SOPHOS
Cybersecurity made simple.

The most comprehensive exploit protection available

Intercept X for Server combines signatureless exploit prevention, deep learning malware detection, and advanced ransomware protection to deliver unparalleled defense against known and unknown threats. It's built to protect servers – which contain an organizations' business-critical applications and that data – from malware, hacking attempts, and data-loss, whether they are deployed on premises or in the public cloud.

Why customers need server protection

- Servers contain an organization's **most valuable information**, so they need the best protection, because while a compromised laptop can be frustrating, **a compromised server can be devastating to the productivity and business of the whole organization.**
- Intercept X for Server: built specifically to protect server applications and data, reducing false positives.
- Designed to **protect against ransomware, exploits, and active adversaries** who want to steal and encrypt data to maximize it to their benefit, using whatever exploits they can to steal credentials and escalate privileges to move laterally.
- Management is easy, with no management server to configure. **Save time** managing all of security through a single pane of glass in Sophos Central.

Who cares, who to talk to

- Security Architect/Analyst
- IT/IS/CIO Manager
- Risk/Security Manager
- IT Operations Manager
- IT Manager

How Sophos is Different vs. Competition

Server-specific: Comprehensive exploit protections

- Vs. Trend (Deep Security): protects against more exploits, and much less expensive
- Vs. Trend (endpoint): protects against more exploits

Protects without impact and effective vs. ransomware

- Vs. Symantec: lacks anti-ransomware and limited exploit; much less expensive than (Data Center)

Simple Management: single console; easy to set up

- Vs. McAfee: complex, enterprise-focused management, with additional products needed for same protections

Call Script	Many customers that don't realize that your servers are not protected with server-specific protections. There are a lot of sophisticated threats today, including ransomware and cryptojacking, and servers are the bullseye on the target for cybercriminals. Sophos Intercept X for Server includes deep learning, anti-exploit, and anti-hacker protections, because a successful attack on a server can devastate an organization.	
Probing Questions	How critical are your servers to your organization's business? Tell me more about your servers and what the the impact to you would be if they were encrypted or if data was stolen from those servers? [Types of Servers: file, application, web, or email servers, or domain controllers]	
	How many servers do you have? Either on-premises, VMs, or in the cloud (instances in AWS or VMs in Azure)? How do you protect these servers today? [Sophos licenses per server]	
	Does your current solution provide comprehensive protection against ransomware and exploits?Have you ever had a ransomware incident on a server? How painful and lengthy was that to remediate?	
Secondary Pitch (per need)	**Ransomware:** Malware has evolved so that half of all malware now includes ransomware, which can leave your servers encrypted and not functioning. Unlike a single laptop, ransomware on a server can cripple an entire business without the apps and data they need. Employees can't be productive, customers aren't getting what they need and paid for, and new orders can't be taken.	**Exploit Prevention and Anti-Hacking:** The best protection for servers today includes protection against a broad set of exploit types and blocking of hackers trying to gain access and hide their presence on servers. Cybercriminals look for personally identifiable, financial, customer, or proprietary data.
	What would happen today if ransomware got onto your server(s)?	What applications and data is your servers?
	Do you have any analytical tools to see where an attack started and how it spread?	How would your organization be impacted if those applications couldn't run? Or if the data was stolen (exfiltrated) from your organization?
	What types of servers sit within your organization? What functions do they provide?	Would your customers still want to do business with you if their information were made public?
	What measures do you have in place to prevent important data from leaving the organization?	How do you protect against exploits today?

StillPointSystems

(818) 528-5600
https://www.stillpointsystems.com/sophos-server-protection/

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS