Panda Adaptive Defense 360

Автоматизированная расширенная защита

Положите конец кибер-угрозам

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЙ

Конечные устройства являются основной мишенью для большинства кибер-атак, и по мере усложнения технологической инфраструктуры организации пытаются найти специалистов и ресурсы, необходимые для мониторинга и управления рисками безопасности конечных устройств. Итак, с какими проблемами сталкиваются компании при внедрении решений для обеспечения их безопасности?

- **Усталость от оповещений**: организации в неделю получают тысячи предупреждений об угрозах, из которых только 19% заслуживают доверия и только 4% из них когда-либо расследовались. 2/3 времени администраторов посвящено управлению оповещениями.
- **Сложность**: специалистам по ИБ часто трудно управлять слишком большим количеством инструментов с различными технологиями в силу недостатка собственных навыков и времени, необходимого для выявления угроз.
- **Низкая производительность**: часто решения для ИБ конечных устройств требуют установки и управления несколькими локальными агентами на каждом защищаемом компьютере, сервере и ноутбуке, что приводит к серьезным ошибкам, низкой производительности и высокому потреблению ресурсов.

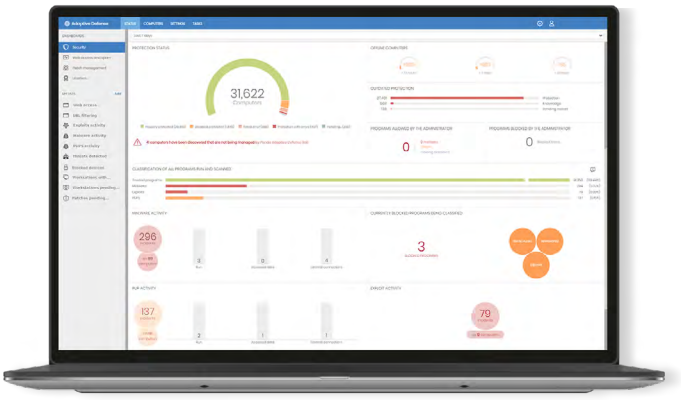
Традиционные технологии защиты конечных устройств, ориентированные на предотвращение заражения, применимы для известных угроз и вредоносного поведения, но их недостаточно для защиты от сложных кибер-угроз. Хакеры используют новые векторы заражения и создают новые угрозы, чтобы уклонобойти средства защиты и использовать возникающие слабые места.

ОТ ПРЕДОТВРАЩЕНИЯ К РЕАГИРОВАНИЮ – АВТОМАТИЗИРОВАННАЯ ЗАЩИТА УСТРОЙСТВ

Panda Adaptive Defense 360 - это инновационное облачное решение информационной безопасности компьютеров, ноутбуков и серверов. Оно автоматизирует процессы предотвращения, обнаружения, сдерживания и реагирования на любые современные и перспективные сложные угрозы, угрозы нулевого дня, шифровальщики, фишинг, эксплойты в памяти, безфайловые атаки и атаки, не использующие вредоносные программы, внутри и за пределами корпоративной сети.

В отличие от других решений, сочетает в себе широчайший спектр технологий защиты конечных устройств (EPP) с функциями автоматического обнаружения и реагирования (EDR). Предлагает два интегрированных управляемых экспертами по безопасности Panda сервиса:

- **Zero-Trust Application Service**: 100% классификация приложений
- **Threat Hunting Service**: обнаружение хакеров и инсайдеров



Panda Adaptive Defense 360 сочетает в себе традиционные технологии защиты конечных устройств (EPP) с инновационными технологиями адаптивной защиты, обнаружения и реагирования (EDR), что позволяет ИТ-специалистам справляться с передовыми кибер-угрозами.

Традиционные превентивные технологии защиты

- Персональный или управляемый файервол (IDS)
- Контроль устройств
- Коллективный разум
- Белые списки / черные списки
- Постоянная защита от вредоносного ПО и проверки по запросу
- Эвристика до выполнения процессов
- URL-фильтрация – веб-защита
- Антифишинг
- Анти-тамперинг
- Восстановление и откат

Расширенные технологии защиты

- Непрерывный мониторинг устройств с помощью EDR
- Облачный искусственный интеллект, обучающийся классифицировать 100% процессов (APT, шифровальщики, руткиты и т.д.)
- Песочницы в реальных окружениях
- Защита от эксплойтов
- Функции Threat Hunting, включая поведенческий анализ и обнаружение индикаторов атак IoA для обнаружения атак типа living off the land (LotL)
- Индикаторы атак в соответствии с матрицей MITRE ATT&CK
- Обнаружение и предотвращение RDP-атак
- Сдерживание и восстановление: изоляция компьютера, блокировка программ по хэшу или названию и т.д.

Поддерживаемые платформы и системные требования Panda Adaptive Defense 360

Поддерживаемые операционные системы:

Windows (Intel и ARM) | macOS | Linux | Android

Поддержка устаревших систем, начиная с Windows XP SP3 и Server 2003

Функции EDR доступны для Windows, macOS и Linux, причем для Windows эти функции предоставляются в полном объеме.

Список совместимых браузеров:

Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge и Opera

ПРЕИМУЩЕСТВА

Проще управлять, сильнее защита

- Его автоматизированные сервисы снижают расходы на высококвалифицированный персонал. Не надо управлять ложными срабатываниями, процессы автоматизированы.
- Не нужна локальная инфраструктура для установки, настройки и пр.
- Не влияет на производительность устройств, т.к. основано на легком агенте и облачной архитектуре.

Легко использовать и управлять

- Покрывает все потребности в защите конечных устройств простым управлением через единую веб-консоль.
- Легко внедрить и настроить на конечные устройства с разными операционными системами.
- Интуитивно понятный интерфейс управления, который можно быстро освоить.

Автоматизированные EDR-функции

- Обнаруживает и блокирует хакерские техники, тактики и процедуры, и эксплойты до возникновения проблем.
- Расследование и реагирование: экспертная аналитика для глубокого расследования каждой атаки и инструменты смягчения последствий.
- Отслеживаемость каждого действия: понятная видимость хакера и его действий, упрощающая расследование инцидента.

МОДУЛЬ НУЛЕВОГО ДОВЕРИЯ ZERO-TRUST: МНОГОУРОВНЕВАЯ ЗАЩИТА

Платформа Panda Aether не полагается только на одну технологию: мы интегрируем целый ряд технологий, снижая шансы хакеров на успех. Работая согласованно, эти технологии используют ресурсы на конечном устройстве, чтобы свести к нулю риск нарушения безопасности.

Модель Zero-Trust: многоуровневая защита

УРОВНИ КОНЕЧНОГО УСТРОЙСТВА:

Уровень 1 / Сигнатурные файлы и эвристические технологии
Эффективные оптимизированные технологии для обнаружения известных атак

Уровень 2 / Контекстные обнаружения
Позволяют обнаруживать безфайловые атаки и атаки, не использующие вредоносное ПО

Уровень 3 / Антиэксплойтная технология
Позволяет обнаруживать безфайловые атаки, использующие уязвимости

ОБЛАЧНЫЕ УРОВНИ

Уровень 4 / Zero-Trust Application Service
Обеспечивает обнаружение, если предыдущий уровень сообщил о нарушении, останавливает атаки на уже зараженные компьютеры и останавливает атаки с горизонтальным перемещением внутри сети

Уровень 5 / Threat Hunting Service
Позволяет обнаруживать скомпрометированные конечные устройства, ранние стадии атак, подозрительную активность и индикаторы атак (IoA)

Сигнатурные файлы и эвристические технологии, известные как традиционная защита конечных устройств (EPP), составляют уровень антивирусной технологии следующего поколения с высокой эффективностью против многих распространенных угроз низкого уровня. Они оптимизированы для обнаружения известных атак на основе сигнатур, общего и эвристического обнаружения, а также блокировки вредоносных URL-адресов.

Контекстное обнаружение является ключевым для обнаружения безфайловых атак и атак, не использующих вредоносное ПО, т.к. оно ищет анормальное использование ресурсов и приложений. Очень эффективно против скриптовых атак и атак, использующих программные средства ОС как PowerShell, WMI и т.д., уязвимости веб-браузеров и других используемых приложений (Java, Adobe...).

Антиэксплойтная технология обнаруживает безфайловые атаки, использующие уязвимости. Она ищет и обнаруживает аномальное поведение – верный сигнал эксплуатируемых процессов. Она критически важна для устройств, на которых ПО не обновлено или ожидает обновления (патчи), а также для устройств с теми ОС, которые больше не поддерживаются производителем.

Наш сервис Zero-Trust Application Service классифицирует 100% процессов, отслеживает активность конечных устройств и блокирует выполнение приложений и вредоносных процессов. В каждом случае в реальном времени и без неопределенности он отправляет локальному агенту свой результат классификации (вредоносное ПО или нет), при этом пользователю не требуется принимать решение и выполнять ручные процессы.

Сервис Threat Hunting основан на наборе правил поиска угроз, созданных специалистами по информационной безопасности, которые автоматически обрабатываются на основе всех данных, собранных с помощью телеметрии. Эти правила генерируют индикаторы атак (IoA) с высокой степенью достоверности и низким уровнем ложных срабатываний для минимизации MTTD (среднее время обнаружения) и MTTR (среднее время реагирования).

WatchGuard

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