# Intercept X for Server, EDR, and MTR Overview

SOPHOS

## Managed by Sophos Central

| | Features | Intercept X Advanced for Server | Intercept X Advanced for Server with EDR | Intercept X Advanced for Server with MTR Standard | Intercept X Advanced for Server with MTR Advanced |
|---|---|---|---|---|---|
| ATTACK SURFACE REDUCTION | Web Security | ✓ | ✓ | ✓ | ✓ |
| | Download Reputation | ✓ | ✓ | ✓ | ✓ |
| | Web Control / Category-based URL blocking | ✓ | ✓ | ✓ | ✓ |
| | Peripheral Control | ✓ | ✓ | ✓ | ✓ |
| | Application Control | ✓ | ✓ | ✓ | ✓ |
| | Application Whitelisting (Server Lockdown) | ✓ | ✓ | ✓ | ✓ |
| 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 | ✓ | ✓ | ✓ | ✓ |
| | Intrusion Prevention System (IPS, coming 2021) | ✓ | ✓ | ✓ | ✓ |
| STOP RUNNING THREAT | Data Loss Prevention | ✓ | ✓ | ✓ | ✓ |
| | Runtime Behavior Analysis (HIPS) | ✓ | ✓ | ✓ | ✓ |
| | Antimalware Scan Interface (AMSI) | ✓ | ✓ | ✓ | ✓ |
| | Malicious Traffic Detection (MTD) | ✓ | ✓ | ✓ | ✓ |
| | Exploit Prevention (details on page 5) | ✓ | ✓ | ✓ | ✓ |
| | Active Adversary Mitigations (details on page 5) | ✓ | ✓ | ✓ | ✓ |
| | Ransomware File Protection (CryptoGuard) | ✓ | ✓ | ✓ | ✓ |
| | Disk and Boot Record Protection (WipeGuard) | ✓ | ✓ | ✓ | ✓ |
| | Man-in-the-Browser Protection (Safe Browsing) | ✓ | ✓ | ✓ | ✓ |
| | Enhanced Application Lockdown | ✓ | ✓ | ✓ | ✓ |
| DETECT | Live Discover (Cross Estate SQL Querying for Threat Hunting & IT Security Operations Hygiene) | | ✓ | ✓ | ✓ |
| | SQL Query Library (pre-written, fully customizable queries) | | ✓ | ✓ | ✓ |
| | Suspicious Events Detection and Prioritization | | ✓ | ✓ | ✓ |
| | Fast Access, On-disk Data Storage (up to 90 days) | | ✓ | ✓ | ✓ |

*Features continue on next page*

# Intercept X for Server, EDR, and MTR Overview

SOPHOS

## Managed by Sophos Central

| | Features | Intercept X Advanced for Server | Intercept X Advanced for Server with EDR | Intercept X Advanced for Server with MTR Standard | Intercept X Advanced for Server with MTR Advanced |
|---|---|---|---|---|---|
| INVESTIGATE | Threat Cases (Root Cause Analysis) | ✓ | ✓ | ✓ | ✓ |
| | Deep Learning Malware Analysis | | ✓ | ✓ | ✓ |
| | Advanced On-demand SophosLabs Threat Intelligence | | ✓ | ✓ | ✓ |
| | Forensic Data Export | | ✓ | ✓ | ✓ |
| REMEDIATE | Automated Malware Removal | ✓ | ✓ | ✓ | ✓ |
| | Synchronized Security Heartbeat | ✓ | ✓ | ✓ | ✓ |
| | Sophos Clean | ✓ | ✓ | ✓ | ✓ |
| | Remote Terminal Access (remotely investigate and take action) | | ✓ | ✓ | ✓ |
| | On-demand Server Isolation | | ✓ | ✓ | ✓ |
| | Single-click "Clean and Block" | | ✓ | ✓ | ✓ |
| VISIBILITY | Cloud Workload Protection (Amazon Web Services, Microsoft Azure, Google Cloud Platform)* | ✓ | ✓ | ✓ | ✓ |
| | AWS Map, Multi-region Visualization | | ✓ | ✓ | ✓ |
| | Synchronized Application Control (visibility of applications) | ✓ | ✓ | ✓ | ✓ |
| | Cloud Security Posture Management (monitor and secure cloud hosts, serverless functions, S3 buckets and more) | | ✓ | ✓ | ✓ |
| CONTROL | Server-specific Policy Management | ✓ | ✓ | ✓ | ✓ |
| | Update Cache and Message Relay | ✓ | ✓ | ✓ | ✓ |
| | Automatic Scanning Exclusions | ✓ | ✓ | ✓ | ✓ |
| | File Integrity Monitoring | ✓ | ✓ | ✓ | ✓ |
| MANAGED SERVICE | 24/7 Lead-driven Threat Hunting | | | ✓ | ✓ |
| | Security Health Checks | | | ✓ | ✓ |
| | Data Retention | | | ✓ | ✓ |
| | Activity Reporting | | | ✓ | ✓ |
| | Adversarial Detections | | | ✓ | ✓ |
| | Threat Neutralization & Remediation | | | ✓ | ✓ |
| | 24/7 Lead-less Threat Hunting | | | | ✓ |
| | Threat Response Team Lead | | | | ✓ |
| | Direct Call-in Support | | | | ✓ |
| | Proactive Security Posture Improvement | | | | ✓ |

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

# Operating System Feature Comparison

SOPHOS

| | FEATURES | WINDOWS | LINUX* |
|---|---|---|---|
| ATTACK SURFACE REDUCTION | Web Security | ✓ | |
| | Download Reputation | ✓ | |
| | Web Control / Category-based URL blocking | ✓ | |
| | Peripheral Control | ✓ | |
| | Application Control | ✓ | |
| | Application Whitelisting (Server Lockdown) | ✓ | |
| BEFORE IT RUNS ON DEVICE | Deep Learning Malware Detection | ✓ | |
| | Anti-Malware File Scanning | ✓ | See note |
| | Live Protection | ✓ | See note |
| | Pre-execution Behavior Analysis (HIPS) | ✓ | |
| | Potentially Unwanted Application (PUA) Blocking | ✓ | |
| | Intrusion Prevention System (IPS, coming 2021) | ✓ | |
| STOP RUNNING THREAT | Data Loss Prevention | ✓ | |
| | Runtime Behavior Analysis (HIPS) | ✓ | |
| | Antimalware Scan Interface (AMSI) | ✓ | |
| | Malicious Traffic Detection (MTD) | ✓ | See note |
| | Exploit Prevention (details on page 5) | ✓ | |
| | Active Adversary Mitigations (details on page 5) | ✓ | |
| | Ransomware File Protection (CryptoGuard) | ✓ | |
| | Disk and Boot Record Protection (WipeGuard) | ✓ | |
| | Man-in-the-Browser Protection (Safe Browsing) | ✓ | |
| | Enhanced Application Lockdown | ✓ | |
| DETECT | Live Discover (Cross Estate SQL Querying for Threat Hunting & IT Security Operations Hygiene) | ✓ | ✓ |
| | SQL Query Library (pre-written, fully customizable queries) | ✓ | ✓ |
| | Suspicious Events Detection and Prioritization | ✓ | |
| | Fast Access, On-disk Data Storage (up to 90 days) | ✓ | ✓ |

*Features continue on next page*

# Operating System Feature Comparison

SOPHOS

| | FEATURES | WINDOWS | LINUX* |
|---|---|---|---|
| INVESTIGATE | Threat Cases (Root Cause Analysis) | ✓ | |
| | Deep Learning Malware Analysis | ✓ | |
| | Advanced On-demand SophosLabs Threat Intelligence | ✓ | |
| | Forensic Data Export | ✓ | |
| REMEDIATE | Automated Malware Removal | ✓ | |
| | Synchronized Security Heartbeat | ✓ | See note |
| | Sophos Clean | ✓ | |
| | Live Response (Remote Terminal Access for further investigation and response) | ✓ | ✓ |
| | On-demand Server Isolation | ✓ | |
| | Single-click "Clean and Block" | ✓ | |
| VISIBILITY | Cloud Workload Protection (Amazon Web Services, Microsoft Azure, Google Cloud Platform) | ✓ | ✓ |
| | AWS Map, Multi-region Visualization | ✓ | ✓ |
| | Synchronized Application Control (visibility of applications) | ✓ | |
| | Cloud Security Posture Management (monitor and secure cloud hosts, serverless functions, S3 buckets and more) | ✓ | ✓ |
| CONTROL | Server-specific Policy Management | ✓ | |
| | Update Cache and Message Relay | ✓ | |
| | Automatic Scanning Exclusions | ✓ | |
| | File Integrity Monitoring | ✓ | |
| MANAGED SERVICE | 24/7 Lead-driven Threat Hunting | ✓ | ✓ |
| | Security Health Checks | ✓ | ✓ |
| | Data Retention | ✓ | ✓ |
| | Activity Reporting | ✓ | ✓ |
| | Adversarial Detections | ✓ | ✓ |
| | Threat Neutralization & Remediation | ✓ | ✓ |
| | 24/7 Lead-less Threat Hunting | ✓ | ✓ |
| | Threat Response Team Lead | ✓ | ✓ |
| | Direct Call-in Support | ✓ | ✓ |
| | Proactive Security Posture Improvement | ✓ | ✓ |

*Linux includes two deployment options. 1) Intercept X Advanced for Server with EDR deployment gives access to the features noted in the table. 2) Sophos Anti-Virus for Linux deployment that includes: Anti-malware, Live Protection, Malicious Traffic Detection and Synchronized Security. Please note that the two deployment options cannot be used together.

# Sophos Intercept X Features

Details of features included with Intercept X

SOPHOS

| | Features | |
|---|---|---|
| EXPLOIT PREVENTION | 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 | ✓ |
| | Dynamic Shellcode Protection | ✓ |
| | EFS Guard | ✓ |
| | CTF Guard | ✓ |
| | ApiSetGuard | ✓ |
| ACTIVE ADVERSARY MITIGATIONS | Credential Theft Protection | ✓ |
| | Code Cave Mitigation | ✓ |
| | Man-in-the-Browser Protection (Safe Browsing) | ✓ |
| | Malicious Traffic Detection | ✓ |
| | Meterpreter Shell Detection | ✓ |

| | Features | |
|---|---|---|
| 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 Cases (Root Cause Analysis) | ✓ |
| | Sophos Clean | ✓ |
| | Synchronized Security Heartbeat | ✓ |

# Managed Threat Response (MTR)

SOPHOS

Sophos Managed Threat Response (MTR) provides 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully-managed service. MTR customers also receive Intercept X Advanced with EDR.

## Sophos MTR: Standard

### 24/7 Lead-Driven Threat Hunting

Confirmed malicious artifacts or activity (strong signals) are automatically blocked or terminated, freeing up threat hunters to conduct lead-driven threat hunts. This type of threat hunt involves the aggregation and investigation of causal and adjacent events (weak signals) to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.

### Security Health Check

Keep your Sophos Central products--beginning with Intercept X Advanced with EDR--operating at peak performance with proactive examinations of your operating conditions and recommended configuration improvements.

### Activity Reporting

Summaries of case activities enable prioritization and communication so your team knows what threats were detected and what response actions were taken within each reporting period.

### Adversarial Detections

Most successful attacks rely on the execution of a process that can appear legitimate to monitoring tools. Using proprietary investigation techniques, our team determines the difference between legitimate behavior and the tactics, techniques, and procedures (TTPs) used by attackers.

## Sophos MTR: Advanced *Includes all Standard features, plus the following:*

### 24/7 Leadless Threat Hunting

Applying data science, threat intelligence, and the intuition of veteran threat hunters, we combine your company profile, high-value assets, and high-risk users to anticipate attacker behavior and identify new Indicators of Attack (IoA).

### Enhanced Telemetry

Threat investigations are supplemented with telemetry from other Sophos Central products extending beyond the endpoint to provide a full picture of adversary activities.

### Proactive Posture Improvement

Proactively improve your security posture and harden your defenses with prescriptive guidance for addressing configuration and architecture weaknesses that diminish your overall security capabilities.

### Dedicated Threat Response Lead

When an incident is confirmed, a dedicated threat response lead is provided to directly collaborate with your on-premises resources (internal team or external partner) until the active threat is neutralized.

### Direct Call-In Support

Your team has direct call-in access to our security operations center (SOC). Our MTR Operations Team is available around-the-clock and backed by support teams spanning 26 locations worldwide.

### Asset Discovery

From asset information covering OS versions, applications, and vulnerabilities to identifying managed and unmanaged assets, we provide valuable insights during impact assessments, threat hunts, and as part of proactive posture improvement recommendations.