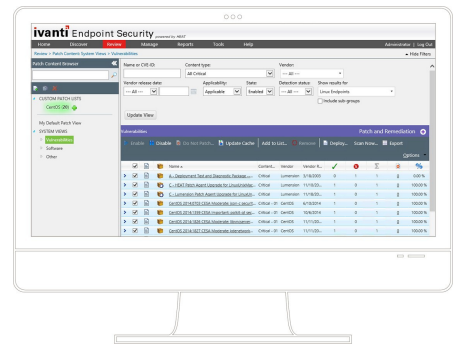


Безопасность вашей гетерогенной среды

Вам необходимо использовать ПО для управления обновлениями на панели инструментов, которое может обрабатывать современные среды смешанных ОС. Расширение процесса патчинга за пределы Windows является обязательным. Используйте единый интерфейс и автоматизированный инструмент для этого.



Патчинг – основа безопасности

Кибер-атаки продолжают расти, а компании активно сопротивляются, иницируя программы для укрепления своей безопасности. Существует множество аргументов в пользу того, что первый шаг к созданию эффективной стратегии многоуровневой безопасности начинается с обновлений. Но процесс обновления все еще остается проблемой. Угрозы продолжают использовать уязвимости, которых можно было бы избежать путем поддержания среды в актуальном состоянии. Патчинг может быть изнурительным, когда ИТ выполняет данную задачу с помощью ручных, трудоемких инструментов, которые сокращают время, доступное для поддержки бизнес-целей, одновременно увеличивая вероятность ошибки. Ivanti® Patch для Linux, UNIX, Mac, powered by Heat, быстро обнаруживает уязвимости в сегодняшней среде - от рабочей станции до ЦОД вне зависимости от ОС.

Агенты за пределами Windows ОС

Защитите тысячи систем с помощью одного инструмента, с поддержкой патчей для Linux, UNIX, Mac и сторонних приложений от сотен поставщиков. Эта консоль, с встроенной автоматизацией, уменьшает вероятность ошибки и упрощает процесс обновления смешанной среды.

Автоматизация оценки уязвимостей и управления исправлениями

Патчинг — это не рядовое событие, а постоянное путешествие. По требованию и интеллектуальному планированию Ivanti Patch для Linux, UNIX, Mac

обеспечивает обнаружение уязвимостей в вашей среде. Новая информация о патче постоянно обновляется и используется для оценки и, при необходимости, исправления уязвимостей в системах автоматически. Задачами развертывания можно управлять и контролировать, чтобы обеспечить обновление, не прерывая ваших пользователей и критическую инфраструктуру. Это, в совокупности с отчетностью по политикам соблюдения, дает вашей компании четкое представление о тех рисках, с которыми она сталкивается.

Обеспечение политик соблюдения

Смотрите, оценивайте и защищайте свои рабочие станции и серверы в соответствии со стандартами безопасности, включая PCI и HIPAA / HITECH. Экономия времени и ресурсов за счет обеспечения соответствия требованиям и предотвращения штрафов за несоблюдение.

Постройте мост между безопасностью и ИТ-операциями

Ivanti Patch для Linux, UNIX, Mac интегрируется с системами безопасности и управления событиями (SIEM) для создания ясной картины видимости для ваших групп безопасности.

Эта интеграция также поможет вам преодолеть разрыв между безопасностью, ИТ и Разработчиками. Например, уязвимости и обновления могут информировать ваши системы управления рисками.

Отдел разработчиков, оснащенный мощными решениями для управления патчами, ведет к созданию более гибких, долговечных и последовательных инфраструктур и систем.

- Команды инженеров и обеспечения качества могут обеспечить согласованные обновления и сторонние библиотеки в своей среде, повышая стабильность их развертывания.
- Команды разработчиков могут автоматизировать развертывание патчей и сторонних библиотек для обеспечения последовательного процесса установки, удаления человеческих ошибок из развертываний.
- Каждый человек пользуется интегрированной отчетностью со свернутой информацией, суммируя текущее состояние и отклонение конфигурации от установленных уровней исправления.

Ключевые преимущества

- Единая веб-консоль с интегрированными отчетами и оповещениями
- Централизованное развертывание патча
- Конфигурация, оценка и развертывание на основе политик
- В режиме реального времени, индивидуальная отчетность
- Полный каталог патчей

www.ivanti.ru

7.495.737.4814

contact@ivanti.ru

Copyright © 2017, Ivanti. All rights reserved. IVI-2016 09/17 MN/BB