Простая и правильная защита конечных точек

Как отделы ИТ и ИБ могут защитить свои организации от сложных современных атак?

Без целенаправленной стратегии безопасности тяжело управлять множеством разрозненных устройств, которые дорого обходятся компаниям. Команды ИТ тратят слишком много времени на управление ими. Кроме того, серьезная нехватка специалистов по кибербезопасности вынуждает компании перераспределять нагрузку на сотрудников. С помощью правильной стратегии можно эффективно использовать комплексные технологии, упростить управление и сфокусироваться на основах безопасности. Это позволит создать высокий защитный барьер от реальных атак и существенное преимущество перед другими решениями.

Все начинается с патчинга

Многие уязвимости могут эксплуатироваться потому, что до сих пор не были установлены давно доступные обновления безопасности.

Как отслеживать и устранять все уязвимости без больших затрат и головной боли для ИТ-отдела? Для этого необходимо уметь быстро и легко находить, оценивать, тестировать и применять патчи по всей организации. Учитывая, что большинство уязвимостей связаны со сторонними приложениями, патчинга и обновления ОС просто недостаточно.

Экономьте время и деньги, фокусируйтесь на основных бизнес-инициативах. Инструменты Ivanti запускаются в считанные минуты. Они помогают автоматически обнаруживать, оценивать и исправлять уязвимости в системах Windows, macOS, Linux и UNIX по всей организации на основе настраиваемых политик. Эти инструменты упрощают обновление физических и виртуальных систем. Кроме того, они находят онлайн и оффлайн рабочие станции и серверы, ищут отсутствующие обновления и устанавливают их. Глубокая интеграция с VMware позволяет обновлять всё от ОС и приложений до виртуальных машин (ВМ), виртуальных шаблонов и гипервизора ESXi.

Ivanti также предлагает плагин для Microsoft System Center Configuration Manager, который автоматически обнаруживает и устанавливает обновления на сторонние приложения с помощью консоли SCCM.

Решения Ivanti сочетают расширенный стек API с СЗИ, сканерами уязвимостей, инструментами для управления конфигурациями и создания отчетов, чтобы объединить ИТ, ИБ и DevOps. Решения позволяют импортировать последние результаты оценки уязвимостей в следующую партию патчей, которые будут тестироваться. Так можно сэкономить немало времени, а ИТ-отдел сможет эффективнее участвовать в защите организации. В свою очередь, DevOps подразумевает непрерывное улучшение и автоматизацию. Его интеграция с управлением обновлениями

позволит повысить устойчивость и надежность инфраструктур и систем. Кроме того, вы можете передавать критичные данные в такие решения, как Splunk, Reporting Services, Archer и Crystal Reports, чтобы ускорить анализ критических инцидентов, реагирование на них и их разрешение.

Блокируйте все, что пока невозможно обновить

К сожалению, обновления не защитят от уязвимостей нулевого дня. Что если нельзя выполнить обновление, например, если системы устарели, или есть опасения, что оно может нарушить работу в среде? В этом случае нужно защитить такие приложения с помощью белых списков.

Также важно, чтобы пользователи имели нужные инструменты и не могли устанавливать неавторизованные приложения, которые могут снизить стабильность устройства, повлиять на его безопасность, стать причиной нарушения соответствия лицензиям, вызвать простой и повысить затраты на управление.

Блокировка компьютеров снижает риски, но в то же время ухудшает удобство использования. При этом снижается производительность сотрудников, они вынуждены чаще обращаться в службу поддержки и даже использовать «теневые ИТ», что создает новые риски безопасности.

Ivanti предлагает ведущие решения, которые помогут предотвратить несанкционированное исполнение кода без необходимости ручной проверки обширных списков и снижения продуктивности пользователей.

Trusted Ownership™ автоматически блокирует исполнение любого, в частности, неизвестного кода от недоверенного владельца, например обычный аккаунт пользователя. Решение легко, на глубоко детализированном уровне управляет привилегиями пользователей и политикой, а также позволяет самостоятельно расширить права в случае исключений. С Ivanti легко назначать пользователям ровно те права, которые им необходимы для выполнения своих ролей. Не больше, не меньше.

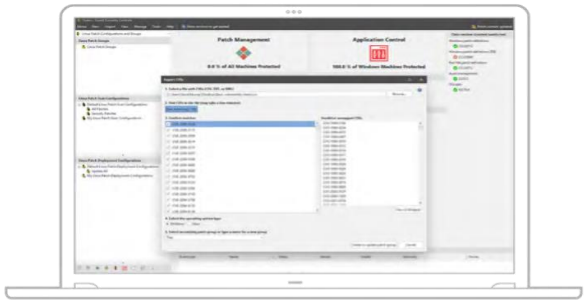
Позаботьтесь о безопасности конфигураций

Настройки ОС и приложений по умолчанию направлены на легкость установки и использования, но не на безопасность. Так или иначе, компаниям необходимо поддерживать набор минимальных стандартных конфигураций.

Ivanti предлагает набор решений безопасности, который при необходимости отключает протокол удаленного рабочего стола (RDP), чтобы предотвратить атаки таких программ-вымогателей, как SamSam. Аналогично после атаки вымогателя WannaCry ИТ-отделам рекомендовали отключить протокол SMBv1. Решения Ivanti выключают его по умолчанию.

Вы также можете настроить политику блокировки учетных записей, чтобы ограничить количество попыток для ввода паролей. Единое решение позволяет отслеживать использование съемных устройств, вводить для них и жестких дисков обязательное шифрование.

Это только некоторые примеры того, что Ivanti предлагает для безопасного управления конфигурациями.



Перейдите на новый уровень с решениями Ivanti

Единое решение Ivanti предлагает ведущие в отрасли автоматизированное управление обновлениями Windows, Red Hat Linux и CentOS, динамическое составление белых списков, детальное управление привилегиями. Решение поддерживает CVE для создания списков обновлений. Патч для REST API интегрирует средства управления безопасностью с другими продуктами, автоматизирует общие процессы и обеспечивает удаленный доступ и управление консолью. С 2019 года Ivanti Security Controls поддерживает устройства на MacOS, а также обеспечивает управление устройствами.

Мы также предлагаем комплект СЗИ, интегрированный в платформу единого управления конечными точками. Платформа позволяет управлять всеми устройствами и защищать их из единой консоли. Решение Ivanti Endpoint Security for Endpoint Manager сочетает расширенные возможности защиты от вредоносного ПО и вирусов с управлением приложениями и обновлениями. Как отмечалось выше, оно также обеспечивает контроль устройств и расширенную защиту от

бесфайловых атак (предотвращает выполнение скриптов, загруженных из интернета, изучает поведение приложений, разрешает только доверенным приложениям запускать скрипты, защищает от атак на оперативную память и др.). Кроме того, вы можете ограничить доступ для авторизованных сетей и IP-адресов, настроить брандмауэры, включая новейшие брандмауэры Windows, под отдельные системы или группы систем. Решение эффективно предупреждает атаки — выявляет попытки зашифровать файлы на локальных устройствах, блокирует процесс шифрования и передает информацию всем другим компьютерам в сети для внесения вредоносного ПО в черный список. Широкие возможности удаленного доступа позволяют изолировать устройства, расследовать инциденты и восстанавливать системы по всей сети.

Создавайте отчеты на информационных панелях в реальном времени

Полноценная защита невозможна без полного понимания среды. Ivanti Xtraction значительно упрощает отчетность, дает возможность по запросу использовать данные из разных решений и легко создавать новые панели мониторинга и отчеты. Необходимая информация поможет директорам, руководителям различных бизнес-подразделений, владельцам приложений быстро и просто принимать лучшие решения.

vanti

ivanti.com
1 800 982 2130
sales@ivanti.com