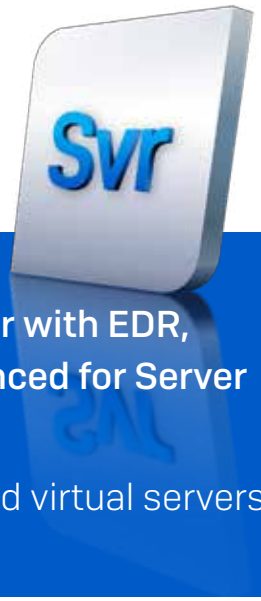
Intercept X for Server



Intercept X Advanced for Server, Intercept X Advanced for Server with EDR, Intercept X Advanced for Server with XDR and Intercept X Advanced for Server with MTR

Sophos Intercept X for Server secures your cloud, on-premises and virtual servers from the latest cybersecurity threats.

Sophos Intercept X for Server employs a comprehensive, defense in depth approach to server security. A combination of powerful defensive techniques and visibility capabilities give organizations the very best protection against the latest threats.

Stop Unknown Threats

Deep learning AI in Intercept X for Server excels at detecting and blocking malware even when it hasn't been seen before. It does this by scrutinizing file attributes from hundreds of millions of samples to identify threats without the need for a signature.

Block Ransomware

Intercept X for Server includes advanced anti-ransomware capabilities that detect and block the malicious encryption processes used in ransomware attacks. Files that have been encrypted will be rolled back to a safe state, minimizing any impact to business productivity.

Prevent Exploits

Anti-exploit technology stops the exploit techniques that attackers rely on to compromise devices, steal credentials and distribute malware. By stopping the techniques used throughout the attack chain Intercept X for Server keeps your organization secure against file-less attacks and zero-day exploits.

Control Your Servers

Ensure only what you want can run. Server Lockdown (whitelisting) makes sure that only applications you have approved can run on a server. File Integrity Monitoring will notify you if there are unauthorized attempts to change critical files.

See Your Wider Cloud Environment

Understand and secure your entire multi-cloud inventory. You can detect your cloud workloads as well as critical cloud services including S3 buckets, databases and serverless functions, identify suspicious activity, spot insecure deployments and close security gaps.

Highlights

- Secures cloud, on-premises and virtual server deployments
- Stops never seen before threats with deep learning AI
- Blocks ransomware and rollback files to a safe state
- Prevents the exploit techniques used throughout the attack chain
- Answers critical IT operations and threat hunting questions with EDR
- See and leverage firewall, email and other data sources with XDR*
- Understand and secure your wider cloud environment such as S3 buckets and databases
- Provides 24/7/365 security delivered as a fully managed service

**Sophos Cloud Optix and Sophos Mobile XDR integration coming soon*

SOPHOS

Endpoint Detection and Response (EDR)

Designed for IT admins and cybersecurity specialists Sophos EDR answers critical IT operations and threat hunting questions. For example, identify servers that have active RDP sessions or analyze cloud security groups to identify resources exposed to the public internet.

Extended Detection and Response (XDR)

Go beyond servers and endpoints, pulling in firewall, email and other data sources*. You get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail. For example, understand office network issues and what application is causing them.

Sophos Cloud Optix and Sophos Mobile XDR integration coming soon

Managed Threat Response (MTR)

24/7/365 threat hunting detection and response service that's delivered by a team of Sophos experts. Sophos analysts respond to potential threats, look for indicators of compromise and provide detailed analysis on events including what happened, where, when, how and why.

Straightforward Management

Intercept X for Server is managed via Sophos Central, the cloud-management platform for all Sophos solutions. It's a single pane of glass for all of you servers, devices and products, making it easy to deploy, configure and manage in cloud, on-premises, virtual and mixed deployments.

Technical Specifications

For the latest information please read the Windows and Linux system requirements. For details on Linux functionality see the Linux datasheet.

Features	Intercept X Advanced for Server	Intercept X Advanced for Server with EDR	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Foundational protection (inc. app control, behavioral detection, and more)	✓	✓	✓	✓	✓
Next-gen protection (inc. deep learning, anti-ransomware, file-less attack protection, and more)	✓	✓	✓	✓	✓
Server controls (inc. Server lockdown, file integrity monitoring and more)	✓	✓	✓	✓	✓
CSPM (Cloud Security Posture Management – see and secure your wider cloud environment)	✓	✓	✓	✓	✓
EDR (Endpoint detection and response)		✓	✓	✓	✓
XDR (Extended detection and response)			✓		See note*
Managed Threat Response (MTR – 24/7/365 threat hunting and response service				✓	✓
MTR Advanced (Leadless hunting, dedicated contact and more)					✓

*Note: The MTR team will have the ability to leverage XDR data and functionality for MTR Advanced customers. However, MTR customers will be limited to EDR functionality in their Sophos Central console, unless they purchase an XDR license.

21-04-05 DS-EN (PS)

SOPHOS

Authorized Distributor :

SecureOne
Optimize with SECURITY

HQ Office (KL)
SecureOne Distribution Sdn Bhd (828358 - X)
No.7, Jalan 109E, Desa Business Park,
Taman Desa, Jalan Kelang Lama,
58100 Kuala Lumpur, Malaysia.

Tel: +6(03) 7984 6086 Fax: +6(03) 7984 6032
Email: sales@secureone.com.my

Northern Office
SecureOne Distribution (Northern) Sdn Bhd (977172 - H)
1A-2-02 @ One Precint (1160),
Lengkok Mayang Pasir,
11950 Bayan Baru, Penang, Malaysia.

Tel: +6(04) 619 2692 Fax: +6(04) 619 2699
Email: northern@secureone.com.my