CLOUD READY

Intercept X for Server

Warum müssen Sie Ihre Server schützen?

Elevator Pitch

Intercept X for Server

- schützt unternehmenskritische Server und die darauf befindlichen Anwendungen und Daten
- schützt Anwendungen und Daten lokal und in der Cloud, sowohl auf VMs als auch auf physischen Servern
- bietet umfassenden Schutz speziell für Server – durch eine Kombination aus signaturloser Exploit Prevention und Anti-Hacker-Funktionen, Malware-Erkennung mit Deep Learning und Anti-Ransomware-Technologie
- bietet einzigartigen Schutz vor bekannten und unbekannten Bedrohungen

52 % aller Datenpannen gehen von Servern aus*

2x höhere Wahrscheinlichkeit für Datenpannen bei Servern als bei Endgeräten*

39 % aller Malware ist Ransomware*

* Verizon Data Breach Report, 2018

Neues Produktportfolio im Bereich Server Protection

	Central Server Protection (SVRC) (ehemals Central Server Standard)	Intercept X Advanced for Server (SVRCIXA) (ehemals Central Server Advanced)
AV-Signaturen / HIPS / Live Protection	✓	✓
Automatische Scan-Ausnahmen**	✓	✓
Workload-Erkennung in der Cloud**	✓	✓
Peripheriekontrolle	✓ NEU	✓
Web Control	✓ NEU	✓
Application Control	✓ NEU	✓
Data Loss Prevention (DLP)	✓ NEU	✓
Malicious Traffic Detection (MTD)	✓ NEU	✓
Synchronized Security Heartbeat	✓ NEU	✓
Server Lockdown (Application Whitelisting)**		✓
CryptoGuard**		✓
WipeGuard**		✓ NEU
Active Adversary Mitigation**		✓ NEU
Exploit-Schutz**		✓ NEU
Ursachenanalyse**		✓ NEU
Deep Learning		✓ NEU

** Serverspezifisch oder von entscheidender Bedeutung für den Schutz von Servern

Schutz unternehmenskritischer Server und der darauf befindlichen Anwendungen und Daten

Kundenbedenken:	Antworten auf die Bedenken:
Preis – Kunden möchten Server nur so schützen wie einen Endpoint	Signaturbasierte Sicherheit reicht nicht aus. Auf Servern befinden sich unternehmenskritische Daten und Anwendungen. Intercept X for Server bietet Schutz, der speziell auf Server ausgerichtet ist, mit niedrigeren False Positive-Raten, und lässt sich in AWS oder Azure bereitstellen. Dank Server Lockdown wird zudem die Angriffsfläche minimiert – und zwar anders als bei anderen Anbietern ganz ohne Zusatzkosten.
Linux-Server müssen nicht geschützt werden	Cyberkriminelle nutzen jede Gelegenheit, wenn sich eine Angriffsfläche bietet, wie etwa ein ungeschützter Server. Linux ist keineswegs vor Angriffen gefeit – ganz im Gegenteil: Das Betriebssystem ist sehr stark an der Ausbreitung von Malware beteiligt.

SOPHOS