

**Dienstanweisung**  
**für die Administration von Sophos Central Intercept X Advanced XDR**  
**an der Universität Kassel**

Der Software-Hersteller Sophos Ltd. hat die On-Premise Varianten seines bisherigen Virenscanners sowie der „Sophos Enterprise Console“ zum 20. Juli 2023 abgekündigt. An deren Stelle sollen auch an der Universität Kassel die entsprechenden Nachfolgeprodukte treten. Sophos Central Intercept X Advanced XDR ist eine sog. „Endpoint-Protection-Software“. „Sophos Central“ bezeichnet dabei das einheitliche Benutzer-Interface von Sophos, und „XDR“ steht für „eXtended Detection and Response“ (Erweiterte Erkennung und Reaktion).

Diese Dienstanweisung ist eine verbindliche Handlungsanweisung für all diejenigen Beschäftigten der Universität Kassel, denen IT-Administrationsrechte für Sophos Central Intercept X Advanced XDR im IT-Servicezentrum oder in den Fachbereichen und zentralen Einrichtungen zugeordnet sind (Sophos-Admins). Sie soll zur Wahrung der Persönlichkeitsrechte derjenigen Beschäftigten beitragen, die Sophos XDR – im eigenen Interesse aber auch mit dem Ziel, die gesamte Universität möglichst vor erfolgreichen Cyberangriffen zu bewahren – auf einem Endgerät einsetzen.

Die Nutzung der einzelnen Funktionen von Sophos XDR erfolgt auf Basis der als Anlage 1 beigefügten Übersicht. Die im Rahmen der Startphase (beginnend ab dem 20.07.2023) genutzten Funktionalitäten sind kenntlich gemacht. Die nicht genutzten Funktionalitäten werden entweder technisch zentral gesperrt oder vom IT-Servicezentrum mit dem Standardwert (Default) „Nein“ belegt. Ein Einschalten solcher Funktionalitäten ist untersagt.

Auf einem dezentral administrierten Endgerät darf Sophos XDR nur auf der Grundlage einer Einwilligung der/des Nutzer:in installiert werden.

Ggf. in der Testphase zugeordnete Berechtigungen, die über den in Anlage 1 definierten zulässigen Umfang hinausgehen, sind entsprechend zu beschränken.

Im Rahmen der Administration von Sophos Central Intercept X Advanced XDR bekanntwerdende personenbezogene Daten oder Nutzungsinformationen dürfen nicht zur Überwachung von Bediensteten verwendet, verwendet oder weitergegeben werden. Administratoren dürfen Auskünfte ausschließlich den Nutzer:innen des jeweiligen Endgeräts geben.

Diese Dienstanweisung gilt analog für den Einsatz von Antiviren-Software bzw. End-Point-Protection-Lösungen, die vergleichbare Funktionen beinhalten.

Kassel, den 18.07.2023

Die Präsidentin

In Vertretung

Gez. im Original  
Dr. Oliver Fromm

Kanzler

# 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>