SOPHOS
Security made simple.

FACTOR GROUP
Мастер-дистрибьютор Sophos

Intercept X Advanced + EDR

Интеллектуальное обнаружение и устранение угроз на конечных точках

Sophos Intercept X Advanced с EDR - это интеграция интеллектуального обнаружения и устранения угроз для конечных точек (EDR) с топовым отраслевым решением для обнаружением нового вредоносного программного обеспечения, высококлассной защитой от эксплойтов и другими непревзойденными функциями защиты

Особенности

- EDR в сочетании с самой надежной защитой конечных точек
- Глубокий анализ вредоносного ПО с возможностями обучения
- Специальный интеллектуальный анализ угроз от SophosLabs по запросу
- Обнаружение подозрительных событий и определение их приоритета на основе машинного обучения
- Изучение с использованием соответствующих рекомендаций делают применение EDR еще более эффективным
- Мгновенное реагирование на инциденты

Обнаружение и устранение угроз на конечных точках начинается с самой надежной защиты

Предотвращение атак до их возникновения является критически важным фактором. Intercept X объединяет в едином решении непревзойденную защиту, обнаружение и устранение угроз на конечных точках. Это означает, что большинство угроз устраняется еще до того, как они смогут нанести ущерб, а Intercept X Advanced с EDR обеспечивает дополнительную кибербезопасность благодаря своей возможности определять, выявлять и устранять возможные угрозы.

Включение EDR в постоянно получающий наилучшие оценки пакет решений позволяет Intercept X значительно снизить нагрузку на решение EDR. Чем больше предотвращается угроз, тем меньше специалистам по безопасности необходимо изучать ложные и незначительные проблемы. Это означает, что специалисты могут оптимизировать ключевые ресурсы и акцентировать свое внимание на ИТ-задачах вместо того, чтобы тратить время на ложные угрозы и избыточное количество предупреждений об опасности.

Углубление экспертных знаний, а не увеличение персонала

Intercept X Advanced с EDR может выполнять те задачи, которые, как правило, решаются опытными аналитиками, поэтому организации могут использовать значительные экспертные знания, не привлекая дополнительного персонала. В отличие от других решений EDR, которые основаны на интерпретации высококлассными аналитиками ответов на заданные вопросы, решение Intercept X Advanced с EDR основано на машинном обучении и дополнено специализированной аналитикой угроз от SophosLabs.

Экспертиза в сфере безопасности.
Intercept X Advanced с EDR предоставляет значительную экспертизу безопасности за счет автоматического выявления возможных угроз и определения их приоритетности. Благодаря машинному обучению подозрительные события выявляются и передаются на более высокий уровень как имеющие особую важность и требующие незамедлительного внимания. Аналитики могут быстро оценить, чему следует уделить внимание и понять, какие устройства могут оказаться под угрозой.

Экспертиза вредоносного ПО.
Большинство организаций полагаются на мнение экспертов по вредоносному ПО, которые занимаются декомпиляцией и анализом подозрительных файлов. Подобный подход не только занимает много времени и сложен в реализации, но и предполагает такой уровень комплексной кибербезопасности, который недоступен большинству организаций. Intercept X Advanced с EDR предоставляет более качественный подход, при котором задействуется глубокий анализ вредоносного ПО с возможностями обучения, позволяющий автоматически анализировать вредоносное ПО во всех подробностях, определять атрибуты и код файлов, сравнивать их с миллионами других. Аналитики могут с легкостью определить, какие атрибуты и сегменты кода похожи на «заведомо хорошие» или «заведомо плохие» файлы, что позволит решить, следует ли блокировать или же разрешить использование того или иного файла.

Интеллектуальная экспертиза угроз.
Если в Intercept X Advanced с EDR подозрительный файл передается на анализ более высокого уровня, то ИТ-администраторы могут воспользоваться дополнительными сведениями, получив доступ к специализированному анализу угроз, предоставляемому компанией SophosLabs по запросу. Лаборатория ежедневно получает и обрабатывает приблизительно 400 000 образцов совершенно нового вредоносного ПО. Эти данные, вместе с другой аналитикой угроз, собираются, агрегируются и сводятся воедино для простоты дальнейшего анализа. Таким образом команды специалистов, в которых нет аналитиков угроз или которые не имеют доступ к дорогим и малопонятным данным по угрозам, могут использовать преимущества одной из лучших в мире групп специалистов, занимающихся исследованием кибербезопасности, а также теорией и методами анализа данных.

Устранение инцидентов под руководством специалистов

Intercept X Advanced с EDR позволяет администраторам отвечать на самые сложные вопросы об инцидентах безопасности за счет полного понимания масштабов атаки, её начала, её последствий и возможностей для реагирования. Группы специалистов любого уровня, занимающиеся безопасностью, могут с легкостью определить уровень безопасности своих организаций благодаря изучению проблем с получением пошаговых рекомендаций, четкому визуальному представлению атак и встроенным анализом. После завершения изучения аналитики могут отреагировать на угрозы одним нажатием кнопки. Возможности быстрого реагирования включают изоляцию конечных точек для немедленного устранения угроз, очистку и блокировку файлов, создание аналитических "снимков".

Примеры использования интеллектуального обнаружения и устранения угроз на конечных точках

Интеллектуальное обнаружение и устранение угроз на конечных точках означает, что группы специалистов, занимающихся безопасностью, обладают пониманием и экспертными знаниями, необходимыми для ответа на самые трудные вопросы, которые могут возникнуть в рамках реагирования на тот или иной инцидент.

Ответы на трудные вопросы в отношении инцидента:

- Понимание масштабов и последствий инцидентов, связанных с безопасностью.
- Определение атак, которые могли пройти незамеченными.
- Поиск индикаторов взлома сети.
- Определение приоритетов событий для дальнейшего изучения.
- Анализ файлов для определения, являются ли они угрозой или потенциально нежелательными.
- Конфиденциальный отчет о положении организации в плане безопасности в любой момент времени.

Выход за рамки обнаружения и устранения угроз на конечных точках

Чтобы предотвратить различные угрозы, Intercept X Advanced с EDR задействует комплексный подход к многоуровневому обеспечению безопасности конечных точек вместо простого использования базового метода обеспечения безопасности. Это «сила сложения» — сочетание ведущих основополагающих и современных методов. Intercept X Advanced с EDR интегрирует ведущие способы обнаружения вредоносного ПО, высококлассную защиту от эксплойтов, интеллектуальное обнаружение и устранение угроз на конечны точках (EDR).

Современные методы включают определение вредоносного ПО с возможностями глубокого машинного обучения, противодействие эксплойтам и функции, направленные против программ-вымогателей. Основополагающие методы включают антивирус, поведенческий анализ, определение вредоносного трафика, предотвращение потери данных и многое другое.

Intercept X Advanced с EDR сочетает в себе возможности обнаружения и устранения угроз на конечных точках с современными функциями Intercept X и основополагающими методами Sophos Central Endpoint Protection, что доступно в рамках единого решения и одного агента.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
Основополагающие методы	✓	✓		✓
Глубокое обучение	✓	✓	✓	
Противодействие эксплойтам	✓	✓	✓	
Противодействие программам-вымогателям CryptoGuard	✓	✓	✓	
Обнаружение и устранение угроз на конечных точках (EDR)	✓			

Попробуйте бесплатно уже сейчас!

Зарегистрироваться на бесплатный 30-дневный ознакомительный период и получить доступ к решению можно на странице sophos.com/intercept-x

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

18-10-02 DS-NA (3098-DD)