Sophos Workload Protection Lizenz-Guide

SOPHOS
Cybersecurity delivered.

Übersicht über Intercept X for Server, XDR, Cloud Native Security und MTR

Verwaltung über Sophos Central

Funktionen	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud-native Sicherheit	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Verwaltung						
Mehrere Richtlinien		✓	✓	✓	✓	✓
Gesteuerte Updates		✓	✓	✓	✓	✓
Reduzierung der Angriffsfläche						
Application Control		✓	✓	✓	✓	✓
Peripheral Control		✓	✓	✓	✓	✓
Web Control/Kategoriebasierte URL-Blockierung		✓	✓	✓	✓	✓
Application Whitelisting (Server Lockdown)		✓	✓	✓	✓	✓
Download Reputation	✓	✓	✓	✓	✓	✓
Web Security	✓	✓	✓	✓	✓	✓
Vor Ausführung auf einem Gerät						
Deep-Learning-Malware-Erkennung	✓	✓	✓	✓	✓	✓
Anti-Malware-Dateiscans	✓	✓	✓	✓	✓	✓
Live Protection	✓	✓	✓	✓	✓	✓
Verhaltensanalysen vor Ausführung (HIPS)	✓	✓	✓	✓	✓	✓
Blockierung pot. unerwünschter Anwendungen (PUAs)	✓	✓	✓	✓	✓	✓
Intrusion Prevention System (IPS)	✓	✓	✓	✓	✓	✓
Stoppen von Bedrohungen bei Ausführung						
Data Loss Prevention		✓	✓	✓	✓	✓
Laufzeit-Verhaltensanalyse (HIPS)	✓	✓	✓	✓	✓	✓
Antimalware Scan Interface (AMSI)	✓	✓	✓	✓	✓	✓

Funktionen	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud-native Sicherheit	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Malicious Traffic Detection (MTD)	✓	✓	✓	✓	✓	✓
Exploit Prevention (Details auf Seite 5)	✓	✓	✓	✓	✓	✓
Active Adversary Mitigations (Details auf Seite 5)	✓	✓	✓	✓	✓	✓
Ransomware File Protection (CryptoGuard)	✓	✓	✓	✓	✓	✓
Disk and Boot Record Protection (WipeGuard)	✓	✓	✓	✓	✓	✓
Man-in-the-Browser Protection (Safe Browsing)	✓	✓	✓	✓	✓	✓
Enhanced Application Lockdown	✓	✓	✓	✓	✓	✓
Erkennung						
Live Discover (umgebungsübergreifende SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben)			✓	✓	✓	✓
SQL-Abfragen-Library (vorformulierte, individuell anpassbare Abfragen)			✓	✓	✓	✓
Datenspeicherung auf Festplatte (bis zu 90 Tage) mit schnellem Datenzugriff			✓	✓	✓	✓
Produktübergreifende Datenquellen (z. B. Firewall, E-Mail)			✓	✓	✓	✓
Liste mit nach Priorität geordneten Erkennungen			✓	✓	✓	✓
Sophos Data Lake (Cloud-Datenspeicher)			30 Tage	30 Tage	30 Tage	30 Tage
Geplante Abfragen			✓	✓	✓	✓
Laufzeitbasierte Container-Transparenz und -Erkennungen			✓	✓	✓	✓
Analyse						
Bedrohungsfälle (Ursachenanalyse)		✓	✓	✓	✓	✓
Deep Learning-Malware-Analyse			✓	✓	✓	✓
Erweiterte Bedrohungsdaten aus den SophosLabs auf Abruf			✓	✓	✓	✓
Export forensischer Daten			✓	✓	✓	✓
KI-gesteuerte Analysen			✓	✓	✓	✓

Funktionen	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud-native Sicherheit	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Bereinigung						
Automatisierte Malware-Entfernung	✓	✓	✓	✓	✓	✓
Synchronized Security Heartbeat	✓	✓	✓	✓	✓	✓
Sophos Clean	✓	✓	✓	✓	✓	✓
Live Response (Remote-Terminal-Zugriff für weitere Analysen und Reaktionsmaßnahmen)			✓	✓	✓	✓
On-Demand-Server-Isolation			✓	✓	✓	✓
Mit einem Klick „Entfernen und blockieren“			✓	✓	✓	✓
Laufzeitbasierte Container-Transparenz und -Erkennungen			✓	✓	✓	✓
Zugriff/Berechtigung						
Synchronized Application Control (Transparenz über Anwendungen)	✓	✓	✓	✓	✓	✓
Update Cache und Message Relay	✓	✓	✓	✓	✓	✓
Automatische Scan-Ausnahmen	✓	✓	✓	✓	✓	✓
File Integrity Monitoring			✓	✓	✓	✓
Cloud-Umgebungen						
Überwachung von Cloud-Umgebungen: AWS, Azure, GCP, Kubernetes, IaC und Docker Hub Registries		1 je Anbieter	1 je Anbieter	Unbegrenzt	1 je Anbieter	1 je Anbieter
Security Monitoring (CSPM-Best-Practice-Richtlinien)		Tägliche Scans	Tägliche Scans	Geplante, tägliche und On-Demand-Scans	Tägliche Scans	Tägliche Scans
Asset Inventory		✓	✓	✓	✓	✓
Erweiterte Suchfunktionen		✓	✓	✓	✓	✓
KI-basierte Erkennung von Anomalien		✓	✓	✓	✓	✓
Warnmeldungen zu schädlichem Datenverkehr von SophosLabs Intelix		✓	✓	✓	✓	✓
E-Mail-Warnhinweise		✓	✓	✓	✓	✓
AWS-native Service-Integrationen (Amazon GuardDuty, AWS Security Hub, Amazon Inspector usw.)		✓	✓	✓	✓	✓
Azure-native Service-Integrationen (Azure Sentinel und Advisor)		✓	✓	✓	✓	✓
Cloud Workload Protection: Agent-Erkennung (Sophos Intercept X Server)		✓	✓	✓	✓	✓
Cloud Workload Protection: Automatische Agent-Entfernung (Sophos Intercept X Server)		✓	✓	✓	✓	✓

Funktionen	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud-native Sicherheit	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Compliance-Richtlinien und Reporting		CIS-Bewertungsrichtlinien	CIS-Bewertungsrichtlinien	CIS-Bewertungsrichtlinien, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2, Sophos Best Practices	CIS-Bewertungsrichtlinien	CIS-Bewertungsrichtlinien
Benutzerdefinierte Richtlinien				✓		
Netzwerkvisualisierung		✓	✓	✓	✓	✓
IAM-Visualisierung		✓	✓	✓	✓	✓
Spend Monitor		✓	✓	✓	✓	✓
Integriertes Alert-Management (Jira, ServiceNow, Slack, Teams, PagerDuty, Amazon SNS)		✓	✓	✓	✓	✓
SIEM-Integrationen (Splunk, Azure Sentinel)		✓	✓	✓	✓	✓
Rest API		✓	✓	✓	✓	✓
Infrastructure-as-Code-Scanvorlagen		✓	✓	✓	✓	✓
Umgebungs-Zugriffskontrolle		✓	✓	✓	✓	✓
Container-Image-Scans (ECR, ACR, Docker Hub, API)		✓	✓	✓	✓	✓
Managed Service						
24/7 indizienbasiertes Threat Hunting					✓	✓
Security Health Checks					✓	✓
Datenspeicherung					✓	✓
Aktivitätsreports					✓	✓
Angriffserkennung					✓	✓
Beseitigung von Bedrohungen und Bereinigung					✓	✓
24/7 indizienloses Threat Hunting						✓
Threat Response Team Lead						✓
Direkter Telefon-Support						✓
Proaktives Security Posture Management						✓
Ransomware File Protection (CryptoGuard)						✓