

tufin

Making Security Manageable

SecureChange

Автоматизация изменений защиты

Промышленный стандарт для автоматизации изменений в системе защиты:

- Превосходное управление рисками
- Повышение сетевой безопасности
- Упреждающее управление ИТ-инфраструктурой
- Расширенная автоматизация ИТ-инфраструктуры
- Принудительное применение корпоративной политики безопасности
- Постоянное соблюдение регулятивных норм
- Разделение обязанностей
- Эффективность эксплуатации

Награды и обзоры:

SC Magazine Review 2013
5/5 Stars Product Review

Network Products Guide 2013
'Most Innovative Company',
'Best Business Expansion' и 'Hot Companies' Winner

Network Computing UK Award 2013
'Best Company' и 'Best Bench Tested Solution of the Year' Finalist

Deloitte Technology Fast 50 2012

CRN Emerging Vendor 2012

SC Magazine Awards 2012 Europe
'Information Security Vendor of the Year' Finalist

Каждое изменение в конфигурации сети является потенциальным риском для безопасности и соответствия требованиям регуляторов. Для защиты жизненно важных приложений и данных, организации должны иметь упреждающее решение для управления изменениями. С помощью Tufin SecureChange™ компании автоматизируют процесс внесения изменения в политику безопасности для анализа рисков, повышения точности и принудительного соблюдения политик. От первоначального запроса до итогового аудита, SecureChange значительно повышает уровень безопасности, при этом время на обработку сокращается вдвое.

УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ ПОЛИТИКИ БЕЗОПАСНОСТИ СЕТИ

SecureChange является решением, специально разработанным для управления изменениями правил межсетевых экранов и устройств безопасности сети, включая маршрутизаторы, коммутаторы, балансировщики нагрузки, шлюзы web-прокси и т. п. SecureChange организует процесс обработки заявок по пользовательским запросам, объединяя автоматизацию бизнес-процессов с всесторонним анализом информационной безопасности и средствами аудита. SecureChange обеспечивает преимущества автоматизации ИТ-процессов для защиты – уменьшение числа задач обрабатываемых вручную, повышения точности и снижения риска.

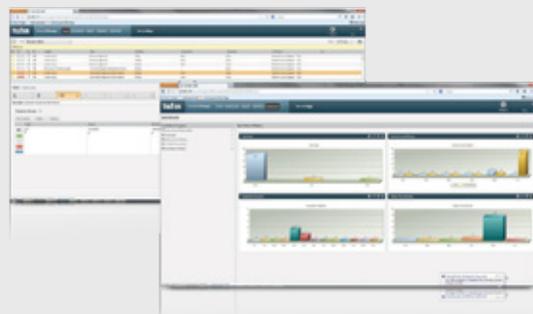


НЕОГРАНИЧЕННЫЕ, ПОЛНОСТЬЮ НАСТРАИВАЕМЫЕ РАБОЧИЕ ПРОЦЕССЫ

Используя удобные шаблоны, основанные на опыте в сфере автоматизации изменений, вы можете быстро определить неограниченное количество рабочих процессов и настроить их в соответствии с требованиями вашей организации. Рабочие процессы могут содержать в себе сложные условия, включая параллельные, автоматические и условные действия. После развертывания системы активно применяются рабочие процессы и разделение обязанностей.

НАДЕЖНОЕ УПРАВЛЕНИЕ ЗАДАЧАМИ

SecureChange предназначен для удобного внесения изменений: более точных; для всех участников; от конечного пользователя, создавшего запрос, до менеджера, который должен выдать разрешение, и особенно для администраторов информационной безопасности. SecureChange сочетает в себе удобный интерфейс Web 2.0 с средствами для повышения производительности, ориентированными на безопасность, что упрощает многочисленные действия, связанные с изменениями защиты.



Устройства серии Т

SecureChange с первого взгляда:

- Автоматизация бизнес-процессов
- Упреждающий анализ рисков
- Конструктор политик
- Автоматизированная обработка изменений
- Исследование топологии сети
- Сквозной аудит и проверка соответствия
- Неограниченное число рабочих процессов с множеством ролей
- Автоматизированная проверка заявок
- Отслеживание Соглашений об уровне предоставления услуг (SLA)
- Интеграция с системой BMC Remedy

“Расчеты рентабельности наглядно показывают, что SecureChange ежегодно в два раза снижает расходы на контроль изменений защиты.”

Ариэль Авитан,,
Отраслевой аналитик
Frost & Sullivan

tufin
Making Security Manageable

www.tufin.com



Copyright © 2014 Tufin Software Technologies Ltd. Tufin, SecureChange, SecureTrack, SecureApp, Automatic Policy Generator и логотип Tufin являются товарными знаками Tufin Software Technologies Ltd. Все другие названия продуктов, упомянутые в настоящем документе, являются торговыми марками или зарегистрированными торговыми марками их соответствующих владельцев.

DS-07-14

УПРЕЖДАЮЩИЙ АНАЛИЗ РИСКОВ И АВТОМАТИЧЕСКИЙ КОНТРОЛЬ

SecureChange позволяет упреждающе оценивать риски и соответствие требованиям до того, как то или иное изменение вступит в силу. Во время процесса выдачи разрешения вы можете принять обоснованное решение на основе анализа рисков. А после того, как изменения завершены, автоматический контроль определяет, соответствует ли фактическое изменение конфигурации первоначальному запросу, и вашей корпоративной политике безопасности.

КОНСТРУКТОР ПОЛИТИК

На стадии проектирования изменений, Конструктор политик (Policy Designer) дает рекомендации на основе данных от производителя о том, как лучше всего осуществить изменение конфигурации для оптимизации защиты и производительности. Рекомендации включают в себя удаление или изменение существующих правил или объектов на всех возможных целевых устройствах. Модуль Network Topology Discovery идентифицирует устройства, которые имеют отношение к запросу на изменение, и отображает их на наглядной визуальной схеме.

АВТОМАТИЧЕСКОЕ ИЗМЕНЕНИЕ ПРЕДОСТАВЛЕНИЯ УСЛУГ

SecureChange может автоматически вносить изменения в правила политики безопасности межсетевых экранов, что позволяет значительно сократить время и повысить точность участвующих в обработке запросов на предоставление доступа. SecureChange рекомендует оптимальные правила или изменения ACL и, если они будут приняты администратором, автоматически вносит изменения в политику межсетевого экрана или маршрутизатора.

ОТСЛЕЖИВАНИЕ SLA

В функции SecureChange входит определение и отслеживание соглашений об уровне обслуживания, как для рабочих процессов, так и для отдельных действий. Данные SLA можно просмотреть в консоли управления, а также в подробных отчетах. Если задача не удовлетворяет требованиям SLA, будут активированы настраиваемые предупреждения или эскалации.

ИНТЕГРАЦИЯ С СИСТЕМАМИ ОБРАБОТКИ ЗАЯВОК И ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ (HELP-DESK)

Для организаций, уже использующих системы обработки заявок и технической поддержки, таких как BMC Remedy, SecureChange добавляет всесторонний анализ защиты, рекомендации о потенциальных рисках и соответствие принятым стандартам защиты, что делает рабочие процессы изменения защиты значительно более эффективными. SecureChange легко интегрируется с системами обработки заявок и управления изменениями для поддержки непрерывного процесса, который начинается и заканчивается в helpdesk-системе.

ПОЛНОФУНКЦИОНАЛЬНЫЙ АУДИТ БЕЗОПАСНОСТИ

В течение всего жизненного цикла изменений конфигурации защиты обеспечивается полнофункциональный аудит. Множество отчетов по результатам аудита обеспечивают полную картину рабочего состояния и возможность полного учета в любой момент. Отчеты по результатам аудита соответствуют отраслевым стандартам (таким, как PCI DSS) и избавляют от необходимости вручную собирать и анализировать информацию перед выполнением процедур внешнего или внутреннего аудита. С помощью Tufin заказчики могут сократить время подготовки к аудиту более чем на 50%.

МАСШТАБИРУЕМОЕ УПРАВЛЕНИЕ ДЛЯ ПРЕДПРИЯТИЙ

SecureChange предлагает полное решение для критически важных центров обработки данных, что обеспечивает высокую доступность, сжатие базы данных и масштабируемость, высокую производительность устройств. Распределенная архитектура Tufin позволяет производить сбор данных с многочисленных устройств и передачу данных через WAN каналы. SecureChange доступен как программное обеспечение на базе Linux, а так же как виртуальное устройство.

TOP – Tufin Open Platform

На основе открытой платформы TOP (Tufin Open Platform) SecureTrack обеспечивает поддержку постоянно расширяющегося набора межсетевых экранов и сетевых устройств. С помощью TOP SDK заказчики и партнеры Tufin могут самостоятельно создавать подключаемые модули (plug-in). Информацию о поддерживаемых устройствах и производителях вы найдете на web-сайте Tufin

