von dem Rechner zu einer externen Quelle zu übertragen, kann er entweder noch mal aufgefordert werden, dies erneut zu bestätigen oder der Vorgang kann geblockt werden. Dieser Versuch wird ebenfalls zu Sophos Central gemeldet.
Sophos Central Konsole	Die Sophos Central Konsole ist der zentrale Punkt, an dem alle Informationen zusammenlaufen. Dort haben Administrator:innen die Möglichkeit, die Instanz zu verwalten, Geräte zu verwalten und Informationen zu erhalten über potenzielle Bedrohungen.
Sophos Central Core	Dieser Part ist der Kern der Sophos Central Software, die auf dem Endgerät installiert wird. Sie kümmert sich um die Kommunikation mit der Sophos Central Konsole. Sie ist ebenfalls dafür zuständig, Nutzer:innen über die Anwendung oder über Benachrichtigungen aufmerksam zu machen, wenn es ein Problem geben sollte.

### Quellen

<https://www.sophos.com/de-de/products/endpoint-antivirus/tech-specs>

<https://doc.sophos.com/central/customer/help/de-de/ManageYourProducts/XDR/index.html>