SOPHOS
Security made simple.

FACTOR GROUP
Мастер-дистрибьютор Sophos

Intercept X

Решение для обнаружение вредоносных программ на основе глубокого обучения, предотвращение эксплойтов, выявления причинно-следственных связей и утилита для сканирования Sophos Clean. Sophos Intercept X использует необходимые технологии в нужное время, чтобы предотвратить неизвестные угрозы и остановить злоумышленников. Рекомендуется использовать вместе с текущим антивирусом или с Sophos Endpoint Protection для обеспечения всесторонней защиты следующего поколения.

Ключевые функции

- Распознаёт ещё неизвестные угрозы с помощью моделей обнаружения на базе глубокого машинного обучения
- Exploit Prevention защищает от использования злоумышленниками уязвимостей в программном обеспечении
- Active Adversary Mitigation предотвращает долговременное воздействие вирусов на компьютеры
- Причинно-следственный анализ позволяет отследить действия вредоносных программ и их источники
- Утилита Sophos Clean удаляет вредоносные программы и все их следы
- Приумножает отдачу от инвестиций в антивирусные решения

Используйте защиту следующего поколения для конечных устройств

Дни обычного сканирования файлов давно прошли. Теперь основная задача - предотвратить проникновение угроз, остановить их до выполнения вредоносного кода, и если они обошли превентивную защиту, то обнаружить и не просто удалить, но и проанализировать произошедшее, исправить все вредоносные действия. Sophos Intercept X использует особую технологию, которая позволяет работать совместно с текущим антивирусным решением и обеспечивать всестороннюю защиту следующего поколения.

Обнаружение угроз с помощью глубокого машинного обучения

Решение Intercept X основано на технологиях глубокого обучения нейронных сетей, которое осуществляется на базе SophosLabs. Именно поэтому оно с высокой точностью обнаруживает новые и ещё неизвестные вредоносные файлы без использования сигнатур. Глубокое обучение, применяемое в Intercept X, само определяет важные атрибуты и разграничивает вредоносные и безопасные файлы. В сочетании с активным обучением данных в SophosLabs, такой подход гарантирует, что между безопасными и вредоносными файлами проводится чёткая граница. Эта модель обучения имеет совсем небольшой размер (менее 20 МБ) и не нуждается в частых обновле-ниях. SophosLabs постоянно совершенствует эту модель и отслеживает её эффективность с помощью новых и ранее не встречавшихся образцов вредоносных программ.

Защита от уязвимостей программного обеспечения

Новые уязвимости появляются с пугающей частотой. Они свидетельствуют о недостатках в программном обеспечении, что требует создания всё новых обновлений программ. С другой стороны, новые методы атак появляются в среднем лишь два раза в год, и именно они раз за разом используются злоумышленниками для каждой новой уязвимости. Технология Exploit Prevention позволяет распознавать эти методы и останавливать злоумышленников, даже если уязвимости еще не закрыты обновлениями.

Эффективное обнаружение программ-вымогателей

Технология CryptoGuard позволяет обнаруживать спонтанное злонамеренное шифрование данных и останавливать работу программ-вымогателей. Даже если важные файлы были скомпрометированы или зашифрованы с целью выкупа, CryptoGuard остановит атаку, вернет файлы в исходное состояние без вмешательства пользователей или сотрудников ИТ-отдела. CryptoGuard работает в фоновом режиме на уровне файловой системы, отслеживая удалённые компьютеры и локальные процессы, которые пытаются изменить файлы.

Причинно-следственный анализ

Обнаружение вредоносных программ, их изоляция и удаление решают насущную проблему. Но известно ли наверняка, какой ущерб они успели нанести и как попали в сеть? Причинно-следственный анализ (Root cause analysis) покажет все события по инцидентам, вплоть до момента обнаружения. Можно будет увидеть, какие файлы, процессы и ключи реестров были затронуты, устранить последствия заражения.

Простое развертывание и управление

Управление безопасностью из облачной панели Sophos Central означает, что больше не нужно устанавливать или разворачивать отдельные серверы для защиты конечных устройств. Sophos Central предоставляет такие политики и рекомендуемые конфигурации по умолчанию, чтобы гарантировать самую эффективную защиту.

	Функции	
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	✓
	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	✓
ACTIVE ADVERSARY MITIGATIONS	Credential Theft Protection	✓
	Code Cave Mitigation	✓
	Man-in-the-Browser Protection (Safe Browsing)	✓
	Malicious Traffic Detection	✓
	Meterpreter Shell Detection	✓

Четыре шага к обеспечению защиты

1. Чтобы во.пользов ть.я пробной версией перейдите на sophos.com/intercept-x
2. Создайте в Sophos Central учетную запись администратора
3. Скачайте и установите агент для Intercept X
4. Управляйте своей безопасностью из панели Sophos Central

Технические характеристики

Sophos Intercept X поддерживает операционные системы Windows версии 7 и выше, 32-х и 64-разрядную версии. Решение может работать параллельно с Sophos Endpoint Protection Standard или Advanced при управлении из Sophos Central. Также оно может работать параллельно с антивирусными решениями и решениями для защиты конечных устройств от сторонних разработчиков, дополняя их функциями обнаружения вредоносных программ с помощью глубокого машинного обучения, защиты от эксплойтов и программ-вымогателей, причинно-следственного анализа и Sophos Clean.

	Функции	
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	Deep Learning Malware Detection	✓
	Deep Learning Potentially Unwanted Applications (PUA) Blocking	✓
	False Positive Suppression	✓
	Live Protection	✓
RESPOND INVESTIGATE REMOVE	Root Cause Analysis	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
DEPLOYMENT	Can run as standalone agent	✓
	Can run alongside existing antivirus	✓
	Can run as component of existing Sophos Endpoint agent	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

*Поддерживаются CryptoGuard, обнаружение вредоносного трафика, синхронизация с Security Heartbeat, Root cause analysis

Если вы уже используете Sophos Endpoint Protection с управлением через панель Enterprise Console, то можете управлять своими конечными устройствами через Sophos Central и настроить автоматическое развертывание Intercept X.

Попробуйте бесплатную версию сейчас

Для 30-дневного пробного периода зарегистрируйтесь на sophos.com/intercept-x

Компания Factor Group - дистрибьютор компании Sophos на территории России и стран СНГ, центр компетенции и центр технической поддержки на русском языке.
Телефон: +7 495 280-33-80, +7 495 780-76-70
E-mail: sophos@fgts.ru Сайт: www.fgts.ru

FACTOR GROUP

2017-09-10-DS-NA (MP) RU