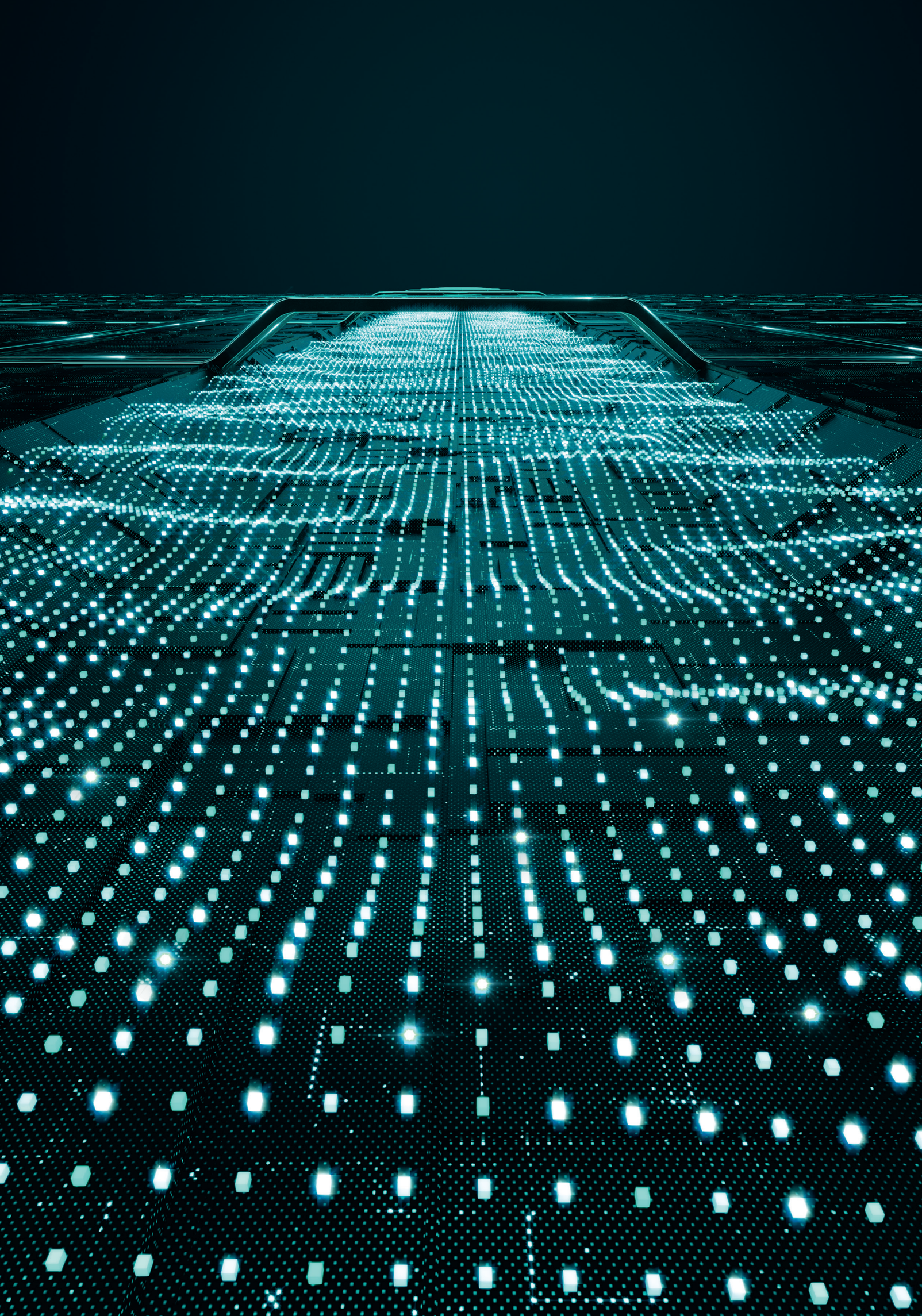
ОБЗОР ПРОДУКТА

ENTERPRISE INSPECTOR

Узнайте о скрытых угрозах в корпоративной сети
с помощью EDR решения глобального игрока рынка
информационной безопасности

АНТИВИРУСНАЯ ЗАЩИТА
БИЗНЕС-КЛАССА

30 РАЗВИВАЕМ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ УЖЕ 30 ЛЕТ



Что такое **Endpoint Detection & Response (EDR)**

ESET Enterprise Inspector – сложное высокотехнологичное решение класса EDR для обнаружения аномального поведения и нарушений, оценки рисков, реагирования на инциденты безопасности, расследования и устранения последствий.

Решение отслеживает и оценивает в режиме реального времени все происходящее в сети (активность пользователей, файлы, процессы, реестр, память, события) и позволяет немедленно принять меры, если это необходимо.

Зачем нужно **EDR решение?**

НАРУШЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ

Когда произошла утечка данных, компании мало обнаружить инцидент – необходимо локализовать и устранить его. Большинство организаций не могут провести полноценное расследование и вынуждены нанимать внешних подрядчиков. Компаниям необходима прозрачность сети, чтобы новые киберугрозы, потенциально опасные действия сотрудников и нежелательные приложения не подвергали риску прибыль и репутацию.

Традиционно жертвами кражи данных становятся представители отраслей, работающих с конфиденциальной информацией – организации финансового и государственного секторов, торговли и здравоохранения. Однако это не означает, что другие отрасли находятся в безопасности – просто хакеры тщательно взвешивают собственные вложения и возможный доход.

APT И ЦЕЛЕВЫЕ АТАКИ

Решения EDR используются для выявления APT или целевых атак с помощью проактивного поиска угроз (Threat Hunting), сокращения времени реагирования на инциденты и предотвращения будущих атак. В частности, обнаружение APT угроз важно для корпораций, поскольку большинство компаний сегодня не готовы к современным кибератакам, которые могут оставаться незамеченными в течение дней и даже месяцев.

ПОВЫШЕНИЕ ПРОЗРАЧНОСТИ

Основные проблемы компаний – фишинговые атаки и инсайдеры. Фишинг довольно эффективен в атаках на корпорации с обширным штатом – хороший шанс, что хоть один работник попадется на крючок и в итоге поставит под угрозу весь бизнес. Атаки инсайдеров также опасны для корпораций, поскольку большое число сотрудников увеличивает вероятность того, что один из них захочет сыграть против интересов работодателя.

Решения EDR обеспечивают необходимую компаниям прозрачность, чтобы видеть, понимать, блокировать и устранять любые проблемы на устройствах корпоративной сети. Возможности EDR включают блокировку опасных вложений электронной почты и обеспечение того, чтобы сотрудники использовали только разрешенные ресурсы.

Платформа для защиты конечных точек ESET
Многоуровневая защита конечных точек, каждый уровень которой отправляет данные в ESET Enterprise Inspector.

+

ESET Enterprise Inspector
Сложное высокотехнологичное решение класса EDR анализирует огромные объемы данных в режиме реального времени, чтобы ни одна угроза не осталась незамеченной.

=

Комплексное решение для предотвращения, обнаружения и реагирования на киберугрозы, которое позволяет быстро анализировать и устранять любые проблемы безопасности в корпоративной сети.

Сегодня компаниям необходима прозрачность сети, чтобы новые **киберугрозы, потенциально опасные действия сотрудников и нежелательные приложения** не подвергали риску прибыль и репутацию.

Рекомендуется использовать ESET Enterprise Inspector в сочетании со следующими сервисами

Внедрение решений и обучение технических специалистов

Инженеры ESET устанавливают и настраивают продукты в корпоративной среде, а также обучают технических специалистов заказчика развертыванию и эффективному использованию этих инструментов с первого дня.

ESET Threat Monitoring

Операторы сервиса постоянно контролируют состояние сети заказчика и безопасность конечных точек, предупреждая в режиме реального времени, когда что-то подозрительное потребует внимания.

ESET Threat Hunting

Специалисты ESET помогают заказчикам исследовать данные, события и срабатывания ESET Enterprise Inspector, анализируют причины инцидентов и выполняют криминалистическое расследование, разрабатывают практические рекомендации по минимизации последствий.

Преимущества ESET

РЕТРОСПЕКТИВНЫЙ ПОИСК УГРОЗ

ESET Enterprise Inspector поддерживает не только настраиваемый поиск угроз, но и ретроспективный анализ. Достаточно настроить правила поведения, а затем «сканировать» базу данных событий. Это позволит идентифицировать любые новые срабатывания, соответствующие настроенным правилам обнаружения. Осуществляется поиск не статического IoC, а динамического поведения с несколькими параметрами.

В ОБЛАКЕ ИЛИ ЛОКАЛЬНО

Используя преимущества гибкой и безопасной архитектуры, ESET Enterprise Inspector поддерживает как облачное, так и локальное развертывание для лучшей масштабируемости – в зависимости от размера и потребностей компании.

ОТКРЫТАЯ АРХИТЕКТУРА

Обеспечивает уникальное детектирование на основе поведения и репутации, прозрачное для службы информационной безопасности. Все правила легко редактируются с помощью XML, поэтому их можно точно настроить или создать заново в соответствии с потребностями конкретной корпоративной среды, включая интеграцию с SIEM.

НАСТРАИВАЕМАЯ ЧУВСТВИТЕЛЬНОСТЬ

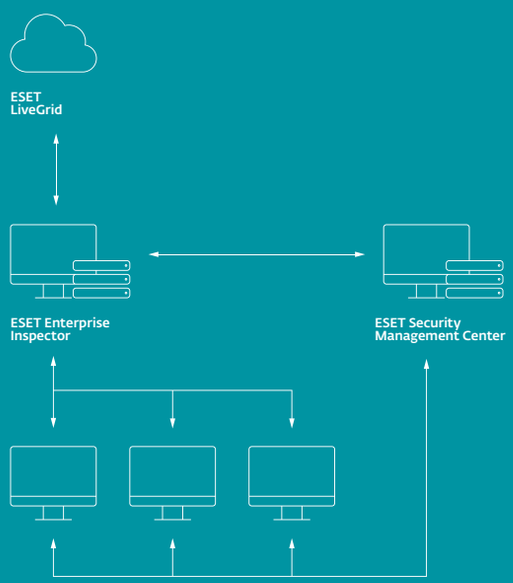
Чтобы исключить ложные срабатывания, достаточно настроить правила обнаружения для разных групп компьютеров и пользователей. Точно задать условия срабатывания можно, объединив такие критерии, как имя файла, путь, хеш, командная строка, владелец подписи.

РЕПУТАЦИОННЫЙ АНАЛИЗ

Всесторонняя фильтрация позволяет инженерам информационной безопасности определять заведомо «хорошие» приложения, используя систему репутации ESET. Эта система содержит базу данных из сотен миллионов файлов и гарантирует, что службы ИБ изучают неизвестные приложения, не отвлекаясь на ложные срабатывания.

СИНХРОННОЕ РЕАГИРОВАНИЕ

Построенный на основе существующих решений ESET для защиты конечных точек, ESET Enterprise Inspector создает комплексную экосистему, которая перекрестно связывает объекты сети и синхронизирует устранение инцидентов. Службы ИБ могут завершать процессы, загружать файлы, вызвавшие срабатывание, просто выключить компьютер или перезапустить его прямо из консоли.



Обеспечивает уникальное детектирование на основе поведения и репутации, прозрачное для службы информационной безопасности.

Примеры использования

Углубленное обнаружение угроз: программы-вымогатели

Современные программы-вымогатели пытаются остаться незамеченными в сети, скрыто распространяясь на максимально возможное число конечных точек. Они проникают в хранилища резервных копий, чтобы гарантировать, что даже откат к предыдущей версии не позволит восстановить систему.

Агент ESET Enterprise Inspector расширяет функциональные возможности решений ESET для защиты конечных точек и позволяет заранее обнаружить программу-вымогатель, действующую в сети. В типичном сценарии атаки пользователь получает электронное письмо с файлом Word во вложении. Открыв документ, он видит запрос на включение макросов. Если пользователь включит макросы, в систему загружается исполняемый файл и начинает шифровать все доступные документы, в том числе содержимое внешних дисков.

ESET Enterprise Inspector предупреждает службу информационной безопасности об этом типе поведения. Инженер ИБ в несколько кликов может проверить, какие системы затронуты, где и когда выполнен конкретный файл, сценарий или действие, проанализировать причины инцидента.

ПРОБЛЕМА

Компании необходим дополнительный инструмент для проактивного обнаружения программ-вымогателей и немедленное уведомление о подозрительном поведении в сети, напоминающем о шифраторах.

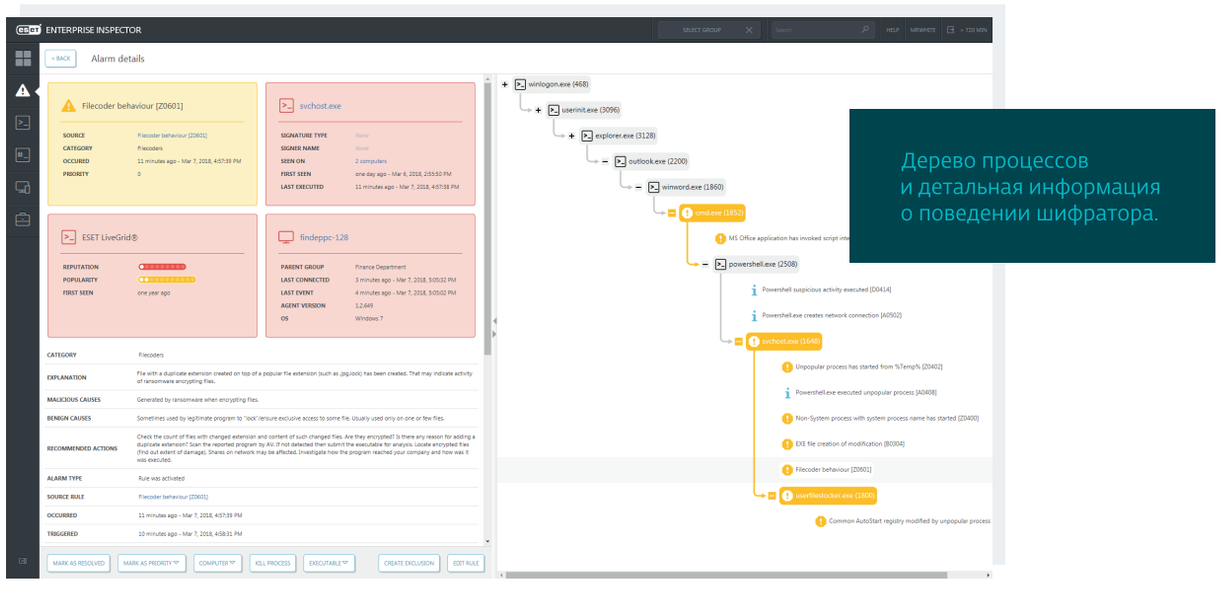
РЕШЕНИЕ

Правила для обнаружения приложений, которые выполняются из временных папок

Правила для определения файлов Microsoft Office (Word, Excel, PowerPoint), когда они выполняют дополнительные скрипты и исполняемые файлы

Срабатывание при обнаружении на устройстве файла с расширением, типичным для известных программ-вымогателей

Обзор в единой консоли срабатываний модуля «Защита от программ-вымогателей» продуктов ESET для защиты конечных точек



Детектирование на основе поведения и повторные нарушения

Слабое звено в информационной безопасности – пользователь, даже если у него нет каких-либо дурных намерений.

ESET Enterprise Inspector позволяет идентифицировать потенциальные угрозы безопасности, сортируя компьютеры по числу уникальных срабатываний. Если действия пользователя вызвали несколько срабатываний, его активность необходимо проверить.

ПРОБЛЕМА

В компании есть пользователи, постоянно сталкивающиеся с вредоносными программами. Одни и те же люди заражают компьютеры раз за разом. Они неосторожны или становятся целью атак чаще, чем другие пользователи?

РЕШЕНИЕ

- ✓ Простой и удобный обзор проблемных пользователей и устройств
- ✓ Быстрый анализ причин инцидента позволяет найти источник заражения
- ✓ Легко обнаружить векторы заражения, такие как электронная почта, интернет или USB-устройства

Проактивный поиск и блокирование угроз

Преимущество ESET Enterprise Inspector – проактивный поиск угроз путем «поиска иголки в стоге сена».

Применяя фильтры к данным, которые сортируются на основе популярности или репутации файла, цифровой подписи, поведения или контекста, можно идентифицировать и расследовать любую вредоносную активность. Установка нескольких фильтров позволяет автоматизировать проактивный поиск угроз и настраивать порог обнаружения в соответствии со средой компании.

Любая вредоносная активность будет идентифицирована и расследована.

ПРОБЛЕМА

Система раннего оповещения или SOC центр выдает новое предупреждение об угрозе. Каковы следующие действия?

РЕШЕНИЕ

- ✓ Использование системы раннего оповещения для получения данных о планируемой или новой угрозе
- ✓ Проверка всех компьютеров на предмет новой угрозы
- ✓ Проверка всех компьютеров на наличие индикаторов компрометации, выполненной до оповещения об угрозе
- ✓ Блокировка угрозы для предотвращения проникновения или выполнения внутри сети компании

Прозрачность сети

ESET Enterprise Inspector – решение с открытой архитектурой, поэтому служба информационной безопасности может корректировать правила детектирования, описывая методы атаки на среду организации.

Открытая архитектура позволяет гибко настраивать ESET Enterprise Inspector для обнаружения нарушений политик компании в отношении используемого ПО, например, торрентов, облачных хранилищ, браузера Tor, запуска собственных серверов и другого нежелательного софта.

ПРОБЛЕМА

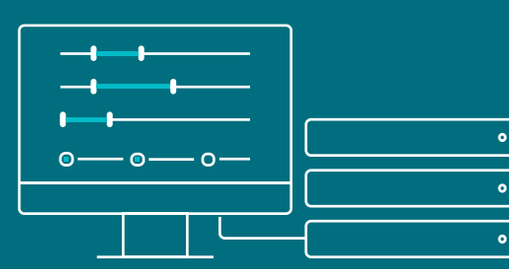
Некоторые компании обеспокоены тем, что пользователи запускают в системе различные приложения. Опасность представляют не только традиционно устанавливаемые приложения, но и переносимые, которые фактически не загружаются в систему. Как их контролировать?

РЕШЕНИЕ

- ✓ Удобный просмотр и фильтрация всех установленных приложений на разных устройствах
- ✓ Просмотр и фильтрация всех скриптов на разных устройствах
- ✓ Простая блокировка запуска неавторизованных скриптов и приложений
- ✓ Исправление проблем путем уведомления пользователей о неавторизованных приложениях и автоматическое удаление

Опасность представляют не только традиционно устанавливаемые приложения, но и переносимые, которые фактически не загружаются в систему. Как их контролировать?

Служба информационной безопасности может корректировать правила детектирования, описывая методы атаки на среду организации.



Контекстно-зависимое расследование и исправление

«Вредоносность» активности зависит от контекста.

Действия, выполняемые на компьютере администратора сети, сильно отличаются от действий, например, финансового департамента. При правильной группировке компьютеров служба информационной безопасности легко определит, может ли данный пользователь выполнять те или иные действия на этом устройстве. Синхронизация групп компьютеров в ESET Security Management Center и правил ESET Enterprise Inspector обеспечивает выдающиеся результаты работы с контекстом.

ПРОБЛЕМА

Данные так же хороши, как их контекст. Для принятия правильных решений необходимо знать, что это за срабатывания, на каких устройствах они зафиксированы, какие пользователи их вызывают.

РЕШЕНИЕ

- ✓ Определить и отсортировать все компьютеры в соответствии с Active Directory, с помощью автоматической или ручной группировки
- ✓ Разрешить или заблокировать приложения или скрипты для групп компьютеров
- ✓ Разрешить или заблокировать приложения или скрипты для пользователей
- ✓ Получать уведомления для определенных групп

Простая настройка и реагирование – не придется привлекать службу ИБ

Даже если в компании есть служба информационной безопасности, ее сотрудникам зачастую сложно расставить приоритеты и выбрать следующий шаг среди всех уведомлений и срабатываний.

Поэтому для каждого срабатывания предлагаются шаги, необходимые для исправления. Обнаружив угрозу, ESET Enterprise Inspector предлагает возможность быстрого реагирования. Определенные файлы могут быть заблокированы по хешу, процессы завершены и помещены в карантин, выбранные компьютеры изолированы или удаленно отключены.

ПРОБЛЕМА

Не во всех компаниях есть служба информационной безопасности. Ввод и внедрение расширенных правил детектирования может стать проблемой.

РЕШЕНИЕ

- ✓ Более 180 предварительно настроенных правил
- ✓ Простое реагирование с помощью одной кнопки позволяет заблокировать, отключить или изолировать устройства
- ✓ Для каждого срабатывания предлагаются дальнейшие шаги, необходимые для решения проблемы
- ✓ Правила можно редактировать через XML, что упрощает их настройку или создание новых правил

«Вредоносность» активности зависит от контекста. Синхронизация групп компьютеров в ESET Security Management Center и правил ESET Enterprise Inspector обеспечивает выдающиеся результаты работы с контекстом.

Для каждого срабатывания предлагаются дальнейшие шаги, необходимые для решения проблемы.

Возможности продукта

ПРОАКТИВНЫЙ ПОИСК УГРОЗ (THREAT HUNTING)

Применение фильтров к данным для сортировки на основе популярности файла, репутации, цифровой подписи, поведения или контекста. Установка нескольких фильтров позволяет обнаруживать угрозы автоматически, фильтры настраиваются в соответствии со средой компании. Позволяет легко обнаруживать угрозы, включая APT и целевые атаки.

ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ (АНАЛИЗ ПРИЧИН)

Быстрый и простой обзор всех инцидентов безопасности в разделе срабатываний. Служба информационной безопасности может в несколько кликов получить анализ причин: что было затронуто, где и когда выполнен исполняемый файл, скрипт или действие.

РАССЛЕДОВАНИЕ И ИСПРАВЛЕНИЕ

Встроенный набор правил и возможность создания своих собственных для реагирования на обнаруженные инциденты. Для каждого срабатывания предлагаются дальнейшие шаги, необходимые для решения проблемы. Функция быстрого реагирования позволяет блокировать определенные файлы по хешу, завершать и помещать в карантин процессы, изолировать или удаленно отключать выбранные компьютеры. Это гарантирует, что ни один инцидент не останется незамеченным.

СБОР ИНФОРМАЦИИ

Просмотр данных о недавно запущенных модулях, включая время запуска, пользователя, время взаимодействия, атакованные устройства. Все данные хранятся локально во избежание утечек.

ДЕТЕКТИРОВАНИЕ IOC

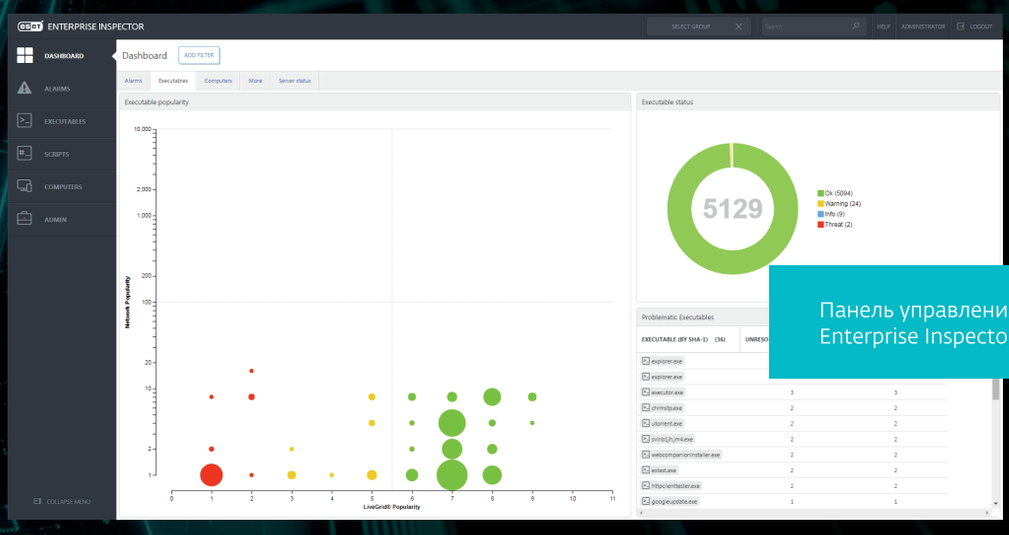
Просмотр и блокировка модулей на основе свыше 30 индикаторов компрометации, включая хеш, модификацию реестра или файлов, сетевые подключения.

ДЕТЕКТИРОВАНИЕ ПО АНОМАЛИЯМ И ПОВЕДЕНИЮ

Проверка исполняемого файла с помощью системы репутации ESET LiveGrid позволяет быстро оценить процессы – безопасны они или подозрительны. Группировка компьютеров по пользователю, отделу и другим критериям помогает службе информационной безопасности оперативно определить, имеет ли пользователь право на выполнение того или иного действия.

НАРУШЕНИЕ ПОЛИТИК КОМПАНИИ

Блокировка запуска вредоносных модулей на любом компьютере корпоративной сети. Открытая архитектура позволяет гибко настраивать ESET Enterprise Inspector для обнаружения нарушений политик компании в отношении используемого ПО, например, торрентов, облачных хранилищ, браузера Tor и другого нежелательного софта.



Панель управления ESET Enterprise Inspector

О компании ESET

ESET, глобальный игрок рынка информационной безопасности, названа «Претендентом» (Challenger) в рейтинге разработчиков платформ для защиты конечных точек Gartner*.

Более 30 лет компания ESET разрабатывает передовое программное обеспечение и сервисы в области информационной безопасности, обеспечивая комплексную защиту от киберугроз для компаний и домашних пользователей по всему миру.

ESET является частной компанией, не зависящей от государственных и политических решений. Компания обладает финансовой свободой и делает максимум для защиты всех клиентов.

ESET В ЦИФРАХ

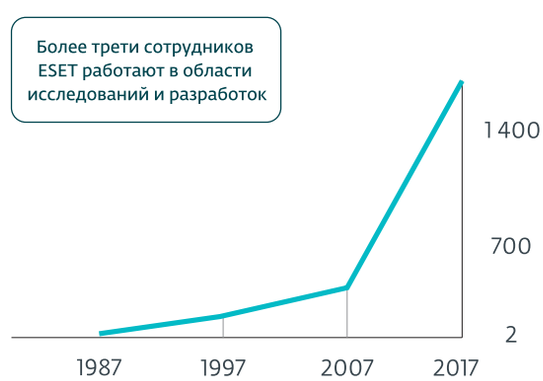
110 млн
пользователей по всему миру

400 тыс.
корпоративных клиентов

200+
стран присутствия

13
центров исследований

СОТРУДНИКИ ESET



ДОХОДЫ ESET

Gartner не рекомендует никаких производителей, продукты или услуги, представленные в отчетах. Аналитические публикации Gartner основаны на мнении исследовательской организации Gartner и не могут считаться констатацией факта. Gartner не дает никаких гарантий, выраженных в явной или подразумеваемой форме, в отношении публикуемых данных, в том числе гарантий коммерческой пригодности или соответствия определенной цели.

НАШИ КЛИЕНТЫ

HONDA

С 2011 года под защитой ESET.
Лицензия продлевалась трижды
и была расширена в два раза

GREENPEACE

С 2018 года под защитой ESET.
После продления лицензия
расширена в 10 раз

Canon

С 2016 года под защитой ESET.
Более 14 000 рабочих станций

T · ·

ISP-партнер по безопасности с 2008 года.
База клиентов – 2 миллиона

НАШИ НАГРАДЫ

SE Labs AAA ENTERPRISE ENDPOINT PROTECTION JUL-SEP 2018

THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE WINNER 2017

AV comparatives Approved Business Product 2017

SC MEDIA RECOMMENDED

«Учитывая хорошие характеристики защиты от вредоносных программ, управляемость, глобальный охват и качественную поддержку клиентов, компания ESET должна быть в финальном списке рассмотрения производителей программного обеспечения для защиты от вредоносных программ»,

— эксперт международной независимой аналитической организации KuppingerCole Leadership Compass, публикация «Корпоративная безопасность рабочих станций: антивирусные решения» от 2018 года.

ESET

АНТИВИРУСНАЯ ЗАЩИТА
БИЗНЕС-КЛАССА