Intercept X for Server Licensing Overview

Managed by Sophos Central

SOPHOS

Software-Express

Ihr Ansprechpartner:
Simon Klein
simon.klein@software-express.de

https://www.software-express.de

	Features	Central Server Protection (SVRC)	Intercept X Advanced for Server (SVRCIXA)	Intercept X Advanced for Server with EDR (SVRCIXAEDR)
ATTACK SURFACE REDUCTION	Application Whitelisting (Server Lockdown)		✓	✓
	Web Security	✓	✓	✓
	Download Reputation	✓	✓	✓
	Web Control/Category-based URL Blocking	✓	✓	✓
	Peripheral Control (e.g. USB)	✓	✓	✓
	Application Control	✓	✓	✓
BEFORE IT RUNS ON DEVICE	Deep Learning Malware Detection		✓	✓
	Anti-Malware File Scanning	✓	✓	✓
	Live Protection	✓	✓	✓
	Pre-execution Behavior Analysis (HIPS)	✓	✓	✓
	Potentially Unwanted Application (PUA) Blocking	✓	✓	✓
STOP RUNNING THREAT	Data Loss Prevention	✓	✓	✓
	Exploit Prevention		✓	✓
	Runtime Behavior Analysis (HIPS)	✓	✓	✓
	Malicious Traffic Detection (MTD)	✓	✓	✓
	Active Adversary Mitigations		✓	✓
	Ransomware File Protection (CryptoGuard)		✓	✓
	Disk and Boot Record Protection (WipeGuard)		✓	✓
	Man-in-the-Browser Protection (Safe Browsing)		✓	✓
	Enhanced Application Lockdown		✓	✓
DETECT	Cross Estate Threat Searching			✓
	Threat Indicators and Prioritization (coming in 2019)			✓
INVESTIGATE	Threat Cases		✓	✓
	Deep Learning Malware Analysis			✓
	Advanced On-demand SophosLabs Threat Intelligence			✓
	Forensic Data Export			✓

Intercept X for Server Licensing Overview

Managed by Sophos Central

Ihr Ansprechpartner:
Simon Klein
simon.klein@software-express.de

https://www.software-express.de

	Features	Central Server Protection (SVRC)	Intercept X Advanced for Server (SVRCIXA)	Intercept X Advanced for Server with EDR (SVRCIXAEDR)
REMEDIATE	Automated Malware Removal	✓	✓	✓
	Synchronized Security Heartbeat	✓	✓	✓
	Sophos Clean		✓	✓
	On-demand Server Isolation			✓
	Single-click "Clean and Block"			✓
VISIBILITY	Cloud Workload Discovery and Protection (AWS EC2/S3, Azure)	✓	✓	✓
	Cloud Workload Protection (Google Cloud Platform)[1]	✓	✓	✓
	AWS Map, Multi-region Visualization	✓	✓	✓
	Synchronized App Control	✓	✓	✓
CONTROL	Server-specific Policy Management	✓	✓	✓
	Update Cache and Message Relay	✓	✓	✓
	Automatic Scanning Exclusions	✓	✓	✓
	File Integrity Monitoring	✓	✓	✓

[1]For Public Cloud support see the Knowledge Base Article: https://community.sophos.com/kb/en-us/132540

Intercept X For Server Features

Details of specific features included in Intercept X for Server

SOPHOS

Features	
Enforce Data Execution Prevention	✓
Mandatory Address Space Layout Randomization	✓
Bottom-up ASLR	✓
Null Page (Null Deference Protection)	✓
Heap Spray Allocation	✓
Dynamic Heap Spray	✓
Stack Pivot	✓
Stack Exec (MemProt)	✓
Stack-based ROP Mitigations (Caller)	✓
Branch-based ROP Mitigations (Hardware Assisted)	✓
Structured Exception Handler Overwrite (SEHOP)	✓
Import Address Table Filtering (IAF)	✓
Load Library	✓
Reflective DLL Injection	✓
Shellcode	✓
VBScript God Mode	✓
Wow64	✓
Syscall	✓
Hollow Process	✓
DLL Hijacking	✓
Squiblydoo Applocker Bypass	✓
APC Protection (Double Pulsar / AtomBombing)	✓
Process Privilege Escalation	✓

(Left table grouped under: **EXPLOIT PREVENTION**)

	Feature	
ACTIVE ADVERSARY MITIGATIONS	Credential Theft Protection	✓
	Code Cave Mitigation	✓
	Man-in-the-Browser Protection (Safe Browsing)	✓
	Malicious Traffic Detection	✓
	Meterpreter Shell Detection	✓
ANTI-RANSOMWARE	Ransomware File Protection (CryptoGuard)	✓
	Automatic File Recovery (CryptoGuard)	✓
	Disk and Boot Record Protection (WipeGuard)	✓
APPLICATION LOCKDOWN	Web Browsers (including HTA)	✓
	Web Browser Plugins	✓
	Java	✓
	Media Applications	✓
	Office Applications	✓
DEEP LEARNING PROTECTION	Deep Learning Malware Detection	✓
	Deep Learning Potentially Unwanted Applications (PUA) Blocking	✓
	False Positive Suppression	✓
RESPOND INVESTIGATE REMOVE	Threat Indicators	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓

Software Express

Ihr Ansprechpartner:
Simon Klein
simon.klein@software-express.de

https://www.software-express.de