Решения для защиты от атак и расследования нарушений

Инструменты и данные, позволяющие опережать хакеров

Panda Adaptive Defense 360

Современный ландшафт угроз сложен, а количество новых вирусов беспрецедентно. Для борьбы с этой новой реальностью требуются не только передовые ресурсы и технологии, но и способность управлять и тем, и другим. Помимо того, что сложные угрозы продолжают появляться в огромных количествах, существует еще и нехватка ИТ-специалистов и ИТ-бюджета для защиты от этих угроз.

Ответ Panda на эту проблему?

Panda Adaptive Defense 360 - это модель ИБ, основанная на трех принципах и предоставляемая в виде сервиса: непрерывный мониторинг приложений на компьютерах и серверах компании, автоматическая классификация с использованием машинного обучения на нашей облачной платформе больших данных и экспертный анализ команды Panda Threat Hunting для анализа тех приложений, которые не были классифицированы автоматически.

Скачать описание >

Panda Patch Management

Упростите управление уязвимостями для сокращения поверхности атак

Решение для управления обновлениями и патчами как для операционных систем, так и для сотен сторонних приложений. Усиливает возможности предотвращения, сдерживания и устранения угроз, сокращая поверхность атак на серверы и рабочие станции Windows.

Обеспечивает видимость состояния работоспособности конечных устройств в режиме реального времени с точки зрения уязвимостей, патчей или ожидающих обновлений, наличия неподдерживаемого ПО в режиме EOL. Обнаруживайте, планируйте, устанавливайте и осуществляйте мониторинг.

Скачать описание >

Panda Full Encryption

Усиление защиты от несанкционированного доступа

Один из наиболее эффективных способов защиты данных от утечки - это автоматическое шифрование жестких дисков рабочих станций, ноутбуков и серверов, обеспечивающее безопасность доступа к данным и соответствие внедренным механизмам аутентификации.

Использует BitLocker - проверенную и стабильную технологию Microsoft для шифрования и дешифрации дисков. Не влияет на работу конечных пользователей и предоставляет дополнительные возможности для централизованного контроля и управления ключами восстановления, хранящимися в облачной платформе управления Aether.

Скачать описание >

Advanced Reporting Tool

От данных к пониманию безопасности и эффективному ИТ

ИТ-персонал перегружен. Увеличение объема данных и сложные атаки приводят к тому, что упускаются из виду важные детали, что ставит под угрозу безопасность всей системы.

Panda Advanced Reporting Tool сопоставляет данные для автоматической генерации сведений по безопасности, обнаружения атак и необычного поведения, а также выявления недопустимого использования корпоративных систем сотрудниками компании.

Скачать описание >

Panda Email Protection

Облачная безопасность и фильтрация электронной почты

Плохая защиты почты может привести к атакам и заражению корпоративных систем, простоям в работе, недоступности сети, потери производительности и компрометации репутации компании.

Panda Email Protection является мощным почтовым файерволом, обеспечивающим высочайший уровень фильтрации почтового трафика в защищенных дата-центрах Panda для защиты от всех видов современных и перспективных угроз.

Скачать описание >

panda
a WatchGuard brand

	Расширенная защита		Традиционная защита		Управление	Защита и управление		Дополнительные модули			Почта
	Panda Adaptive Defense	Panda Adaptive Defense 360	Panda Endpoint Protection	Panda Endpoint Protection Plus	Panda Systems Management	Panda Fusion	Panda Fusion 360	Panda Patch Management	Panda Full Encryption	Advanced Reporting Tool	Panda Email Protection
УПРАВЛЕНИЕ											
Централизованное управление из единой администраторской веб-консоли*	■ [1]	■ [1]	■ [1]	■ [1]	■ [2]	■ [3]	■ [3]	■ [1]	■ [1]	■	■
Клиентская веб-консоль для конечных пользователей											■
Единый легкий агент на конечное устройство	■	■	■	■	■	2 агента	2 агента	■	■		
Установка через MSI-пакеты и загрузочные URL	■	■	■	■	■	■	■	■	■		
Установка собственными средствами веб-консоли	■	■	■	■		■	■	■	■		
Обнаружение неуправляемых устройств	■	■	■	■	■	■	■	■	■		
Поддержка сетевых устройств без Интернета	■ [4]	■ [4]	■ [4]	■ [4]	■ [5]	■ [4,5]	■ [4,5]	■ [4]	■ [4]	■ [4]	
Возможность локальных обновлений в сети	■ [6]	■ [6]	■ [6]	■ [6]		■ [6]	■ [6]	■ [6]	■ [6]		
Настраиваемые роли пользователей	■	■	■	■	■	■	■	■	■	■	■
Журнал активности пользователей в веб-консоли	■	■	■	■		■	■	■	■		
Коммуникации из консоли к компьютерам в реальном времени	■	■	■	■	■	■	■	■	■		
Настройка политик по группам и отдельным устройствам	■	■	■	■	■	■	■	■	■	■	■
Стандартные и настраиваемые панели, отчеты и оповещения в реальном времени	■	■	■	■	■	■	■	■	■	■	■
ЗАЩИТА, СОКРАЩЕНИЕ ПЛОЩАДИ АТАКИ											
Защита от вредоносных программ (вирусы, фишинг, шифровальщики, трояны и т.д.)	■	■	■	■		■	■				■
Защита от скриптов и вредоносных макросов в документах MS Office и т.д.	■	■	■	■		■	■				
Защита от сложных направленных атак до их запуска и во время запуска	■	■					■				
Защита от RDP-атак	■	■					■				
Персональный и управляемый файервол, IDS/HIPS**		■	■	■		■	■				
Анти-тампериング***	■	■	■	■		■	■				
Контроль устройств		■	■	■		■	■				
Блокировка нежелательных приложений	■	■					■				
Разрешенное ПО по хэшу или свойствам программы	■	■					■				
URL-фильтрация по категориям (веб-мониторинг)		■		■		■	■				
Анти-вор (Android): геолокация, удаленная блокировка/очистка, фото вора, сигнал тревоги		■	■	■		■	■				
Виртуальный патчинг неподдерживаемых систем	■	■					■				
Управление патчами и обновлениями для Windows и стороннего ПО					Только ОС	Только ОС	Только ОС	■			
Управление приложениями в EOL (End of Life)								■			
Исключение определенных патчей и ПО, откат патчей								■			
Централизованное отключение Windows Update								■			
Патчинг в реальном времени и по расписанию					■			■			
Шифрование/дешифрация дисков (BitLocker)									■		
Централизованное управление и восстановление ключей шифрования									■		
Централизованное применение политик шифрования									■		
Шифрование съемных запоминающих устройств									■		
Расширенные технологии защиты от спама											■
Расширенные техники антифишинга (антиспуфинг, SPF, DKIM, DMARC и т.д.)											■
Контент-фильтрация почты											■
Обязательные безопасные коммуникации (TLS) для выбранных получателей писем											■
Строгая проверка отправителей писем											■
ОБНАРУЖЕНИЕ											
Обнаружение неизвестных эксплойтов по поведению скомпрометированных процессов в памяти	■	■					■				
Обнаружение индикаторов атак (IoA) до их запуска	■	■	■	■		■	■				
Поведенческое и контекстное обнаружение IoA во время запуска	■	■					■				
Машинное обучение и глубокое обучение на статичных, динамичных и контекстных аттрибутах	■	■					■				
Zero-Trust Application Service: 100% классификация приложений	■	■					■				
Threat Hunting & Investigation Service: активный поиск, обнаружение и расследование угроз	■	■					■				
Обнаружение взломанных легальных приложений	■	■					■				

panda
a WatchGuard brand

	Расширенная защита		Традиционная защита		Управление	Защита и управление		Дополнительные модули			Почта
	Panda Adaptive Defense	Panda Adaptive Defense 360	Panda Endpoint Protection	Panda Endpoint Protection Plus	Panda Systems Management	Panda Fusion	Panda Fusion 360	Panda Patch Management	Panda Full Encryption	Advanced Reporting Tool	Panda Email Protection
МОНИТОРИНГ											
Мониторинг активности систем Windows, macOS, Linux	■	■					■			■	
Мониторинг устройств (с агентом и без него)					■	■	■				
Мониторинг компьютеров и серверов (CPU, память, VMI, журнал событий и т.д.)					■	■	■				
Мониторинг посещения сайтов		■		■		■	■				
Хранение данные в течение года для анализа атак	■	■					■			■	
СДЕРЖИВАНИЕ, РЕАГИРОВАНИЕ И ВОССТАНОВЛЕНИЕ											
Автоматизированное лечение и восстановление	■	■	■	■		■	■				
Сдерживание атаки из консоли: контролируемая изоляция компьютеров	■	■					■				
Сдерживание атаки из консоли: контролируемая перезагрузка компьютеров	■	■	■	■	■	■	■				
Централизованный карантин, доступный из списка обнаружений (Malware Freezer)	■	■	■	■		■	■				
Централизованный карантин, управляемый администратором или локальным пользователем											■
Бэкап входящей почты											■
Почтовый уведомитель на конечных устройствах											■
ЭКСПЕРТНЫЙ АНАЛИЗ											
Интеграция со сторонними SIEM-системами (опция)	■	■					■				
Жизненный цикл обнаружений, история выполнения процессов и экспертный анализ	■	■					■				
Сопоставление индикаторов атак матрице MITRE ATT&CK	■	■					■				
Экспорт экспертной информации в файл	■	■					■			■	
Панели, виджеты и предварительно настроенные запросы по KPI безопасности										■	
KPI по уязвимостям, установленным и запущенным приложениям										■	
KPI по необычному доступу к файлам с данными на конечных устройствах										■	
KPI по запуску приложений из "теневого" ИТ										■	
УДАЛЕННОЕ УПРАВЛЕНИЕ УСТРОЙСТВАМИ											
Инвентаризация "железа" и ПО	■	■	■	■	■	■	■				
Централизованная установка ПО и контроль лицензий					■	■	■				
Автоматизация задач и сценарии					■	■	■				
Магазин компонентов ComStore					■	■	■				
Тикетинг/Help Desk/Чат					■	■	■				
Удаленное управление (командная строка, передача файлов, службы и пр.)					■	■	■				
Подключение к удаленному рабочему столу					■	■	■				
ПОДДЕРЖКА ОПЕРАЦИОННЫХ СИСТЕМ											
Поддержка Windows Intel	■	■	■	■	■	■	■	■	■	■	
Поддержка Windows ARM	■	■	■	■		■	■	■	■	■	
Поддержка macOS, Linux	■	■	■	■	■	■	■			■[7]	
Поддержка виртуальных систем - постоянных и непостоянных (VDI)****	■	■	■	■		■	■				
Поддержка Android		■	■	■		■	■				

Модуль Advanced Reporting Tool доступен только для Adaptive Defense, Adaptive Defense 360 и пакета Fusion 360. Модули Patch Management и Full Encryption доступны для Endpoint Protection, Endpoint Protection Plus, Adaptive Defense, Panda Adaptive Defense 360, пакетов Fusion и Fusion 360.

* Единая облачная консоль: централизованное управление, доступное всегда и везде. Снижает расходы на инфраструктуру и обслуживание.
** Intrusion Detection System/Host-Based Intrusion Prevention System - Система обнаружения вторжений / Система предотвращений вторжений на уровне хоста.
*** Защита от несанкционированного вмешательства в работу решения Panda со стороны пользователей или процессов.
**** Совместимые системы со следующими типами виртуальных машин: VMWare Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp, XenServer, MS Virtual Desktop и MS Virtual Servers. Решения Panda Adaptive Defense 360 и Panda Fusion 360 совместимы с Citrix Virtual Apps, Citrix, Desktops 1906 и Citrix Workspace App for Windows. Panda Securtity верифицирована как партнер Citrix Ready.

1. Единая облачная консоль Aether для всех решений и модулей Panda Security для защиты конечных устройств
2. Облачная консоль Panda Systems Management
3. Облачная консоль Panda Cloud. Предоставляет доступ к консолям решений Systems Management, Endpoint Protection и Endpoint Protectoin Plus, Adaptive Defense и Adaptive Defense 360
4. Настройка встроенного прокси-сервера Panda в веб-консоли Aether
5. Настройка сетевых узлов в веб-консоли Panda Systems Management
6. Настройка кеш-компьютеров в веб-консоли Aether
7. Ограниченная телеметрия

WatchGuard

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

Решение	Описание	Клиент	Ключевые функции
Panda Adaptive Defense Panda Adaptive Defense 360	Комплексное решение безопасности, предоставляющее функции предотвращения, обнаружения и реагирования на любые виды угроз безопасности на рабочих станциях, серверах и ноутбуках внутри и за пределами корпоративной сети. Решение интегрирует все доступные технологии превентивной защиты (EPP) и передовые функции обнаружения атак и реагирования на них (EDR) в едином легком агенте. Плюс, решение предоставляет два уникальных на рынке управляемых сервиса безопасности, включенные в решение без дополнительных или скрытых расходов: 1. 100% Attestation Service для классификации всех приложений и процессов, запущенных на конечных устройствах 2. Threat Hunting Service против внешних хакерских и внутренних инсайдерских атак.	SB (26-100) MB (101- 500) LB (501-1000) KA (>1000)	· Технологии предотвращения, обнаружения и реагирования плюс управляемые сервисы безопасности против: 1)известных и неизвестных угроз (шифровальщики, трояны, черви, APT и пр.); 2) эксплойтов (атак через память) и атак с использованием административных утилит; 3) внешних хакерских и внутренних инсайдерских атак. · Машинное обучение в облачной среде Больших данных. · Управляемые сервисы безопасности без скрытых или дополнительных расходов · Видимость активности процессов и приложений в реальном времени. · Быстрое и прозрачное внедрение и установка. · Облачная веб-консоль централизованного управления. · Оповещения в реальном времени. Подробные отчеты для руководителей. ДОПОЛНИТЕЛЬНО В Panda Adaptive Defense 360 - Автоматизированное лечение. Инструменты удаленного восстановления и реагирования. - Файервол, IDS/IPS. - Контроль уст ройств и URL-фильтрация.
Panda Patch Management	Модуль для управления уязвимостями в Windows и приложениях под него. Полностью интегрирован во все решения для защиты конечных устройств. Позволяет в реальном времени централизованно видеть уязвимости в ПО, ожидаемые патчи, обновления и неподдерживаемое ПО (EOL). Прост в использовании для установки и контроля обновлений.	SB (26-100) MB (101- 500) LB (501-1000) KA (>1000)	· Управление патчами в Windows и сторонних приложениях · Патчи, сервис-паки, обновления и приложения с EOL · Интеграция функций обнаружения, изоляции и применения патчей · Откат примененных патчей
Advanced Reporting Tool	Дополнительный модуль для Panda Adaptive Defense [360], который предоставляет необходимые инструменты для обнаружения атак и аномального поведения, а также интеллектуальные технологии для формирования обоснованных выводов об ИТ-управлении и безопасности в компании.	SB (26-100) MB (101- 500) LB (501-1000) KA (>1000)	· Сохраняет и сопоставляет информацию по активности на конечных устройствах. · Мониторинг и визуализация данных в реальном времени и ретроспективе, позволяющие анализировать индикаторы безопасности и использование ресурсов кмпании, обнаруживать потенциальные риски и аномальное поведение. · Содержит панели мониторинга с ключевыми индикаторами, опции поиска и преднастроенные оповещения для трех направлений: 1) инциденты безопасности; 2) доступ к критической информации; 3) использование приложений и сетевых ресурсов
Panda Full Encryption	Использует BitLocker - проверенную и стабильную технологию Microsoft для шифрования и дешифрации дисков без влияния на работу конечных пользователей. Также позволяет централизованно контролировать и управлять ключами восстановления, хранящимися в облачной консоли управления Aether.	SoHo (6-25) SB (26-100) MB (101- 500)	· Полное шифрование/дешифрация жестких дисков с использованием BitLocker · Централизованное управление и восстановление ключей шифрования · Централизованное применение политик шифрования · Панели мониторинга шифрования, виджеты и отчеты
Panda Endpoint Protection	Кроссплатформенная защита для всех типов конечных устройств. Легкая, безопасная, полнофункциональная и простая в использовании.	SoHo (6-25) SB (26-100) MB (101- 500)	· Комплексная защита от вредоносного ПО. · Усовершенствованные инструменты лечения и восстановления. · Файервол с централизованным или персональным управлением. · IDS/IPS. · Контроль устройств. · Веб-консоль централизованного управления. · Подробные отчеты.
Panda Endpoint Protection Plus	Безопасность и производительность из облака всех конечных устройств и серверов Exchange.	SoHo (6-25) SB (26-100) MB (101- 500)	Все функции Endpoint Protection плюс мониторинг веб-доступа и URL-фильтрация
Panda Systems Management	Systems Management - это простой и доступный способ управления, мониторинга и поддержки всех устройств в вашей компании в любое время из любого места.	SoHo (6-25) SB (26-100) MB (101- 500) LB (501-1000)	· Инвентаризация и аудит аппаратного и программного обеспечения. · Непрерывный мониторинг. · Автоматизация задач. Шифрование. · Управление патчами и обновлениями. · Централизованное внедрение ПО. · Незаметная удаленная поддержка. · Подробные отчеты.
Panda Fusion	Интегрированное решение, предоставляющее безопасность, управление ИТ-активами и удаленную поддержку для всех ваших устройств в сети.	SoHo (6-25) SB (26-100) MB (101- 500)	Все функции Systems Management и Endpoint Protection Plus
Panda Fusion 360	Интегрированное решение, предоставляющее расширенную безопасность, управление ИТ-активами и удаленную поддержку для всех ваших устройств в сети.	SB (26-100) MB (101- 500) LB (501-1000))	Все функции Systems Management и Adaptive Defense 360
Panda Email Protection	Облачное решение для защиты электронной почты от вредоносного ПО и спама.	SB (26-100) MB (101- 500) LB (501-1000) KA (>1000)	· Антивирусная и антиспамовая защита · Контент-фильтр · Непрерывный доступ к почте через веб-почту · Резервное копирование входящей почты