Лекция 8: Защита конечных точек и систем

Тема: Технологии безопасности и защита инфраструктуры

Технический университет Молдовы

Лектор: Максим Масютин

Введение

Здравствуйте. Сегодня мы сосредоточимся на защите конечных точек и систем — технологиях безопасности, которые защищают устройства, на которых работают пользователи и хранятся данные. Именно здесь часто решается исход борьбы, поскольку конечные точки — это место, где люди взаимодействуют с технологиями, и это взаимодействие создает как возможности, так и риски.

Рассмотрим следующее: согласно отчёту Ponemon Institute, исследовательской компании в области информационной безопасности, State of Endpoint Security за 2025 год, более 70% нарушений безопасности начинаются на конечных точках. Будь то фишинговые письма, загрузка вредоносного ПО, скомпрометированные веб-сайты или зараженные USB-накопители — злоумышленники постоянно нацеливаются на конечные точки как на место входа. Получив закрепление на конечной точке, они продвигаются глубже в сеть.

Ландшафт безопасности конечных точек претерпел кардинальные изменения. Двадцать лет назад антивирус считался достаточной мерой — вы устанавливали обнаружение вредоносного ПО на основе сигнатур и надеялись на лучшее. Сегодня мы сталкиваемся с продвинутыми постоянными угрозами, или APT (Advanced Persistent Threat), бесфайловым вредоносным ПО, атаками с использованием штатных средств и изощренными программами-вымогателями. Традиционный антивирус совершенно неадекватен против этих угроз. Нам необходима эшелонированная защита, включающая обнаружение и реагирование на конечных точках, или EDR (Endpoint Detection and Response), хостовые средства безопасности, усиление защиты операционной системы, строгое управление обновлениями, управление мобильными устройствами и предотвращение утечки данных.

Давайте подробно рассмотрим каждую из этих областей.

Часть 1: Эволюция безопасности конечных точек

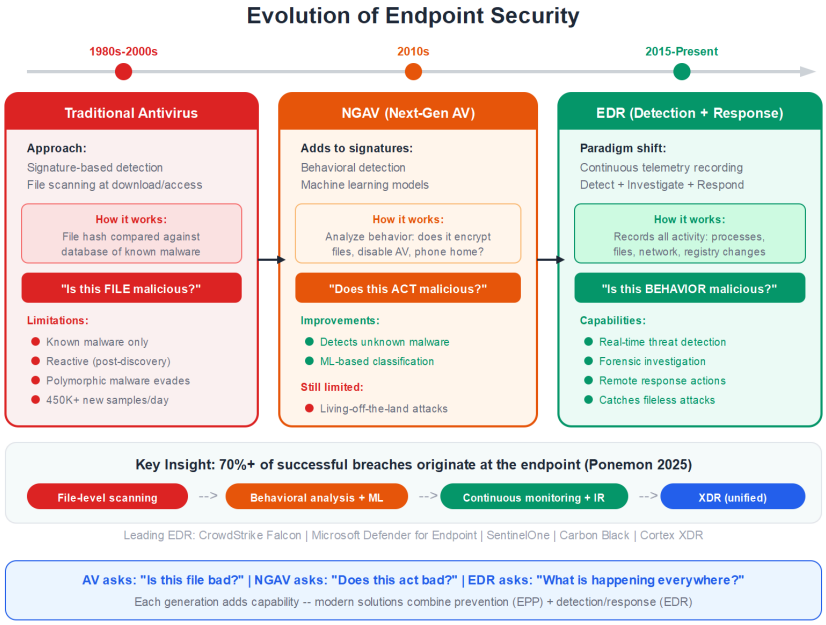

Рисунок 1: Эволюция защиты конечных точек: от антивируса к EDR

Прежде чем перейти к современным технологиям, давайте разберемся, как мы пришли к текущему состоянию дел. История безопасности конечных точек отражает эволюцию ландшафта угроз.

Традиционный антивирус появился в конце 1980-х годов, обнаруживая вредоносное ПО с помощью сигнатур — уникальных последовательностей байтов, идентифицирующих известные вредоносные файлы. Когда вы загружали файл, антивирус сравнивал его со своей базой данных сигнатур. Если сигнатура совпадала, файл помещался в карантин или удалялся.

Обнаружение на основе сигнатур работало достаточно хорошо, когда вредоносное ПО было редким и менялось медленно. Но злоумышленники адаптировались. Полиморфное вредоносное ПО изменяет свой код при каждом заражении, обходя статические сигнатуры. Объем вредоносного ПО резко возрос — производители средств безопасности ежедневно обнаруживают сотни тысяч новых образцов вредоносного ПО. Обнаружение на основе сигнатур не может за этим поспевать.

Антивирус нового поколения, или NGAV (Next-Generation Antivirus), добавил поведенческое обнаружение и машинное обучение. Вместо того чтобы просто искать известные вредоносные сигнатуры, NGAV анализирует поведение — пытается ли эта программа зашифровать файлы, отключить средства безопасности или подключиться к известным вредоносным серверам? Модели машинного обучения, обученные на миллионах образцов, способны идентифицировать вредоносное ПО, которое они никогда раньше не видели.

Но даже NGAV имеет ограничения. Изощренные злоумышленники используют легитимные системные инструменты для достижения вредоносных целей — техника, называемая "использованием штатных средств" (Living off the Land). PowerShell, WMI и другие инструменты администрирования могут загружать код, осуществлять горизонтальное перемещение и проводить эксфильтрацию данных без развертывания какого-либо вредоносного ПО. Нет вредоносного файла, который NGAV мог бы обнаружить.

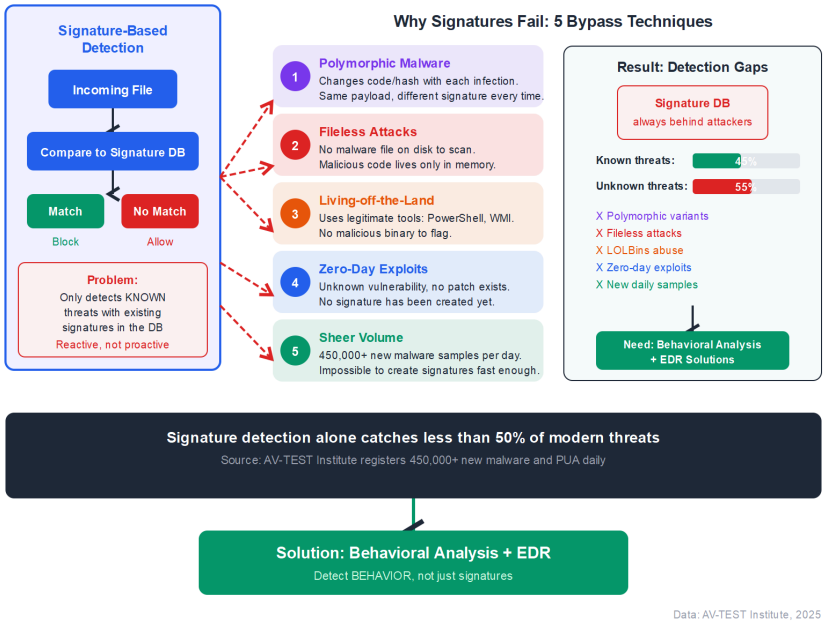

Рисунок 2: Почему сигнатурное обнаружение не справляется с современными угрозами

Именно здесь на сцену выходит обнаружение и реагирование на конечных точках.

Часть 2: Обнаружение и реагирование на конечных точках (EDR)

Обнаружение и реагирование на конечных точках (EDR) представляет собой современный уровень развития безопасности конечных точек. EDR выходит за рамки предотвращения, предоставляя возможности обнаружения, расследования и реагирования.

Основные возможности EDR

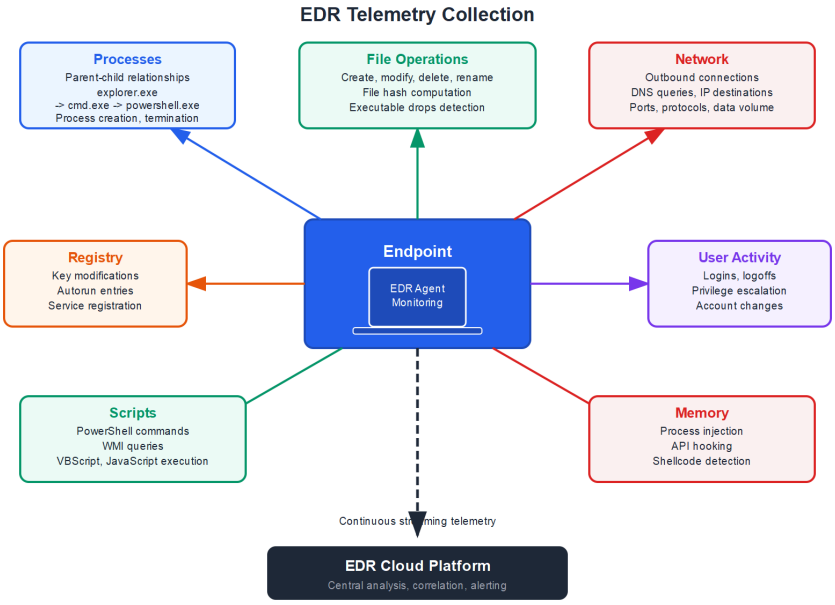

Рисунок 3: Телеметрия EDR: непрерывный сбор данных с конечных точек

Непрерывный мониторинг и запись — агенты EDR собирают обширную телеметрию с конечных точек, включая выполнение процессов, файловые операции, сетевые соединения, изменения реестра и многое другое. Эти данные передаются на центральную платформу и сохраняются для анализа. В отличие от традиционного антивируса, который проверяет файлы только в определенные моменты, EDR наблюдает за всем постоянно.

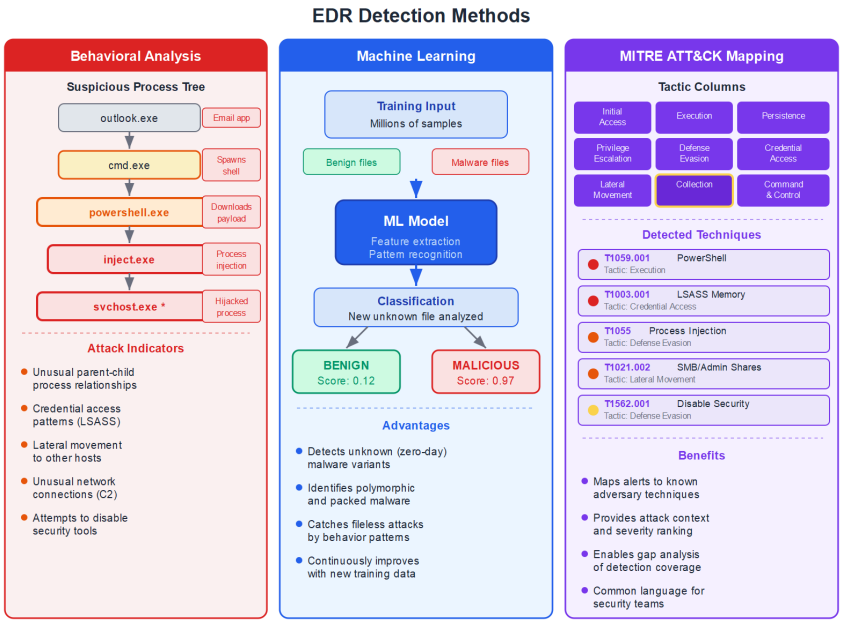

Рисунок 4: Методы обнаружения EDR: поведенческий анализ и аналитика угроз

Обнаружение угроз с использованием поведенческого анализа и машинного обучения — платформы EDR анализируют собранную телеметрию для выявления вредоносной активности. Они ищут индикаторы атак: подозрительные отношения "родительский-дочерний" между процессами, необычные сетевые соединения, попытки отключить средства безопасности, паттерны доступа к учетным данным и сотни других сигналов. При обнаружении вредоносного поведения генерируется оповещение.

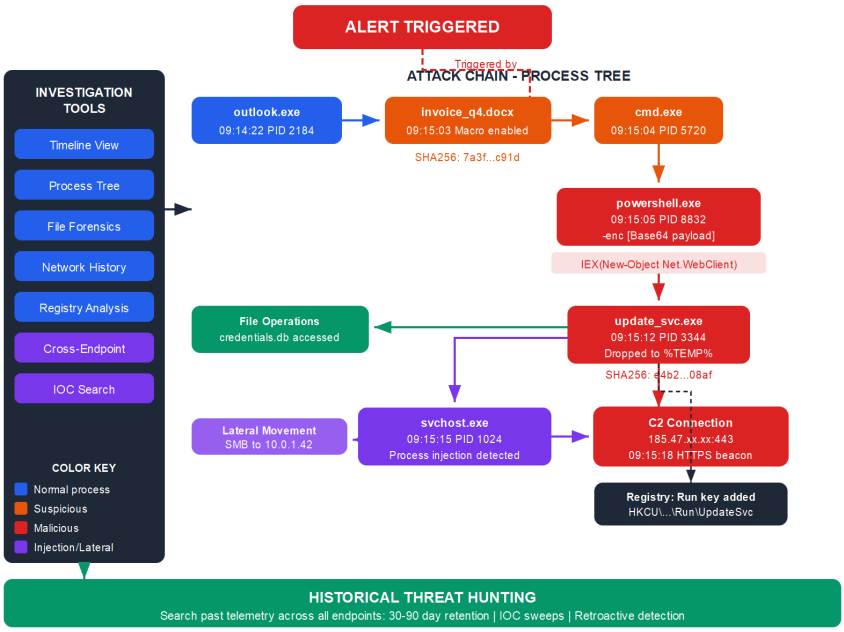

Рисунок 5: Расследование EDR: анализ первопричин и восстановление хронологии

Возможности расследования — когда срабатывает оповещение, аналитикам безопасности необходимо понять, что произошло. Платформы EDR обеспечивают видимость полной цепочки событий, предшествовавших оповещению и последовавших за ним. Какой процесс породил какой? К каким файлам был получен доступ? Какие сетевые соединения были установлены? Этот контекст позволяет аналитикам определить, представляет ли оповещение реальную угрозу, и понять ее масштаб.

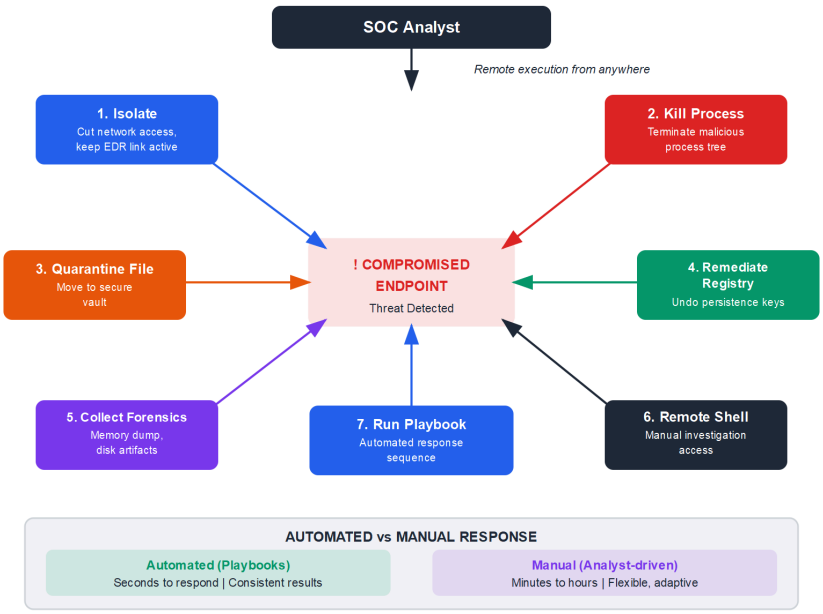

Рисунок 6: Действия реагирования EDR: возможности изоляции и устранения

Действия по реагированию — EDR позволяет специалистам по реагированию предпринимать немедленные действия: изолировать конечную точку от сети, завершить вредоносные процессы, удалить вредоносные файлы, собрать криминалистические артефакты и многое другое. Эти действия могут выполняться удаленно, обеспечивая быстрое реагирование независимо от местонахождения конечной точки.

EDR в сравнении с традиционным антивирусом

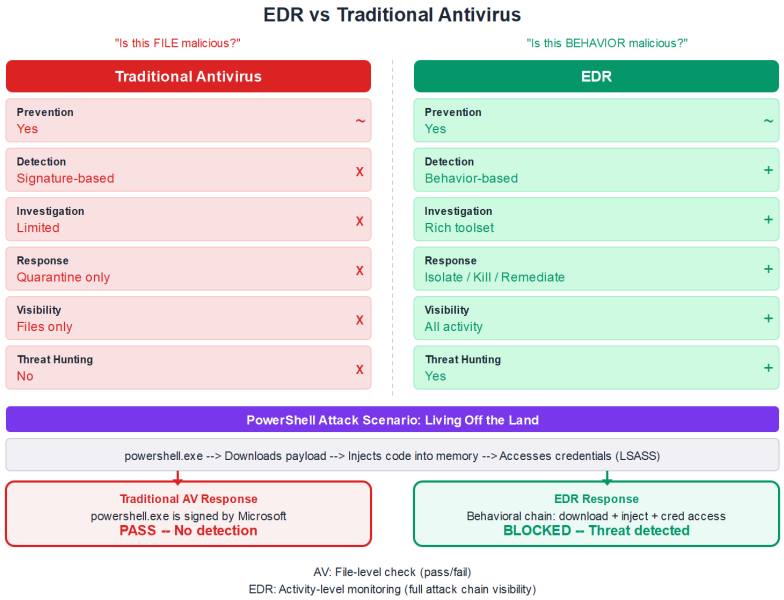

Рисунок 7: EDR и традиционный антивирус: сравнение возможностей

Различие между EDR и традиционным антивирусом принципиально. Антивирус задает вопрос: "Является ли этот файл вредоносным?" EDR задает вопрос: "Является ли это поведение вредоносным?" Антивирус работает на уровне файлов; EDR работает на уровне активности.

Рассмотрим атаку на основе PowerShell. Традиционный антивирус может проверить powershell.exe и признать его легитимным (потому что так и есть). Атака продолжается. EDR наблюдает, как PowerShell загружает данные с подозрительного URL, как эти данные внедряют код в другой процесс, и как этот процесс пытается получить доступ к учетным данным. Вредоносного файла не существует, но вредоносное поведение обнаружено и остановлено.

EDR также даёт историческую видимость. Если вы обнаружите компрометацию сегодня, вы можете выполнить поиск по телеметрии EDR, чтобы понять, когда она началась и что произошло. Традиционный антивирус не предоставляет такой возможности.

Ведущие решения EDR

Рынок EDR значительно созрел. К ведущим производителям относятся:

CrowdStrike, разработчик решений кибербезопасности, Falcon — облачная платформа, известная своим легковесным агентом и мощными возможностями обнаружения. CrowdStrike первой внедрила концепцию "предполагай нарушение" и предлагает обширную интеграцию с аналитикой угроз.

Microsoft Defender for Endpoint — интегрированный с Windows и более широкой экосистемой безопасности Microsoft. Особенно эффективен для организаций, активно использующих технологии Microsoft.

Компания SentinelOne, разработчик решений безопасности конечных точек, известна возможностями автономного реагирования, способными сдерживать угрозы без вмешательства человека.

Платформа Carbon Black (подразделение VMware) эффективна в корпоративных средах благодаря обширному хранению исторических данных и возможностям проактивного поиска угроз.

Palo Alto Networks Cortex XDR — выходит за рамки конечных точек, интегрируя сетевые и облачные данные в единую платформу обнаружения.

Аспекты развертывания EDR

Развертывание EDR требует тщательного планирования. Агент должен быть установлен на всех конечных точках — ноутбуках, настольных компьютерах, серверах. Неполное развертывание создает слепые зоны, которые злоумышленники найдут и используют.

EDR генерирует значительные объемы данных. Необходимо планировать требования к хранению и пропускной способности сети. Облачные решения EDR решают этот вопрос автоматически; локальные решения требуют инвестиций в инфраструктуру.

Объем оповещений может быть чрезмерным. Платформы EDR обнаруживают больше, чем традиционный антивирус, включая множество безобидных действий, которые выглядят подозрительно. Настройка и приоритизация оповещений необходимы, чтобы не перегружать команды безопасности.

EDR требует квалифицированных аналитиков для реализации своего полного потенциала. Платформа предоставляет видимость и инструменты, но именно люди должны расследовать оповещения, проводить проактивный поиск угроз и принимать решения о реагировании. Команды с недостаточным штатом могут обращаться с EDR как с дорогим антивирусом, упуская его истинный потенциал.

Часть 3: Хостовые средства безопасности

Помимо EDR, многочисленные хостовые средства безопасности защищают конечные точки.

Хостовые межсетевые экраны

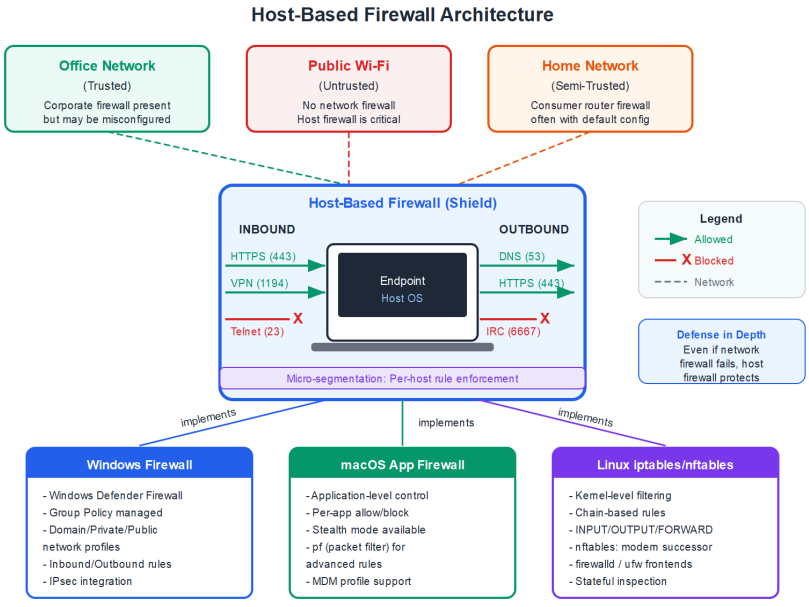

Рисунок 8: Межсетевой экран на хосте: контроль сетевого доступа по приложениям

Каждая современная операционная система включает межсетевой экран. Windows Firewall, межсетевой экран приложений macOS и iptables/nftables в Linux

контролируют сетевой трафик на конечной точке. Эти межсетевые экраны должны быть включены и настроены на блокировку ненужных входящих соединений.

Хостовые межсетевые экраны обеспечивают эшелонированную защиту. Даже если сетевые межсетевые экраны неправильно настроены или обойдены, хостовые межсетевые экраны обеспечивают дополнительный уровень защиты. Они особенно важны для мобильных устройств, подключающихся к ненадежным сетям.

Расширенные конфигурации могут реализовать микросегментацию на уровне конечной точки. Например, Windows Firewall с расширенной безопасностью может ограничивать соединения на основе пользователя, приложения и направления, создавая гранулярные сетевые контроли.

Контроль приложений

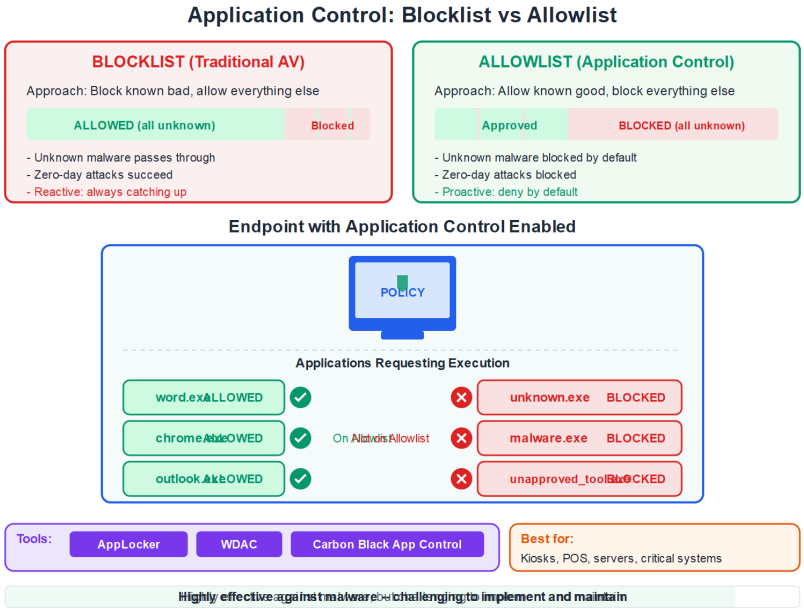

Рисунок 9: Контроль приложений: подходы на основе белых и чёрных списков

Контроль приложений, также называемый белым списком приложений, предотвращает выполнение неавторизованных приложений. Вместо попыток идентифицировать вредоносное ПО (заведомо проигрышная стратегия), контроль приложений определяет, какое программное обеспечение разрешено, и блокирует все остальное.

Этот подход высокоэффективен против вредоносного ПО. Если могут выполняться только одобренные приложения, вредоносное ПО не сможет запуститься, даже если оно достигнет конечной точки. Однако контроль приложений сложен в реализации. Необходимо провести инвентаризацию всех легитимных приложений, поддерживать актуальность белого списка по мере обновления программ и обрабатывать исключительные случаи, когда пользователям требуются программы, отсутствующие в списке.

Microsoft AppLocker и Windows Defender Application Control (WDAC) обеспечивают контроль приложений для Windows. macOS включает аналогичные возможности через Gatekeeper и профили MDM (Mobile Device Management, управление мобильными устройствами). Корпоративные решения, такие как Carbon Black App Control, обеспечивают централизованное управление.

Контроль приложений наиболее практичен для конечных точек с фиксированными функциями (киоски, POS-терминалы (Point of Sale, точка продажи)), где набор программ стабилен. Для рабочих станций общего назначения может потребоваться более гибкий подход.

Управление привилегиями конечных точек

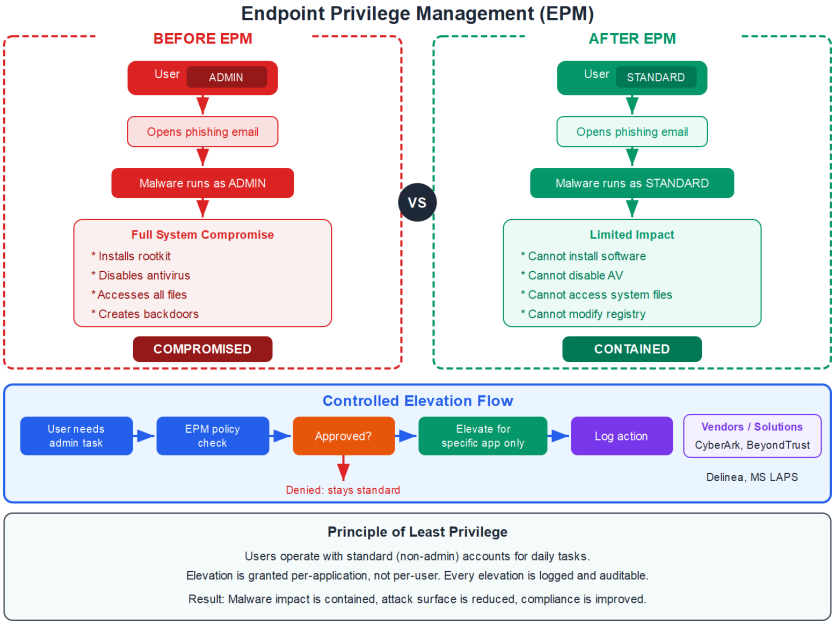

Рисунок 10: Управление привилегиями конечных точек: применение принципа минимальных привилегий

Управление привилегиями конечных точек, или EPM (Endpoint Privilege Management), контролирует административные привилегии на конечных точках. Большинству пользователей не нужны права администратора для повседневной работы, однако многие организации предоставляют локальные права администратора по умолчанию, поскольку это проще, чем управлять исключениями.

Работа с правами администратора существенно увеличивает риск. Вредоносная программа, выполняющаяся с правами администратора, может устанавливать руткиты, отключать средства безопасности и получать доступ к любым данным в системе. Та же вредоносная программа, выполняющаяся от имени стандартного пользователя, гораздо более ограничена в своих возможностях.

Решения EPM позволяют пользователям работать как стандартные пользователи, обеспечивая при этом контролируемое повышение привилегий для конкретных задач. Когда пользователю необходимо установить программу или внести изменения в систему, он может запросить повышение привилегий. Запрос может быть автоматически одобрен (для известных безопасных операций), требовать одобрения или быть отклонен в соответствии с политикой.

К ведущим производителям EPM относятся CyberArk, BeyondTrust и Delinea, производители решений управления привилегированным доступом. Решение Microsoft LAPS (Local Administrator Password Solution, решение для управления паролями локального администратора) решает часть проблемы путем управления паролями локальных администраторов.

Безопасная конфигурация

Безопасная конфигурация обеспечивает развертывание конечных точек с настройками, соответствующими требованиям безопасности. Конфигурации по умолчанию часто отдают приоритет удобству, а не безопасности — включены ненужные службы, разрешены небезопасные протоколы, допускается слабая аутентификация.

Стандарты безопасности от таких организаций, как Центр интернет-безопасности, или CIS (Center for Internet Security), предоставляют руководства по безопасной конфигурации. Стандарты конфигурации CIS существуют для Windows, macOS, Linux и многих других платформ, предоставляя конкретные настройки и их обоснование с точки зрения безопасности.

Инструменты управления конфигурацией, такие как Microsoft Intune, JAMF, Ansible и Puppet, могут обеспечивать применение безопасных конфигураций в масштабе. Регулярные аудиты подтверждают, что конфигурации остаются соответствующими требованиям, и обнаруживают несанкционированные изменения.

Часть 4: Усиление защиты операционной системы

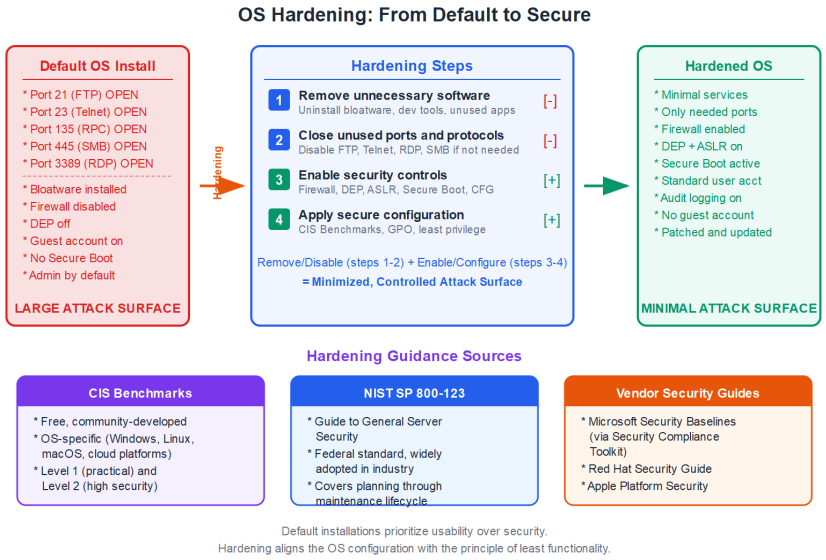

Рисунок 11: Укрепление операционной системы: сокращение поверхности атаки

Усиление защиты операционной системы сокращает поверхность атаки путем отключения ненужных функций и включения средств безопасности.

Сокращение поверхности атаки

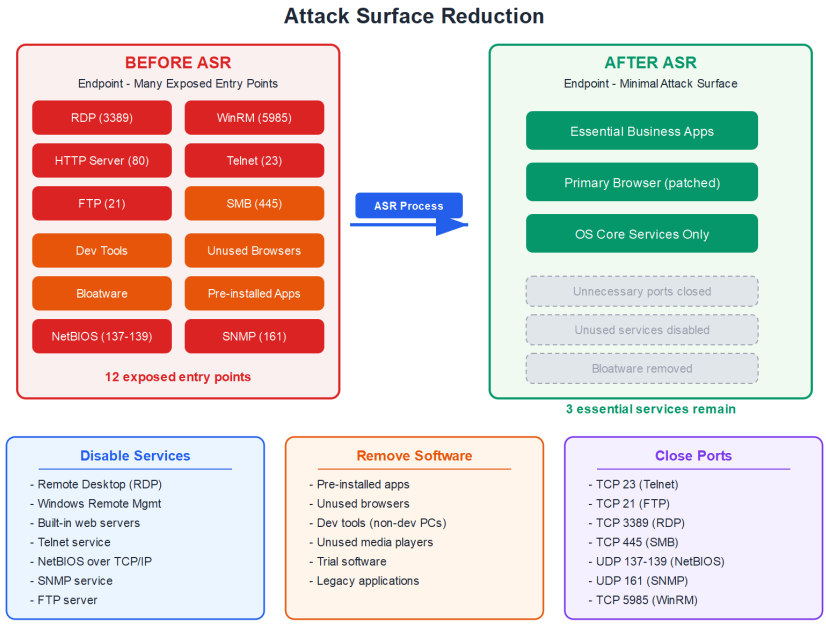

Рисунок 12: Сокращение поверхности атаки: отключение ненужных функций и служб

Сокращение поверхности атаки, или ASR (Attack Surface Reduction), ограничивает способы, которыми злоумышленники могут скомпрометировать системы. Каждая включенная служба, установленное приложение и открытый порт — это потенциальный вектор атаки. Их сокращение снижает риск.

Отключение ненужных служб — стандартные установки операционных систем включают службы, которые большинству пользователей никогда не понадобятся. Удаленный рабочий стол, удаленное управление Windows, встроенные веб-серверы и другие службы создают поверхность атаки. Отключайте то, что вам не нужно.

Удаление ненужных программ — предустановленные приложения, плагины браузера и другие программы накапливаются со временем. Каждое приложение — это потенциальная поверхность атаки. Проводите аудит установленных программ и удаляйте то, что не требуется.

Закрытие ненужных портов — сетевые порты должны быть открыты только при необходимости. Регулярное сканирование портов выявляет неожиданно открытые порты, которые следует закрыть.

Windows включает правила сокращения поверхности атаки, которые блокируют конкретные техники, используемые вредоносными программами и эксплойтами. Эти правила могут блокировать создание дочерних процессов приложениями Office, предотвращать запуск исполняемого содержимого из электронной почты, блокировать запуск загруженных исполняемых файлов JavaScript и VBScript и многое другое.

Защита от эксплойтов

Современные операционные системы включают технологии защиты от эксплойтов, которые затрудняют атаки даже при наличии уязвимостей.

Рандомизация размещения адресного пространства, или ASLR (Address Space Layout Randomization), делает случайными адреса памяти, по которым загружаются программы и библиотеки. Многие эксплойты зависят от знания точных адресов памяти — ASLR делает эти адреса непредсказуемыми, нарушая работу многих эксплойтов.

Предотвращение выполнения данных, или DEP (Data Execution Prevention), помечает области памяти как неисполняемые, предотвращая выполнение кода из областей, предназначенных только для данных. Это блокирует многие эксплойты переполнения буфера, которые внедряют и выполняют код.

Защита потока управления, или CFG (Control Flow Guard), и технология контроля потока выполнения, или CET (Control-flow Enforcement Technology), предотвращают перехват злоумышленниками потока выполнения программы. Эти технологии проверяют, что косвенные вызовы и переходы направлены на допустимые участки кода.

Безопасная загрузка (Secure Boot) гарантирует, что при запуске системы загружается только доверенные программы. Прошивка UEFI (Unified Extensible Firmware Interface, унифицированный расширяемый интерфейс встроенного ПО) проверяет подписи загрузчика перед выполнением, предотвращая руткиты и буткиты, которые пытаются загрузиться до операционной системы.

Windows Defender Exploit Guard предоставляет настраиваемую защиту от эксплойтов, включая ASLR, DEP и дополнительные механизмы защиты. Включайте эти средства защиты для всех приложений, уделяя особое внимание часто атакуемым программам, таким как браузеры и средства просмотра документов.

Безопасная загрузка и измеренная загрузка

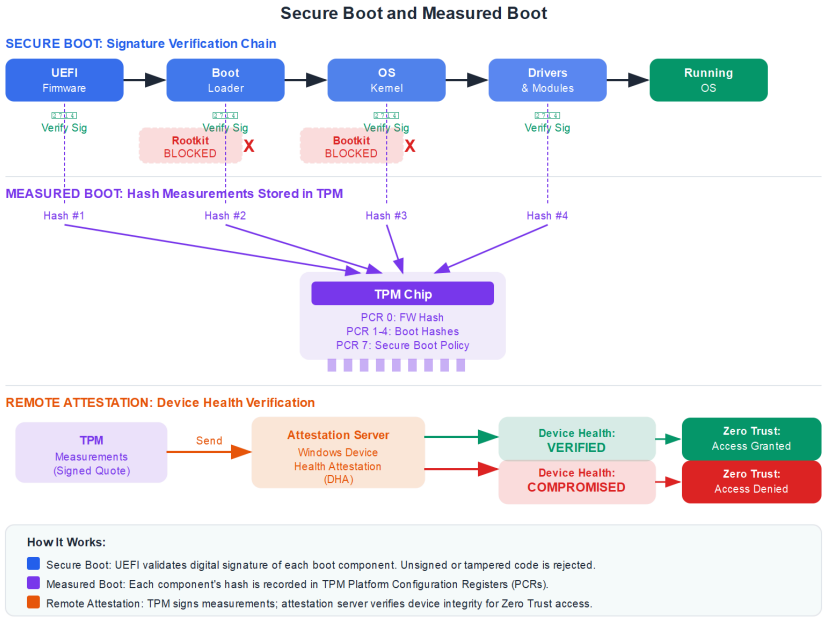

Рисунок 13: Secure Boot: цепочка проверки целостности прошивки

Безопасная загрузка (Secure Boot), упомянутая выше, проверяет, что компоненты загрузки подписаны доверенными организациями, прежде чем разрешить их выполнение. Это предотвращает вредоносные программы уровня загрузки, которые в противном случае загружались бы до средств безопасности.

Измеренная загрузка (Measured Boot) расширяет этот подход, записывая измерения (криптографические хеши) каждого компонента загрузки в доверенный платформенный модуль, или TPM (Trusted Platform Module, доверенный платформенный модуль). Эти измерения могут быть проверены удаленно (удаленная аттестация) для подтверждения того, что система загрузилась с ожидаемыми компонентами. Это обеспечивает реализацию сценариев нулевого доверия, где решения о доступе зависят от состояния здоровья устройства.

Windows Device Health Attestation использует измеренную загрузку для проверки состояния здоровья устройства перед предоставлением доступа к конфиденциальным ресурсам. Аналогичные возможности существуют для macOS и мобильных платформ.

Часть 5: Управление обновлениями

Управление обновлениями (Patch Management) — это процесс получения, тестирования и установки обновлений ПО. Несмотря на концептуальную простоту, управление обновлениями остается значительной проблемой для организаций.

Проблема установки обновлений

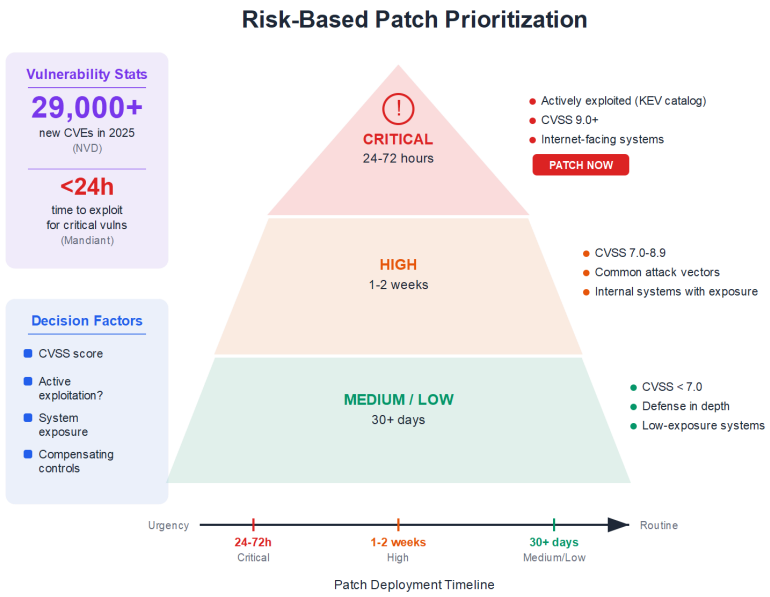

Рисунок 14: Приоритизация патчей: устранение уязвимостей на основе рисков

Уязвимости ПО обнаруживаются постоянно. В Национальной базе данных уязвимостей NIST (National Institute of Standards and Technology, Национальный институт стандартов и технологий) в 2025 году было зарегистрировано более 29 000 новых уязвимостей. Многие из них затрагивают программы, работающие на ваших конечных точках. Без установки обновлений ваши системы остаются уязвимыми для известных атак.

Окно между раскрытием уязвимости и активной эксплуатацией сократилось. По данным Mandiant (подразделение Google Cloud по кибербезопасности), в 2025 году среднее время до эксплуатации критических уязвимостей составляло менее 24 часов для наиболее серьёзных проблем. Злоумышленники отслеживают раскрытия уязвимостей и быстро разрабатывают эксплойты. Медленная установка обновлений означает длительную подверженность атакам.

Однако установка обновлений сопряжена с рисками. Обновления могут нарушить работу приложений, вызвать нестабильность системы или привести к появлению новых уязвимостей. Инцидент с CrowdStrike в 2024 году, когда дефектное обновление привело к сбою миллионов систем Windows, наглядно продемонстрировал, что обновления могут быть опасны.

Процесс управления обновлениями

Эффективное управление обновлениями следует структурированному процессу:

Обнаружение и инвентаризация — вы не можете обновить то, о чем не знаете. Поддерживайте точный учет всего оборудования, программ и конфигураций. Инструменты обнаружения активов сканируют сети для идентификации систем и установленных программ.

Оценка и приоритизация — не все обновления одинаково срочны. Критические обновления безопасности, устраняющие активно эксплуатируемые уязвимости, требуют немедленного внимания. Функциональные обновления и незначительные исправления могут подождать. Используйте оценки серьёзности уязвимостей по шкале CVSS (Common Vulnerability Scoring System, общая система оценки уязвимостей) и аналитику угроз для приоритизации.

Тестирование — перед широким развертыванием тестируйте обновления в репрезентативной среде. Убедитесь, что критически важные для бизнеса приложения продолжают функционировать. Автоматизированное тестирование может ускорить этот процесс.

Развертывание — выпуск обновлений в производственные системы. Поэтапное развертывание снижает риск — сначала обновите подмножество систем, проверьте наличие проблем, затем расширьте охват. Современные инструменты развертывания могут автоматизировать этот процесс.

Проверка — убедитесь, что обновления были успешно применены. Сканируйте системы для выявления тех, которые остались без обновлений. Разберитесь с неудачными установками.

Инструменты управления обновлениями

Microsoft предоставляет несколько механизмов управления обновлениями. Windows Update доставляет обновления на отдельные системы. WSUS (Windows Server Update Services, службы обновления Windows Server) обеспечивает централизованное управление для сред Windows. Microsoft Intune обеспечивает облачное управление обновлениями, интегрированное с управлением конечными точками. Microsoft Configuration Manager (ранее SCCM, System Center Configuration Manager) обеспечивает управление обновлениями и конфигурацией корпоративного уровня.

Сторонние решения для управления обновлениями охватывают программы за пределами Windows. Qualys, разработчик решений управления уязвимостями, Ivanti, разработчик решений управления ИТ-инфраструктурой, ManageEngine, разработчик решений управления ИТ-услугами, и другие могут развертывать обновления для тысяч приложений в разнородных средах.

Сканеры уязвимостей, такие как Nessus (от Tenable, разработчика решений управления уязвимостями), Qualys VMDR и Rapid7, разработчик решений кибербезопасности, выявляют отсутствующие обновления в вашей среде, позволяя расставлять приоритеты на основе рисков.

Автоматическая установка обновлений

Автоматизация необходима для своевременной установки обновлений в масштабе. Современные подходы включают:

Автоматическое обновление Windows Update для конечных точек может обеспечить автоматическую актуальность систем потребителей и малого бизнеса. Предприятия обычно отключают автоматические обновления для сохранения контроля.

Инструменты оркестрации обновлений могут автоматически развертывать одобренные обновления во время окон обслуживания, управляя перезагрузками и проверками.

Подходы неизменяемой инфраструктуры, популярные в облачных средах, заменяют установку обновлений пересборкой. Когда необходимо обновление безопасности, создаются новые образы систем с включенным обновлением, и работающие системы заменяются, а не обновляются на месте. Это устраняет риск неудачных обновлений и обеспечивает согласованную конфигурацию.

Часть 6: Безопасность мобильных устройств

Мобильные устройства — смартфоны и планшеты — представляют уникальные вызовы безопасности. Они являются очень личными, постоянно подключены к сети и хранят конфиденциальные данные. Они подключаются к ненадежным сетям, запускают приложения из публичных магазинов и легко могут быть потеряны или украдены.

Ландшафт мобильных угроз

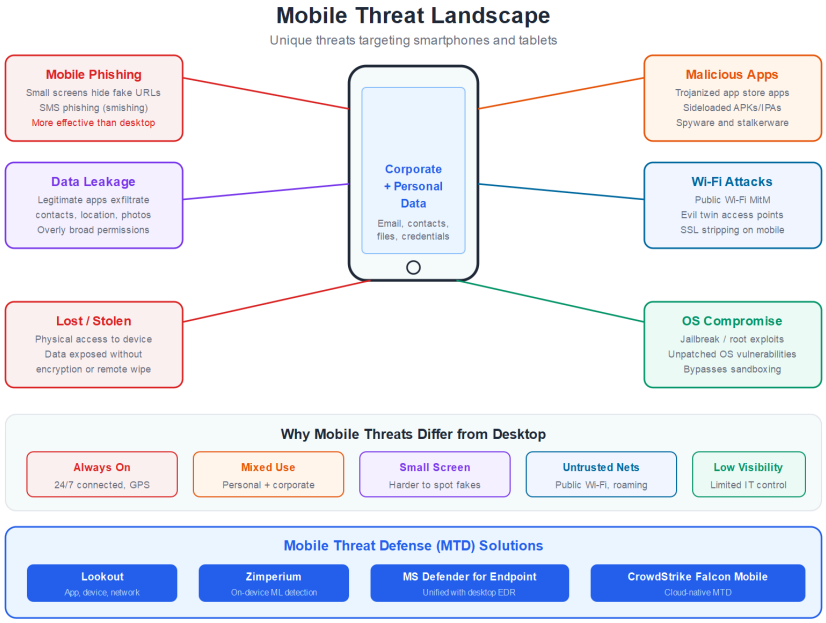

Рисунок 15: Ландшафт мобильных угроз: риски устройств, приложений и сети

Мобильные вредоносные программы существуют, но менее распространены, чем программы для настольных компьютеров, главным образом потому, что мобильные операционные системы более ограничительны. К более серьезным рискам относятся:

Утечка данных через легитимные приложения, которые извлекают контакты, данные о местоположении и другую конфиденциальную информацию. Эти приложения могут быть функционально легитимными, тайно собирая при этом данные.

Фишинговые атаки на мобильных устройствах фактически более эффективны, поскольку меньшие экраны затрудняют идентификацию поддельных веб-сайтов, а почтовые клиенты скрывают полные URL-адреса.

Сетевые атаки в публичных сетях Wi-Fi могут перехватывать незашифрованный трафик. Атаки типа "человек посередине" могут скомпрометировать даже зашифрованные соединения, если пользователь принимает недействительные сертификаты.

Потерянные и украденные устройства раскрывают все данные на устройстве, если оно не защищено надлежащим образом. В отличие от ноутбуков, телефоны легко теряются и достаточно ценны, чтобы их украсть.

Управление мобильными устройствами (MDM)

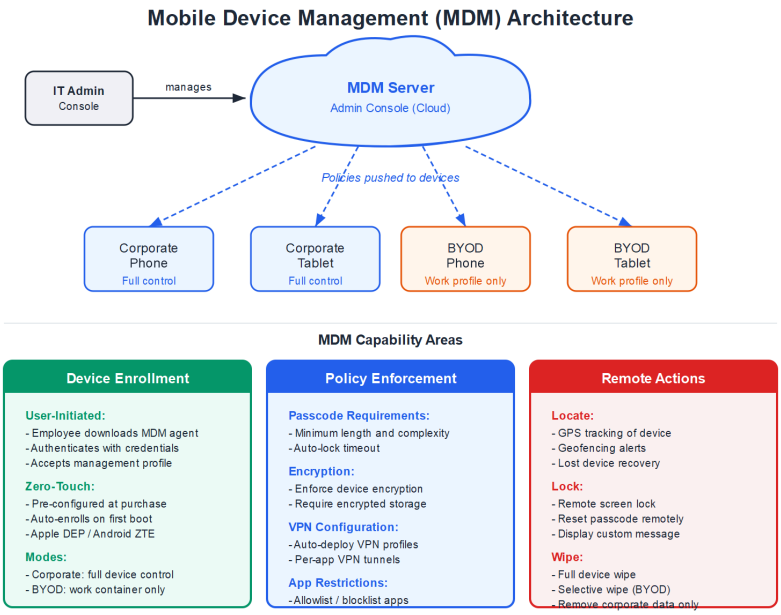

Рисунок 16: Архитектура MDM: централизованное управление мобильными устройствами

Решения для управления мобильными устройствами (MDM) позволяют организациям управлять мобильными устройствами и обеспечивать их безопасность в масштабе. MDM даёт видимость мобильных устройств и контроль над их конфигурацией.

Регистрация устройств регистрирует устройства на платформе MDM. Регистрация может быть инициирована пользователем или автоматической (бесконтактная регистрация для корпоративных устройств). Зарегистрированные устройства получают профили конфигурации и становятся управляемыми.

Применение политик устанавливает конфигурации безопасности на устройствах. MDM может требовать пароли, включать шифрование, настраивать VPN, ограничивать установку приложений и применять десятки других настроек. Устройства, не соответствующие требованиям, могут быть заблокированы от доступа к корпоративным ресурсам.

Управление приложениями контролирует, какие приложения могут быть установлены и как они функционируют. MDM может развертывать корпоративные приложения, блокировать опасные приложения и создавать контейнеры, разделяющие рабочие данные и личные данные.

Удаленные действия позволяют администраторам определять местоположение потерянных устройств, блокировать их, стирать данные или выборочно удалять корпоративные данные, оставляя личные данные нетронутыми. Эти возможности необходимы для реагирования на потерю или кражу устройств.

Управление мобильными приложениями (MAM)

Управление мобильными приложениями, или MAM (Mobile Application Management), фокусируется на приложениях, а не на устройствах. MAM может применять политики к конкретным приложениям без контроля над всем устройством — что ценно для сценариев использования личных устройств, или BYOD (Bring Your Own Device, использование личных устройств), когда сотрудники используют личные устройства для работы.

Возможности MAM включают конфигурацию приложений (предоставление приложениям необходимых настроек), защиту приложений (шифрование данных, предотвращение копирования/вставки в личные приложения, требование аутентификации) и управление жизненным циклом приложений (развертывание, обновление и удаление управляемых приложений).

Microsoft Intune, VMware Workspace ONE и аналогичные платформы предоставляют возможности как MDM, так и MAM, позволяя организациям выбирать соответствующий уровень контроля для различных сценариев.

Лучшие практики безопасности мобильных устройств

Включайте шифрование устройства — и iOS, и Android поддерживают полное шифрование устройства. Это должно быть обязательным для любого устройства, получающего доступ к корпоративным данным.

Требуйте надежную аутентификацию — пароли должны содержать не менее 6 цифр; биометрия создаёт удобство при сохранении безопасности. Включайте автоматическую блокировку при бездействии.

Поддерживайте устройства в актуальном состоянии — обновления мобильных ОС и приложений часто устраняют уязвимости безопасности. Включайте автоматические обновления или контролируйте обновление через MDM.

Ограничивайте источники приложений — корпоративные среды должны ограничивать установку приложений доверенными источниками. На Android отключите установку из неизвестных источников. На iOS предотвратите установку потребительских приложений на корпоративные устройства.

Используйте VPN для сетевой безопасности — виртуальная частная сеть (VPN) защищает трафик в ненадежных сетях. Современные мобильные VPN могут активироваться автоматически при подключении к некорпоративным сетям.

Внедряйте защиту от мобильных угроз — решения MTD (Mobile Threat Defense, защита от мобильных угроз) обнаруживают специфические для мобильных устройств угрозы, включая вредоносные приложения, сетевые атаки и компрометацию устройств. К ведущим производителям MTD относятся Lookout, разработчик решений мобильной безопасности, и Zimperium, разработчик

решений защиты мобильных устройств, а также Microsoft Defender for Endpoint (который включает мобильные возможности).

Часть 7: Предотвращение утечки данных (DLP)

Технологии предотвращения утечки данных, или DLP (Data Loss Prevention), предотвращают выход конфиденциальных данных из организации через несанкционированные каналы. DLP адресует риск эксфильтрации данных, будь то через действия злонамеренных инсайдеров, случайный обмен или деятельность злоумышленников.

Концепции DLP

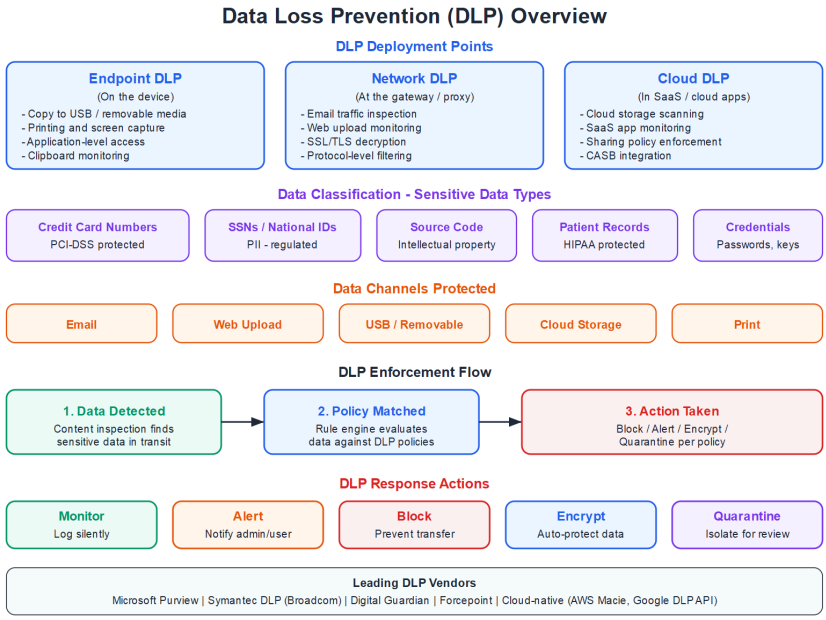

Рисунок 17: Предотвращение утечки данных (DLP): защита конфиденциальной информации

Обнаружение и классификация данных — это фундамент. DLP требует понимания того, какие конфиденциальные данные у вас есть и где они хранятся. Классификация может быть ручной (пользователи маркируют документы) или автоматической (анализ содержимого выявляет конфиденциальные данные). К распространенным типам конфиденциальных данных относятся персональные данные, или PII (Personally Identifiable Information), финансовые данные, медицинская информация, интеллектуальная собственность и учетные данные.

Определение политик описывает, какие данные должны быть защищены и каким образом. Политики могут блокировать передачу номеров кредитных карт по

электронной почте, предотвращать копирование секретных документов на USB-накопители или предупреждать, когда большие объемы данных загружаются в облачное хранилище.

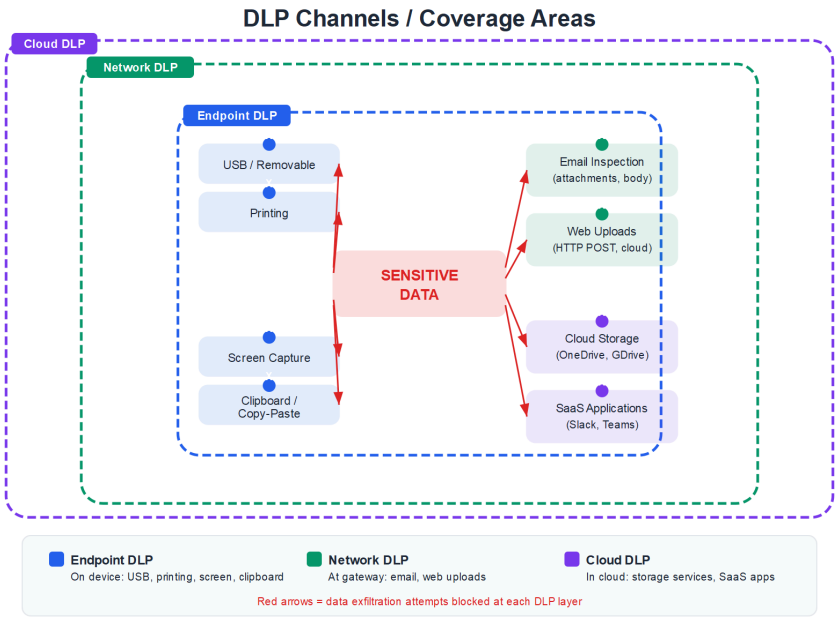

Рисунок 18: Каналы мониторинга DLP: конечные точки, сеть и облако

Механизмы применения реализуют политики через различные каналы:

DLP конечных точек отслеживает данные на конечных точках, контролируя копирование на съемные носители, печать, захват экрана и доступ приложений.

Сетевой DLP отслеживает сетевой трафик, проверяя электронную почту, веб-загрузки и другие передачи на наличие конфиденциальных данных.

Облачный DLP отслеживает облачные приложения и хранилище, предотвращая ненадлежащее хранение или распространение конфиденциальных данных в облачных сервисах.

Трудности внедрения DLP

Внедрение DLP сопряжено с трудностями. Ложные срабатывания возникают, когда легитимная бизнес-деятельность блокируется. Пропуски возникают, когда конфиденциальные данные избегают обнаружения. Настройка DLP для минимизации обоих типов ошибок требует постоянных усилий.

Зашифрованные данные представляют проблему — DLP не может проверить то, что не может прочитать. Инспекция SSL/TLS может решить проблему сетевого шифрования, но каналы со сквозным шифрованием могут обходить обнаружение.

Обходные пути пользователей появляются, когда DLP слишком ограничительна. Пользователи находят изобретательные способы выполнения заблокированных задач — архивирование файлов, переименование расширений, использование

личных устройств. DLP должна балансировать между безопасностью и удобством использования.

К ведущим производителям DLP относятся Microsoft Purview (ранее Microsoft 365 DLP и Azure Information Protection), Symantec DLP (подразделение Broadcom), Digital Guardian, разработчик решений защиты данных, и Forcepoint, разработчик решений кибербезопасности. Облачные провайдеры также предлагают встроенные возможности DLP для своих сервисов.

Часть 8: Пограничный сервис безопасного доступа (SASE)

SASE (Secure Access Service Edge, произносится "сэсси") — это формирующаяся архитектура, объединяющая сетевую безопасность и возможности WAN (Wide Area Network, глобальная сеть) в облачный сервис. SASE решает задачи обеспечения безопасности распределенной рабочей силы, использующей облачные приложения.

Компоненты SASE

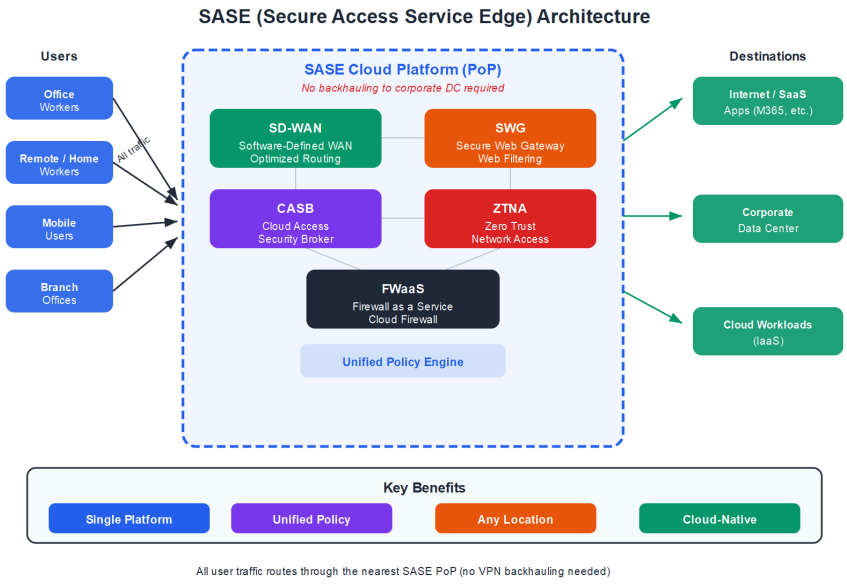

Рисунок 19: Обзор SASE: конвергентные сетевые сервисы и сервисы безопасности

Программно-определяемая глобальная сеть, или SD-WAN (Software-Defined Wide Area Network), обеспечивает интеллектуальную маршрутизацию трафика через множество сетевых подключений (MPLS, широкополосный доступ, LTE). SD-WAN оптимизирует производительность и снижает затраты по сравнению с традиционными архитектурами WAN.

Безопасный веб-шлюз, или SWG (Secure Web Gateway), выполняет веб-фильтрацию, сканирование на вредоносные программы и применение политик для веб-трафика. SWG защищает пользователей от вредоносных веб-сайтов и контролирует соблюдение политик допустимого использования.

Брокер безопасности облачного доступа, или CASB (Cloud Access Security Broker), даёт видимость и контроль использования облачных приложений. CASB обнаруживает теневые ИТ, применяет политики и предотвращает утечку данных в облачных сервисах.

Сетевой доступ с нулевым доверием, или ZTNA (Zero Trust Network Access), предоставляет безопасный доступ к приложениям на основе идентификации и контекста, а не сетевого расположения. ZTNA заменяет традиционный VPN для доступа к приложениям.

Межсетевой экран как услуга, или FWaaS (Firewall as a Service), предоставляет возможности межсетевого экрана в облаке, защищая трафик независимо от местоположения пользователя.

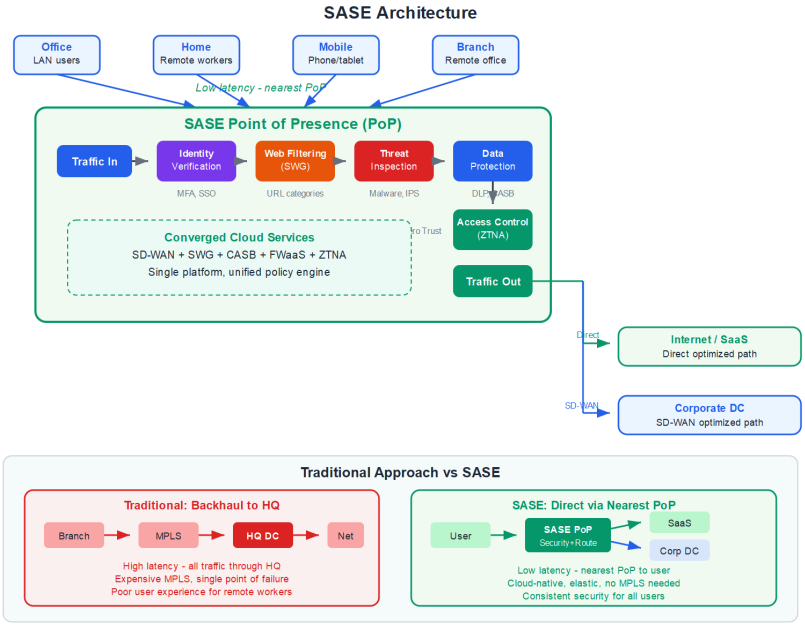

Рисунок 20: Архитектура SASE: облачная безопасность на периферии

Преимущества SASE

Снижение сложности — вместо развертывания и управления множеством отдельных продуктов организации потребляют конвергентную безопасность с единой платформы.

Улучшение производительности — трафик направляется к ближайшей точке присутствия SASE вместо обратной передачи через центр обработки данных. Пользователи ощущают лучшую производительность, особенно для облачных приложений.

Единообразная безопасность — одни и те же политики применяются независимо от местоположения пользователя. Пользователь дома получает ту же защиту, что и пользователь в офисе.

Масштабируемость — облачные сервисы масштабируются автоматически. Организациям не нужно выделять мощности для пиковой нагрузки.

Производители SASE

Рынок SASE стремительно развивается. К ключевым производителям относятся:

Zscaler, разработчик решений облачной безопасности, — пионер в области облачной безопасности с платформой Zero Trust Exchange.

Palo Alto Prisma Access — предоставляет SASE, построенный на возможностях безопасности Palo Alto.

Cisco — объединила SD-WAN (Viptela) и безопасность (Umbrella) в свое предложение SASE.

Netskope, разработчик решений облачной безопасности, — предлагает мощные возможности CASB и SWG в своей платформе SASE.

Cloudflare One — использует свою глобальную сеть для предоставления сервисов SASE.

Часть 9: Унифицированное управление конечными точками

По мере того как организации управляют разнообразными типами устройств — Windows, macOS, iOS, Android, Linux — платформы унифицированного управления конечными точками, или UEM (Unified Endpoint Management), предоставляют единую консоль для управления всеми устройствами.

UEM развилось из конвергенции традиционных инструментов управления ПК и управления мобильными устройствами. Вместо использования отдельных инструментов для ПК и мобильных устройств UEM реализует согласованное управление политиками для всех типов конечных точек.

К ключевым возможностям UEM относятся:

Регистрация и настройка устройств — подключение устройств и автоматическое применение конфигураций. Бесконтактная регистрация позволяет отправлять устройства непосредственно пользователям и настраивать при первом использовании.

Управление приложениями — развертывание, обновление и удаление приложений. Предоставление каталогов приложений самообслуживания.

Управление конфигурациями приложений.

Мониторинг соответствия — проверка того, что устройства соответствуют требованиям безопасности. Несоответствующие устройства могут быть заблокированы от корпоративных ресурсов или автоматически исправлены.

Интеграция с защитой конечных точек — UEM все активнее интегрируется с EDR и другими средствами безопасности, предоставляя единое представление о состоянии безопасности устройства.

К ведущим платформам UEM относятся Microsoft Intune, VMware Workspace ONE, IBM MaaS360 и Citrix Endpoint Management. Эти платформы различаются по своим сильным сторонам для разных типов устройств и сценариев управления.

Заключение

Защита конечных точек и систем охватывает обширный массив технологий и практик. От EDR, обеспечивающего возможности обнаружения и реагирования, через хостовые средства контроля, обеспечивающие эшелонированную защиту, до усиления защиты операционной системы, сокращающего поверхность атаки, до управления обновлениями, закрывающего известные уязвимости, до управления мобильными устройствами, защищающего устройства в карманах пользователей, до DLP, предотвращающего утечку данных — каждый уровень вносит вклад в общую безопасность.

Ключевые принципы, которые следует запомнить:

Эшелонированная защита — ни одно средство контроля не является достаточным. Наслаивайте множество технологий, чтобы при отказе одной другие сохраняли защиту.

Видимость необходима — вы не можете защитить то, чего не видите. EDR, журналирование и мониторинг дают видимость, необходимую для обнаружения угроз и реагирования на них.

Предотвращение важно, но обнаружение и реагирование не менее критичны — несмотря на все ваши превентивные усилия, нарушения безопасности будут происходить. Способность быстро обнаруживать нарушения и эффективно реагировать определяет конечный ущерб.

Поддерживайте системы в актуальном состоянии — установка обновлений остается одной из наиболее эффективных мер безопасности. Большинство атак эксплуатируют известные уязвимости, для которых доступны обновления.

Пользователи важны — одних технологий недостаточно. Обучение по информационной безопасности, четкие политики и удобные для пользователей средства безопасности — все это вносит вклад в безопасность конечных точек.

Мы рассмотрели основные технологические области информационной безопасности — управление доступом, аутентификацию, сетевую безопасность и защиту конечных точек. В последующих лекциях мы исследуем операции безопасности, реагирование на инциденты и другие темы, которые связывают эти технологии в комплексную программу безопасности.

Вопросы для обсуждения

1. Как организациям следует балансировать между необходимостью безопасности конечных точек и производительностью и конфиденциальностью пользователей?
2. Какие стратегии могут помочь организациям сократить время между раскрытием уязвимости и развертыванием обновления?
3. По мере размывания границы между личными и корпоративными устройствами, как должны адаптироваться подходы к безопасности конечных точек?

Благодарю за внимание. Увидимся в следующий раз.

Контрольные вопросы

1. Чем EDR (Endpoint Detection and Response, обнаружение и реагирование на конечных точках) отличается от традиционного антивируса? Какие возможности EDR предоставляет помимо обнаружения?
2. Объясните концепцию атак с "использованием штатных средств" (Living off the Land) и почему они представляют сложность для традиционных средств безопасности.
3. Что такое контроль приложений и каковы трудности его внедрения?
4. Опишите три технологии защиты от эксплойтов и как они защищают от атак.
5. Почему управление обновлениями остается сложной задачей, несмотря на концептуальную простоту?
6. Сравните подходы MDM (Mobile Device Management, управление мобильными устройствами) и MAM (Mobile Application Management, управление мобильными приложениями) к мобильной безопасности. Когда вы бы использовали каждый из них?
7. Каковы основные компоненты решения DLP (Data Loss Prevention, предотвращение утечки данных)? С какими трудностями сталкивается DLP?
8. Объясните архитектуру SASE (Secure Access Service Edge, пограничный сервис безопасного доступа) и ее преимущества по сравнению с традиционными

подходами к безопасности.

Ключевые термины

- **Белый список приложений**: Практика безопасности, разрешающая выполнение на системе только одобренных приложений
- **ASLR**: Рандомизация размещения адресного пространства (Address Space Layout Randomization)
- **Поведенческая аналитика**: Технология безопасности, использующая машинное обучение для обнаружения аномального поведения пользователей и сущностей
- **CASB**: Брокер безопасности облачного доступа (Cloud Access Security Broker)
- **DEP**: Предотвращение выполнения данных (Data Execution Prevention)
- **DLP**: Предотвращение утечки данных (Data Loss Prevention)
- **EDR**: Обнаружение и реагирование на конечных точках (Endpoint Detection and Response)
- **EPM**: Управление привилегиями конечных точек (Endpoint Privilege Management)
- **HIDS**: Хостовая система обнаружения вторжений, отслеживающая подозрительную активность на отдельном хосте
- **HIPS**: Хостовая система предотвращения вторжений, активно блокирующая обнаруженные угрозы на отдельном хосте
- **MAM**: Управление мобильными приложениями (Mobile Application Management)
- **MDM**: Управление мобильными устройствами (Mobile Device Management)
- **MTD**: Защита от мобильных угроз (Mobile Threat Defense)
- **NGAV**: Антивирус нового поколения (Next-Generation Antivirus)
- **Управление обновлениями**: Процесс выявления, получения, тестирования и установки обновлений ПО для устранения уязвимостей
- **SASE**: Пограничный сервис безопасного доступа (Secure Access Service Edge)
- **SD-WAN**: Программно-определяемая глобальная сеть (Software-Defined Wide Area Network)
- **SWG**: Безопасный веб-шлюз (Secure Web Gateway)
- **UEM**: Унифицированное управление конечными точками (Unified Endpoint Management)
- **ZTNA**: Сетевой доступ с нулевым доверием (Zero Trust Network Access)