Panda Endpoint Protection

Эволюция безопасности конечных устройств

РАЗВИТИЕ ИТ-СРЕД ПРЕДПРИЯТИЙ

За последние несколько лет быстрое развитие технологий, а также широкое применение Интернета, мобильных устройств и облачных систем хранения данных и приложений привело к настоящей революции в корпоративной среде. Впрочем, она не лишена рисков. Хотя эти преимущества и являются стимулом для развития предприятий, они также могут использоваться и кибер-преступниками.

Фактически, в 2020 году ежедневно регистрировалось[1] **свыше 350 000 новых вредоносных программ**. Хакеры нацелены на уязвимые конечные устройства, где предприятия имеют свои **самые ценные активы**. Причина? Как это часто бывает, ради экономической выгоды. **Вредоносные программы и шифровальщики** стали одними из самых распространенных угроз, хотя, как это ни парадоксально, прямой ущерб не всегда является основной проблемой - скорее, это **простои в работе**, к которым они приводят. В итоге компании **вынуждены предпринимать меры** по повышению уровня своей безопасности.

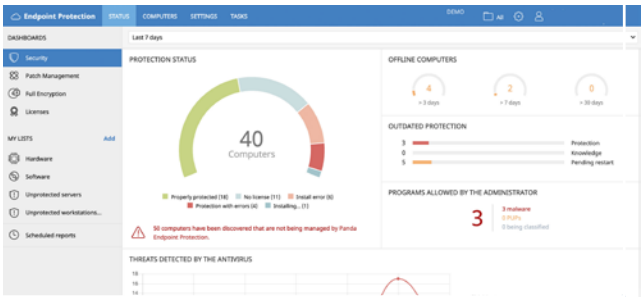
ЗАЩИТИТЕ ВАШУ КОМПАНИЮ ОТ ВРЕДОНОСНОГО ПО И ШИФРОВАЛЬЩИКОВ

Растущая подверженность компаний новым типам вредоносных программ и угроз ставит под угрозу их безопасность, требуя новых подходов, способных снизить воздействие возможных атак.

Panda Endpoint Protection - это эффективное облачное решение для обеспечения безопасности компьютеров, ноутбуков и серверов. Оно централизованно управляет безопасностью конечных устройств, расположенных как внутри, так и за пределами корпоративной сети.

Включает в себя набор EPP-технологий для предотвращения вредоносных программ, шифровальщиков и новых угроз. Решение в режиме реального времени сверяется с огромным репозиторием Panda Threat Intelligence, которое получает информацию от новейших алгоритмов машинного обучения, для оперативного обнаружения вредоносных атак.

Более того, нет необходимости в обслуживании аппаратного и программного обеспечения. Легкий агент решения не влияет на производительность конечных устройств, упрощая управление безопасностью и повышая эффективность работы.



[1] **AV-Test:** https://www.av-test.org/en/statistics/malware/

ПРЕИМУЩЕСТВА

Мультиплатформенная защита

- Защита от известных и неизвестных угроз: обнаруживает и блокирует вредоносное ПО, трояны, фишинг и шифровальщики.
- Защита всех векторов атак: браузеры, почта, файловые системы и внешние подключенные устройства.
- Автоматический анализ и лечение компьютеров.
- Поведенческий анализ для обнаружения известных и неизвестных вредоносных программ.
- Кросс-платформенная безопасность: системы Windows, Linux, macOS, Android и виртуальные среды (VMware, Virtual PC. MS Hyper-V, Citrix). Управление лицензиями, принадлежащими постоянным и непостоянным объектам виртуальной инфраструктуры (VDI).

Простое управление

- Просто обслуживать: для внедрения решения не требуется специальная инфраструктура. В этом случае ИТ-отдел может сосредоточиться на более важных задачах.
- Просто защищать удаленных пользователей: каждый компьютер, защищенный решением Panda Endpoint Protection, связывается с облаком, а потому можно быстро и легко защищать удаленные офисы и пользователей без дополнительной инфраструктуры.
- Просто внедрять: доступно несколько способов внедрения с автоматическим удалением других антивирусных продуктов для быстрого перехода с предыдущих решений.
- Легко освоить: простая в управлении и интуитивно понятная веб-консоль с доступом к основным опциям за один клик.

Низкое влияние на производительность

- Локальные агенты требуют минимального использования ресурсов процессора, памяти и сети, т.к. все операции выполняются в облаке.
- Не требует установки, обслуживания и управления новыми аппаратными ресурсами в ИТ-инфраструктуре предприятия.

ЦЕНТРАЛИЗОВАННАЯ ЗАЩИТА УСТРОЙСТВ

Централизованное управление безопасностью и обновлениями продукта для всех рабочих станций и серверов через обычный веб-браузер. Управляйте защитой всех Ваших устройств с Windows, Linux, Mac OS X или Android через единую веб-консоль.

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО И ШИФРОВАЛЬЩИКОВ

Panda Endpoint Protection анализирует поведение и хакерские техники для обнаружения и блокировки известных и неизвестных вредоносных программ, шифровальщиков, троянов и фишинга.

panda
a WatchGuard brand

УЛУЧШЕННОЕ ЛЕЧЕНИЕ

При нарушении безопасности Endpoint Protection позволяет быстро восстановить пострадавшие компьютеры до их состояния перед инцидентом с помощью дополнительных средств лечения и карантина, который хранит подозрительные и удаленные файлы.

Также позволяет администраторам удаленно перезагружать компьютеры и серверы, если необходимо установить последние обновления продукта.

МОНИТОРИНГ В РЕАЛЬНОМ ВРЕМЕНИ И ОТЧЕТЫ

Веб-консоль предоставляет подробный мониторинг безопасности в реальном времени с помощью комплексных панелей и легко интерпретируемых графиков.

Автоматическое создание и отправка отчетов о статусе защиты, обнаружениях и нежелательном использовании устройств.

ГИБКАЯ НАСТРОЙКА ПРОФИЛЕЙ

Настройка требуемых политик безопасности для определенных профилей пользователей, чтобы к каждой группе пользователей применялись наиболее подходящие настройки безопасности.

ЦЕНТРАЛИЗОВАННЫЙ КОНТРОЛЬ УСТРОЙСТВ

Остановите угрозы и потерю данных, блокировав различные типы устройств ("флэшки", USB-модемы, веб-камеры, DVD/CD-устройства и т.д.), разрешив только конкретные устройства и типы действий (блокировка доступа, только чтение, запись).

ГИБКАЯ И БЫСТРАЯ УСТАНОВКА

Внедрение защиты по электронной почте со ссылкой для скачивания в письме, или прозрачно на выбранные устройства с помощью собственной утилиты распространения. Доступен MSI-инсталлятор, который совместим со сторонними утилитами (ActiveDirectory, Tivoli, SMS и пр.).

КАРАНТИН MALWARE FREEZER

Malware Freezer помещает обнаруженные угрозы в карантин на семь дней, а в случае ложного срабатывания он автоматически восстанавливает файл из карантина обратно в систему.

СООТВЕТСТВИЕ ISO 27001 И SAS 70. ДОСТУПНОСТЬ 24x7

Решение размещено на платформе Aether с полной гарантией защиты данных. Наши дата-центры сертифицированы в соответствии с ISO 27001 и SAS 70, позволяя нашим клиентам избегать дорогостоящих простоев в работе и вредоносных заражений.

ОБЛАЧНАЯ ПЛАТФОРМА УПРАВЛЕНИЯ

Aether Platform

Облачная платформа и консоль управления Aether, общая для всех решений Panda для конечных устройств, предлагают оптимальное управление расширенной адаптивной безопасностью как внутри сети, так и за ее пределами. Простота, гибкость, детализация и масштабируемость.

Больше и быстрее. Простое внедрение

- Внедрение, установка и настройка за считанные минуты. Максимальная ценность с первого дня.
- Единый легкий агент для всех продуктов и всех платформ (Windows, Mac, Linux и Android).
- Автоматическое обнаружение незащищенных устройств. Удаленная установка
- Собственные технологии прокси, репозитория/кэша. Оптимальные коммуникации даже с устройствами без подключения к Интернету.

Простота управления. Адаптация к Вашей компании

- Интуитивно понятная веб-консоль. Гибкое и модульное управление, снижающее полную стоимость владения.
- Роли пользователей с полными или ограниченными правами. Журналы активностей.
- Политики безопасности по устройствам и группам. Предустановленные и настраиваемые роли.
- Инвентаризация "железа" и ПО. Журналы изменений.

Легкое масштабирование возможностей управления и безопасности

- Для внедрения новых модулей не требуется новая инфраструктура. Нет расходов на внедрение.
- Связь с конечными устройствами в реальном времени из единой веб-консоли.
- Панели контроля и индикаторы для каждого модуля.

Совместимые решения на платформе Aether:

Panda Endpoint Protection Panda Endpoint Protection Plus

Рабочие станции и серверы Windows:
http://go.pandasecurity.com/endpoint-windows/requirements

Устройства macOS:
http://go.pandasecurity.com/endpoint-macos/requirements

Рабочие станции и серверы Linux:
http://go.pandasecurity.com/endpoint-linux/requirements

Мобильные устройства Android:
http://go.pandasecurity.com/endpoint-android/requirements

WatchGuard

В МИРЕ +1 (206) 613-08-95 В РОССИИ И СНГ +7 (495) 105-94-51 watchguard.com | pandasecurity.com | cloudav.ru