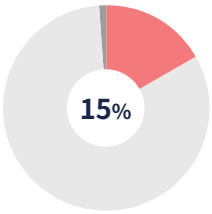
Panda Adaptive Defense 360 для партнеров

Переосмысливая свои сервисы информационной безопасности

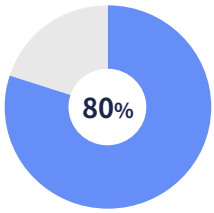
ПРОГНОЗЫ GARTNER[1] НА 2020:



15% всех **средних и крупных компаний** будут использовать **сервисы обнаружения и реагирования (EDR), управляемые провайдерами**.

15% к 2020 году

~1% сегодня



80% провайдеров сервисов ИБ в мире будут предлагать **управляемые сервисы обнаружения и реагирования (EDR).**

80% к 2020 году

ВОСПОЛЬЗУЙТЕСЬ ВОЗМОЖНОСТЬЮ

Провайдеры (MSP и MSSP) имеют возможность расширить свой набор услуг: теперь настало время действовать и помочь своим клиентам внедрить адаптированные под их нужды решения с расширенными возможностями защиты. EDR-решения с **автоматизированными управляемыми сервисами обнаружения атак и реагирования на них** - это самый быстрый и рентабельный инструмент, т.к. не требуются инвестиции в собственные технологии и экспертную поддержку, но при этом мгновенно создается дополнительная ценность для клиентов.

Panda Adaptive Defense 360 - это облачное решение ИБ для рабочих станций, ноутбуков и серверов, которое автоматизирует процессы предотвращения, обнаружения, сдерживания и реагирования на любые существующие и будущие сложные угрозы, неизвестное вредоносное ПО, шифровальщики, фишинг, эксплойты, работающие в памяти, и атаки, не использующие вредоносное ПО.

Решение отличается от других тем, что сочетает в себе широкий спектр **традиционных технологий защиты** конечных устройств (EPP) с **автоматизированными EDR-возможностями**, благодаря двум сервисам **под управлением экспертов Panda Security**:

- Zero-Trust Application Service
- Threat Hunting Service

Эти сервисы обеспечивают идентификацию угроз прежде, чем они смогут запуститься и причинить ощутимый ущерб всей компании.

РАСШИРЕННАЯ И АДАПТИВНАЯ ЗАЩИТА ДЛЯ КОНЕЧНЫХ УСТРОЙСТВ

Традиционная безопасность, основанная на обнаружении известных вредоносных процессов, уже не эффективна. Gartner призвала предприятия переходить от "реагирования на инцидент" к "непрерывному реагированию", чтобы предприятия постоянно стремились к обеспечению безопасности, т.к. конечные устройства постоянно находятся под угрозой со стороны злоумышленников.

Panda Adaptive Defense 360 усиливает четыре фазы архитектуры адаптивной безопасности Gartner[2]:

- **Предотвращение**: Модель останавливает запуск неизвестных процессов, пока они не будут одобрены технологиями Машинного обучения под наблюдением аналитиков и экспертов по вредоносному ПО.
- **Обнаружение**: Машинное обучение и мониторинг поведения процессов выявляют атаки, преодолевшие превентивные меры.
- **Реагирование и экспертный анализ**: Сдерживание атаки, предотвращение горизонтальных перемещений, устранение последствий, ответы на вопросы что, где и почему и т.д.
- **Прогноз атак**: Предугадывайте их, анализируйте тенденции, переходите от реактивного к проактивному подходу для сокращения поверхности атаки и охоте за угрозами.

ВОЗМОЖНОСТИ

Конечные устройства – новый периметр

Мобильность, процессинг и облачные хранилища произвели революцию в корпоративной среде. **Конечные устройства - новый периметр**. Решения безопасности на конечных устройствах должны быть **передовыми, адаптивными и автоматическими**, с высокими уровнями предотвращения обнаружения злоумышленников, которым рано или поздно удастся избежать превентивных мер. Такие решения также должны предлагать гибкие инструменты для оперативного реагирования, минимизации ущерба и сокращения поверхности атаки.

Профессионализация хакеров

Враги становятся изощреннее, их количество растет в результате повышения уровня профессионализма, доступности технологий и постоянных утечек данных.

Кибер-угрозы следующего поколения разрабатываются так, чтобы оставаться полностью незамеченными для традиционных решений безопасности, используя различные **хакерские техники** (например, использование легитимных программ для вредоносных целей).

Проблемы для организаций

Неавтоматизированные **EDR**-решения повышают **нагрузку**, требуя специальных ресурсов ИБ для сопоставления миллионов событий и анализа множества генерируемых оповещений, которые зачастую являются ложными. Такая помощь - скудная и дорогостоящая.

Компании ждут от своих поставщиков продукты, технологии и управляемые комплексные сервисы, которые делают расширенные и адаптивные системы безопасности жизнеспособными.

ПРЕПЯТСТВИЯ ДЛЯ ПАРТНЕРОВ

Многие провайдеры сервисов (MSP/MSSP) страдают от последствий **коммерциализации данного сектора с падением прибылей**. Они испытывают непрерывный переход клиентов к другим партнерам и (MSSP и SoC), которые предлагают сервисы расширенной ИБ на периметре, в сети и на самих конечных устройствах, используя собственные технологии и специализированные ресурсы, что требует серьезных первоначальных инвестиций.

Им также не хватает **видимости** и опыта мониторинга **устройств**.

[1] Gartner Market Guide for Managed Detection and Response Services. Toby Bussa, Craig Lawson, Kelly M. Kavanagh, Sid Deshpande.

[2] Designing an Adaptive Security Architecture for Protection from Advanced Attacks. Neil MacDonald and Peter Firstbrook - ID G00259490

Внедрение модели расширенной и адаптивной безопасности требует, среди прочего, идеальной синхронизации технологий и экспертов в области Больших данных, машинного обучения, анализа ИБ и автоматизированных средств реагирования и восстановления.

Panda Adaptive Defense 360 и его модули (Panda Patch Management, Panda Full Encryption, Panda Data Control и Advanced Reporting Tool) предоставляют инструменты, которые требуются нашим партнерам для развития своих сервисов расширенной безопасности конечных устройств без серьезных инвестиций.

На рисунке 1 ниже показаны некоторые сервисы расширенной и адаптивной безопасности, которые наши партнеры могут предлагать своим клиентам с помощью Panda Adaptive Defense 360 и его модулей.

ПРЕИМУЩЕСТВА ДЛЯ ПАРТНЕРОВ

- **Более широкий спектр** востребованных услуг, **конкурентное отличие** вашей компании.
- **Модернизация и допродажи клиентам**, повышение дохода с клиента, рост ARPU.
- **Улучшенные возможности предотвращения и обнаружения, мгновенное реагирование**, что снижает ваши операционные расходы на каждый инцидент. Рост прибыли.
- **Выше качество сервиса**, выше лояльность клиентов. Регулярные доходы.
- Инструменты для партнеров: **Panda Partner Center** и **Партнерская программа**.

Рис. 1. Управляемые сервисы наших партнеров, реализованные с помощью Panda Adaptive Defense 360 и его модулей в соответствии с архитектурой адаптивной безопасности Gartner.

ПАРТНЕРСКАЯ ПРОГРАММА

Мы предлагаем свою партнерскую программу для тех сервис-провайдеров, которые хотят предлагать своим клиентам глобальные сервисы и решения расширенной и адаптивной безопасности. Наши решения безопасности, признанные клиентами и аналитиками во всем мире, в сочетании с высокой доходностью и широким набором сервисов, представляют собой привлекательные и уникальные бизнес-возможности для наших партнеров. Подробнее: https://www.cloudav.ru/partners/

Преимущества программы:

- Обучение продажам
- Обучение техперсонала
- Сертификация
- Выделенный менеджер по работе с партнерами
- Маркетинговые материалы
- Маркетинговые кампании
- Портал для партнеров
- Совместные инициативы
- Лучшие решения по оценкам аналитиков и специалистов
- Широкий набор продуктов и сервисов
- Поддержка на русском языке
- Пулы лицензий. Доп. прибыли от объема
- Инструменты для улучшенного сервиса
- Доступ к партнерской консоли Panda
- NFR-лицензии (не для продажи)

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