Panda Adaptive Defense

Обнаружение и реагирование на атаки против конечных устройств

Endpoint Detection and Response (EDR)

panda
a WatchGuard brand

КИБЕР-ЗАЩИТА ПРОТИВ СЛОЖНЫХ УГРОЗ

Современные кибер-атаки предназначены для обхода защиты, обеспечиваемой традиционными решениями безопасности. Эти атаки становятся все более частыми и изощренными по мере того, как хакеры становятся более профессиональными. Их развитие также является результатом недостаточного внимания к исправлению уязвимостей в системах безопасности.

В свете этого сценария традиционные платформы защиты конечных устройств (EPP) не обеспечивают достаточно подробной информации о процессах и приложениях, запущенных в корпоративных сетях. Более того, некоторые EDR-решения не позволяют эффективно решать проблемы, но при этом создают дополнительный стресс и увеличивают рабочую нагрузку администратора безопасности, делегируя ответственность за управление предупреждениями и заставляя их вручную классифицировать угрозы.

ПОВЫСЬТЕ ВАШУ БЕЗОПАСНОСТЬ – ПЕРЕХОДИТЕ НА АВТОМАТИЧЕСКИЙ EDR

Panda Adaptive Defense - инновационное облачное решение информационной безопасности для 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.

Panda Adaptive Defense был создан для обеспечения полной видимости ваших конечных устройств путем мониторинга и выявления вредоносных действий, которые обходят традиционные решения. Решение устанавливается поверх существующих антивирусных решений и позволяет добавить полный набор возможностей EDR, включая следующие автоматизированные службы:

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

Решение предоставляет средства для эффективной борьбы с угрозами и реагирования на вредоносные атаки, используя следующие передовые технологии безопасности:

- 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
- Возможности сдерживания и восстановления, такие как изоляция компьютера и блокировка программ по хэшу или названию

ПРЕИМУЩЕСТВА

Упрощает процессы безопасности, снижает расходы

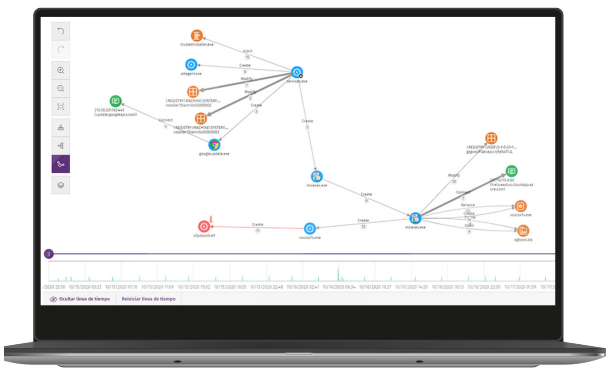
- Управляемые сервисы решения снижают расходы на высококвалифицированный персонал. Не надо управлять ложными срабатываниями, процессы автоматизированы.
- Управление всеми устройствами из единой веб-консоли.
- Не влияет на производительность устройств, т.к. основано на легком агенте и облачной архитектуре.

Автоматизирует и сокращает время обнаружения

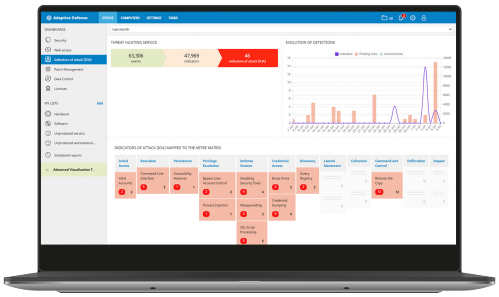
- Приложения, представляющие риск безопасности, могут быть заблокированы (по названию или хэшу).
- Блокирует запуск угроз, вредоносного ПО "нулевого дня", безфайловых атак и атак, не использующих вредоносное ПО, шифровальщиков и фишинга.
- Обнаруживает и блокирует хакерские техники, тактики и процедуры.

Автоматизирует и сокращает время реагирования и расследования

- Расследование и реагирование: экспертная аналитика для тщательного расследования каждой попытки атаки и инструменты для смягчения их последствий (лечение).
- Отслеживаемость каждого действия: понятная видимость хакера и его действий. Расширенное расследование индикаторов атак (IoA).
- Корректировки политик безопасности на основе выводов экспертного анализа.



ZERO-TRUST И THREAT HUNTING



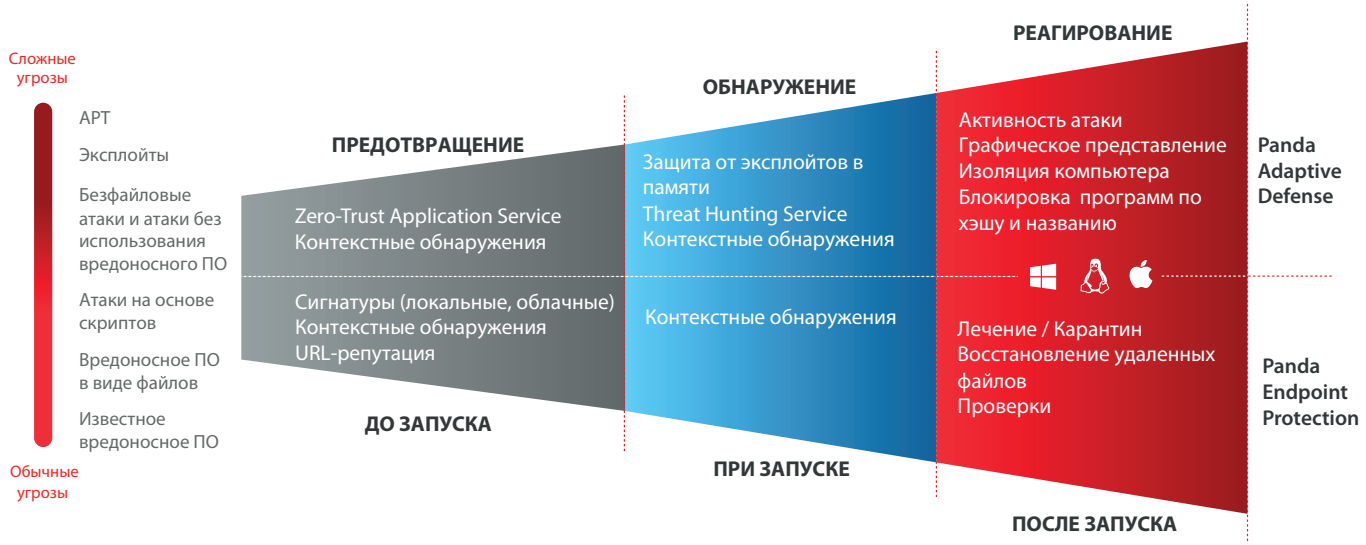
Платформа Panda Aether не полагается только на одну технологию: мы интегрируем целый ряд технологий, снижая шансы хакеров на успех. Работая согласованно, эти технологии используют ресурсы на конечном устройстве, чтобы свести к нулю риск нарушения безопасности.

Сервис Zero-Trust Application Service классифицирует 100% процессов, отслеживает активность на конечных устройствах и блокирует исполнение 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. Все это возможно благодаря мощности, скорости, адаптируемости и масштабируемости ИИ и облачной обработки.

Сервис объединяет технологии больших данных и многоуровневые методы машинного обучения, включая глубокое обучение, результаты непрерывного контроля и автоматизацию опыта и знаний, накопленных командой Panda по борьбе с угрозами.

Сервис поиска угроз 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).

Эти индикаторы атаки являются результатом непрерывного процесса выявления субъектов угроз с использованием расширенной аналитики данных, нашей собственной информации об угрозах и опыта наших аналитиков. Специалисты Threat Hunting в Panda Security исходят из того, что организации постоянно подвергаются риску.



Поддерживаемые платформы и системные требования Panda Adaptive Defense

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

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