ivanti

ОБЗОР РЕШЕНИЯ

Ivanti Endpoint Security for Endpoint Manager

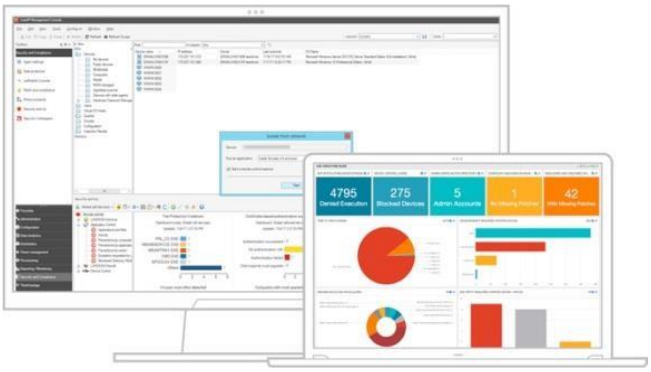
Решение Ivanti® Endpoint Security для Endpoint Manager, разработанный Landesk, предотвращает, обнаруживает и исправляет последствия заражения даже самыми сложными и опасными вымогателями и другими вирусами. Мощная, многоуровневая защита автоматизирует обнаружение, инвентаризацию и управление обновлениями, предотвращает запуск и распространение вредоносного ПО. В сочетании с Ivanti Unified Endpoint Manager это решение предоставляет уникальную возможность изолировать устройство, но при этом удаленно управлять им, а также восстановить зараженную систему или перезалить ее образ. Благодаря интеграции этих двух продуктов управление ИТ-средой становится гораздо эффективнее.

Защитите Вашу инфраструктуру от вирусов-вымогателей и других угроз

С Ivanti Endpoint Security для Endpoint Manager вы получите все необходимое, чтобы находить и устранять вредоносное ПО, диагностировать неполадки и выявлять неисправные или неавторизованные процессы. Если вредоносное ПО проникает в вашу сеть, Endpoint Security поймает его, нейтрализует, оповестит другие машины и заблокирует запуск этого ПО на них. Широкие возможности удаленного управления позволяют изолировать, исследовать и очистить компьютеры по всей сети. В дополнение, блокировка устройств и управление соединениями позволяет контролировать и ограничивать доступ для устройств ввода / вывода. Функции управления приложениями защищают от уязвимостей нулевого дня, стелс-атак и других сложных угроз. А функции защиты данных предотвращают шифрование ваших файлов вирусами-шифровальщиками.

Обнаружение и инвентаризация всех сетевых устройств и ПО

Активные и пассивные технологии обнаружения идентифицируют и инвентаризуют все устройства с поддержкой IP-сети в режиме реального времени - даже те, которые находятся за брандмауэрами. Автоматическое обнаружение также помогает найти все программное обеспечение на этих устройствах,



включая сведения об использовании. А при использовании с Ivanti® Cloud Services Appliance, Ivanti Endpoint Security может инвентаризировать системы и устройства, не подключенные к корпоративной сети, без необходимости подключения виртуальных частных сетей (VPN).

Надежность и безопасность среды с помощью автоматизированной установки обновлений

Ivanti Endpoint Security для Endpoint Manager упрощает управление обновлениями с помощью лучших практик, автоматических процессов, не влияет на пользователей и быстро развертывается. Он надежно защищает все устройства и стороннее программное обеспечение в вашей сети - даже те устройства, которые находятся за пределами сети, на удаленном сайте или в режиме сна

Защита с помощью блокировки соединений и внешних устройств

Функции управления устройством и фильтр приложений ограничивают типы внешних устройств или соединений, к которым могут обращаться компьютеры. Вы также можете обнаруживать и блокировать вредоносное ПО на внешних устройствах, которые подключаются к рабочим станциям, и блокировать обращения от вредоносного ПО, что делает большую часть функций вируса бесполезной. Решение регистрирует, какие файлы копируются на внешние устройства, поэтому вы можете быть уверены, что пройдете проверку безопасности

Настройка и обновление	
Функционал	**Возможности**
Обнаружение устройств	Активное, пассивное, а также без помощи агентов обнаружение и инвентаризация – для зашиты и обновления конечных точек. Обнаружение и выявление местоположения беспроводных точек доступа.
Обновления	Автоматизированное обновление различных ОС и сторонних приложений.
	Планирование и развертывание исправлений с использованием пилотных групп и дальнейшего развертывания в бизнес среде
	Установка обновлений не влияет на продуктивность пользователей, т. к. это происходит в период обслуживания, и сами пользователи могут управлять перезагрузкой.
Аналитика по обновлениям	Обратная связь от конечных пользователей для более точного выявления проблем, вызванных обновлениями и снижающими продуктивность.
Управление настройками безопасности	Встроенный пакет контента для проверки соответствия стандарту PCI.
	Возможность создавать дополнительные скрипты для приведения системы в соответствие с требованиями.
Межсетевой экран	Блокировка вредоносных программ и передач данных.

Обнаружение и предотвращение	
Функционал	**Возможности**
Обнаружение программ- -вымогателей	Выявление и устранение вирусов-шифровальщиков, а также оповещение о них других устройств в сети.
Блокировка программ-вымогателей	Защита файлов от шифрования и от распространения самого шифровальщика по сети.
Обнаружение вредоносного ПО	Обнаружение вредоносного ПО на основе сигнатур, поведения или сетевого трафика.
Обнаружение вредоносных сайтов	Пользователи не смогут зайти на подозрительные сайты.
Предотвращение бесфайловых атак	Блокировка бесфайловых атак, вызываемых из макросов Microsoft.
Управление приложениями	Динамическое составление белых списков позволяет узнать, какие приложения есть в среде, и предотвратить несанкционированное исполнение кода.
Управление устройствами	Запрет на использование портов и съемных носителей, которые могут использоваться для внедрения вредоносного ПО или использоваться для переноса важных корпоративных данных с записью всех действий по копированию в журнал.

Восстановление и мониторинг	
Функционал	**Возможности**
Изоляция от сети	Предотвращение распространения вредоносного ПО, при этом к изолированным устройствам можно получить удаленный доступ.
Сдерживание вредоносного ПО	Изоляция вируса при обнаружении.
Удаленный доступ	Удаленное управление, в том числе файлами; удаленная остановка процессов и переустановка образов; удаленное развертывание других инструментов и скриптов для расследования.
Информационные панели и отчеты	Панели Ivanti Xtraction: мощная аналитика без участия эксперта по электронным таблицам. Панели мониторинга уязвимостей, обновлений и операций по защите сети, а также уведомления об угрозах и подробные отчеты по кибербезопасности.
Интеграция с SIEM	Интеграция журнала событий с инструментами SIEM для продолжения расследования и получения аналитики.
Лучшие решения объединённого IT	**Возможности**
Миграция на Windows 10 и Windows как услуга (обновления)	Автоматизированное предоставление устройств на Windows 10, которые уже персонализированы и готовы к использованию. Обслуживание всех обновлений и каналов связи, которые предоставляет Microsoft.
Наем на работу и увольнение	Необходимые права доступа, приложения и ресурсы, когда пользователь вступает в должность или переходит на другую, и удаление этих прав, когда он увольняется.
Само-обслуживание IT	Создайте каталог услуг, который объединяет все в фоновом режиме — различные услуги, развертывание, управление активами — пользователю достаточно просто нажать на кнопку.

Защита от угроз нулевого дня с помощью расширенного управления приложениями

Функции управления приложениями защищают от файловых атак и бесфайловых угроз, предотвращая запуск и выполнение вредоносного ПО и скриптов, а также используя методы защиты памяти. Возможности обучения минимизируют ложные срабатывания и позволяют проверенным приложениям работать бесперебойно. Сервис репутации файлов предоставляет дополнительные сведения о том, какие приложения имеют повышенный риск или доверие, чтобы запускаться в вашей среде.

Отслеживайте, действуйте и показывайте результаты

Ivanti Endpoint Security для Endpoint Manager также предоставляет систему отчетов и активных графических панелей, которые помогут вам контролировать эффективность ваших усилий по обеспечению безопасности. К ним относятся подробные отчеты о соблюдении политики, уровнях соответствия, поведении пользователей, состоянии обновлений, предупреждениях об угрозах безопасности в режиме реального времени и многом другом.

Усовершенствуй безопасность с помощью объединённого ИТ

Как видно из названия, решение Ivanti Endpoint Security интегрируется с Ivanti Endpoint Manager и тем самым объединяет процессы защиты конечных точек и их управления. Это позволяет быстро автоматизировать внедрение как политик безопасности, так и политик ИТ-управления, что в итоге оптимизирует использование ИТ-ресурсов. Прозрачность всех действий по безопасности и управлению ИТ снижает риски и позволяет принимать более взвешенные решения.

В качестве дополнения для защиты от вредоносных программ, уже известных или выявляемых поведенческим анализом, можно использовать Ivanti Antivirus. Однако, если вы пользуетесь другим антивирусом, им также можно управлять через Ivanti Endpoint Security для Endpoint Manager.