

# Endpoint Protection

## Тщательно продуманная и простая защита рабочего места

Sophos Endpoint Protection упрощает защиту систем Windows, Mac и Linux от вредоносных программ и сложных угроз, таких как направленные атаки. Система защиты нового поколения объединяет инновационные технологии, с помощью которых производится обнаружение вредоносного трафика в режиме реального времени, а информация об актуальных угрозах своевременно поступает от SophosLabs. Пользователи оказываются под защитой политик доступа к сети Интернет, приложениям и периферийным устройствам повсеместно. Межсетевой экран и конечные устройства могут обмениваться информацией с помощью Security Heartbeat.

### Ключевые функции

- ▶ Инновационная защита включает антивирус, систему предотвращения вторжений (HIPS) и обнаружение вредоносного трафика
- ▶ Контроль web-трафика приложений, устройств и потока данных для полного соблюдения политик безопасности
- ▶ Принудительная фильтрация web-трафика на конечных устройствах, независимо от того, подключены пользователи к корпоративной сети или нет
- ▶ Остановка шифровальщиков и автоматическое восстановление поврежденных файлов
- ▶ Exploit Prevention защищает от использования уязвимостей в программном обеспечении
- ▶ Глубокая очистка системы на основе расследования инцидентов
- ▶ Выбор управления через облачную панель Sophos Central или локально развернутую Sophos Enterprise Console

### Инновационная защита

Sophos Endpoint Protection выходит далеко за рамки защиты от известных вредоносных программ на основе сигнатур. Решение определяет подозрительное поведение и активность с помощью данных об угрозах от SophosLabs в режиме реального времени. Конечные устройства и данные на них будут защищены от целого спектра угроз - от вредоносных URL-адресов до программного кода, использующего эксплойты, а также от неожиданных изменений системы до трафика с командных серверов. В результате будет меньше зараженных компьютеров, защита позволит противостоять направленным атакам и компрометации данных.

### Полный контроль

Усиление безопасности для web-трафика, приложений, устройств и политик работы с данными стало возможным благодаря интеграции агента на конечном устройстве с панелью управления.

- ▶ **Контроль web-трафика** - принудительная web-фильтрация по категориям, как внутри корпоративной сети, так и за её пределами.
- ▶ **Контроль приложений** - блокировка приложений одним нажатием по категориям или названиям.
- ▶ **Контроль периферийных устройств** - управляемый доступ к съемным носителям и мобильным устройствам.
- ▶ **Предотвращение утечек данных (DLP)** - останавливает несанкционированные потоки данных с помощью встроенных или настраиваемых правил.

### Облегчённая производительность

Решение Sophos Endpoint Protection постоянно обновляется для улучшения производительности. Лёгкий агент обеспечивает безопасность пользователей без замедления работы системы. Обновления безопасности выпускаются маленькими пакетами (обычно до 30 Kb), поэтому они легко устанавливаются по сети на конечные устройства.

*«Решения Sophos для конечных устройств лёгкие, стабильные и логичные. Развёртывание решений Sophos усилило нашу безопасность в десятки раз»*

### Тщательно продуманная простота

Sophos Endpoint Protection предоставляет расширенные функциональные возможности в простом и интуитивно понятном пользовательском интерфейсе. Быстрое и лёгкое развёртывание, сбалансированные политики по умолчанию и автоматическая конфигурация HIPS - это только несколько отличий от конкурентов.

### Гибкость лицензирования и развёртывания

С помощью облачной панели управления Sophos Central или программы Sophos Enterprise Console можно применять политики безопасности, устанавливать обновления и получать отчеты. Sophos Intercept X позволяет проводить причинно-следственный анализ, который доступен при управлении конечными устройствами через Sophos Central, где можно использовать преимущества облачного масштабирования, производительности и аналитики.

		ENDPOINT PROTECTION					INTERCEPT X
SKU		ENDPOINT PROTECTION STANDARD	ENDPOINT PROTECTION ADVANCED	ENDPOINT EXPLOIT PREVENTION	CENTRAL ENDPOINT STANDARD	CENTRAL ENDPOINT ADVANCED	CENTRAL INTERCEPT X
ATTACK SURFACE REDUCTION	Web Security	✓	✓		✓	✓	
	Download Reputation	✓	✓		✓	✓	
	Web Control / Category-based URL Blocking	✓	✓			✓	
	Peripheral Control (e.g. USB)	✓	✓			✓	
	Application Control	✓	✓			✓	
	Client Firewall	✓	✓				
PREVENT 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	✓	✓		✓	✓	
	Patch Assessment		✓				
	Data Loss Prevention		✓			✓	
	Exploit Prevention				✓		✓
DETECT STOP RUNNING THREAT	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)			✓			✓
RESPOND INVESTIGATE AND REMOVE	Automated Malware Removal	✓	✓		✓	✓	✓
	Synchronized Security Heartbeat					✓	✓
	Root Cause Analysis						✓
	Sophos Clean			✓			✓