Содержание:

Описание Tripwire Enterprise

Неправильно сконфигурированная физическая и виртуальная IT инфраструктура – одна из основных причин низкого уровня IT-безопасности, которая открывает двери утечке и порче информации, хакерским и вирусным атакам, угрозам со стороны инсайдеров. В результате, организации сталкиваются с растущим количеством стандартов и рекомендаций, призванных защитить IT инфраструктуру и сделать ее более безопасной. Для того чтобы решить эту проблему необходимо привести конфигурации всех устройств, приложений и сервисов в соответствие с безопасным доверенным состоянием и постоянно поддерживать это соответствие.

Tripwire Enterprise – это комплексное решение для управления безопасностью конфигураций, включающее следующие возможности:

- Управление политиками безопасности
- Контроль целостности файлов
- Управление восстановлением конфигураций

Это решение позволяет быстро привести всю IT-инфраструктуру компании в соответствие с политиками или стандартами безопасности, а также иметь возможность легко продемонстрировать, как защищены ключевые активы и сервисы компании. После этого Tripwire Enterprise постоянно поддерживает это соответствие, несмотря на установку патчей, апдейтов и вносимые в конфигурацию изменения, которые обычно приводят к ослаблению уровня безопасности.

Компоненты Tripwire Enterprise

Tripwire Enterprise состоит из трех компонентов, каждый из которых оптимизирован для выполнения конкретной задачи, а вместе, благодаря тесной интеграции, они представляют целостное законченное решение по энтерпрайз-уровня.

Policy Manager предназначен для управления политиками, определяющими доверенное состояние систем. Библиотека Policy Manager включает более 300 политик, определяющих доверенное состояние в соответствии с международными отраслевыми стандартами, в том числе и политики по оптимизации систем и сервисов в плане доступности и производительности. Помимо этого можно создать свои политики в соответствии с внутренними стандартами компании.

File Integrity Manager – стандарт де-факто для проверки целостности в большой гетерогенной инфраструктуре. А вместе с Policy Manager он превращает «пассивную» проверку конфигураций в решение по непрерывной защите IT-инфраструктуры, которое моментально обнаруживает отклонение от ожидаемой защищенной конфигурации в режиме реального времени.

Remediation Manager – компонент Tripwire Enterprise, который позволяет отделу IT-безопасности автоматизировать восстановление конфигураций до доверенного состояния в случае обнаружения отклонений или изменений. Помимо этого Remediation Manager позволяет автоматизировать процесс конфигурации новых систем, так как ручное конфигурирование систем в соответствии со всеми политиками и рекомендациями по безопасности – это процесс требующий больших временных затрат с высокой вероятностью совершения ошибок.

Лицензирование Tripwire Enterprise

С точки зрения лицензирования Tripwire Enterprise состоит из двух основных компонентов:

1. **Лицензия Tripwire Enterprise Console** – требуется 1 лицензия Enterprise Console для каждой отдельной инфраструктуры, в которую внедряется Tripwire Enterprise. Для работы Tripwire Enterprise Console требуется база данных, как правило, устанавливаемая на отдельный сервер и лицензии Tripwire Enterprise Console различаются по типу используемой базы данных – Microsoft SQL, Oracle, MySQL. БД MySQL входит в состав Tripwire Enterprise Console для MySQL, но данная БД предназначена для небольших внедрений (до 100 серверов). Лицензии на БД Oracle и Microsoft SQL **не входят** в состав Tripwire Enterprise Console.
2. **Лицензии на устройства и приложения (node license)** – для каждого устройства и приложения, мониторинг которого осуществляется средствами Tripwire Enterprise, требуется приобрести соответствующую лицензию. Данные лицензии различаются в зависимости от типа устройства или приложения:

Тип узлов	Поддерживаемые устройства и приложения	Контролируемые параметры конфигураций
Файловые системы серверов и рабочих станций	Windows Solaris Red Hat Linux SUSE Linux AIX HP-UX	• Разрешения на доступ к файлам и директориям, стойкость пароля • Доступные сетевые сервисы – *Многие сетевые сервисы должны быть отключены, если они не используются (например, FTP, TFTP, Print Server, File Replication, Fax Service, Messenger, RPC Locator и т.д.)* • Опции загрузки
Базы данных	Oracle SQL DB2	• Разрешения • Привилегии • Безуспешные попытки входа, стойкость пароля • Параметры в init.ora, предотвращающие спуффинг, неавторизованный доступ к БД • Параметры в init.ora, которые обеспечивают разграничение полномочий • Параметры, предоставляющие доступ к определенным таблицам БД
Сетевые устройства	Cisco IOS Foundry HP ProCurve Nokia Alcatel *Агенты достаточно гибкие, чтобы обеспечить поддержку 95% устройств*	• Аутентификация пользователей • Конфигурация SNMP • Отключение невостребованных сервисов доступа и управления • Конфигурация NTP • Системные журналы
Службы каталогов	Active Directory Sun Java System Directory Novell eDirectory LDAP	• Политики аудита событий • Политики учетных записей, например, стойкость пароля • Политики логгирования
Гипервизоры	Vmware ESX Solaris Zones	• Межсетевые экраны для сервисных портов виртуальных машин • Шифрование передаваемых данных • Синхронизация времени • Отключение ненужных возможностей (например, скринсейверы) • Аудит

Middleware	BEA WebLogic IBM WebSphere J2EE .NET	• Нет преднастроенных политик для middleware
Приложения - Microsoft IIS	Microsoft IIS	• Методы аутентификации • Включении SSL на порту 443 • Дебаггинг приложения на стороне клиента • Таймаут HTTP соединений • Использование имени хоста в перенаправленных запросах
Приложения – Microsoft Exchange	Microsoft Exchange	• Ограничения размеров входящих и исходящих сообщений • Ограничение количества получателей • Фильтрация получателей не из домена Acvite Directory • Настройки аутентификации • Включение логирования SMTP

Конкурентные преимущества

- **Управление политиками** тесно интегрировано с контролем целостности файлов в едином решении.
- **Мониторинг целостности файлов** обеспечивает 100% видимость и контроль над всеми изменениями конфигураций во всей физической и виртуальной инфраструктуре.
- **Автоматизированное восстановление** нарушенной конфигурации экономит время и деньги.
- **Экспертная оценка состояния соответствия стандартам** обеспечивается большим количеством преднастроенных политик и тестов для большинства международных стандартов.
- **Обширный каталог отчетов и информационных панелей** может быть легко адаптирован под любую инфраструктуру и потребности.
- **Интеграция с лидирующими Helpdesk решениями** (BMC, HP и CA).
- **Поддержка большого количества устройств, приложений и сервисов** – ключевые бизнес-приложения, серверы, файловые системы, службы каталогов, виртуализация, сетевые устройства, базы данных и middleware.
- **Tripwire Enterprise – признанный лидер среди решений по контролю конфигурации** виртуальных и физических IT инфраструктур, используемый тысячами средних и крупных организаций из различных отраслей по всему миру.

Техническая поддержка

К лицензиям и программно-аппаратным комплексам обязательно приобретается техническая поддержка минимум на 1 год. Техническая поддержка дает право на получение программных обновлений к приобретенным решениям, а также возможность обращения в службу технической поддержки вендора для разрешения проблем, возникающих в процессе использования решения.

Варианты технической поддержки:

- 9x5, 1 год (обращение в службу техподдержки в рабочие часы по будним дням)
- 24x7, 1 год (возможность круглосуточного обращения в службу техподдержки по будним и выходным дням)

Дополнительные материалы

- Библиотека материалов по Tripwire Enterprise на английском языке
- Запрос ознакомительной версии Tripwire Enterprise