



CITIC TELECOM CPC



TrustCSI™ MAS

Управляемая безопасность веб-приложений

Проверенная платформа, услуги экспертов, безопасные приложения

Интернет-атаки значительно видоизменились с появлением преступников, извлекающих выгоду из своей незаконной деятельности с использованием изощренных методов. Атаки через сеть стали самой серьезной угрозой для предприятий, уязвимых к таким мошенническим технологиям, как межсайтовый скриптинг (XSS), внедрение SQL-кода (SQLi) и межсайтовая подделка запроса (CSRF), которые давно уже стали стандартными уловками.

Теперь вы можете быть уверены, что ваш веб-сайт всегда будет работать. Инженеры Центров SOC компании CITIC Telecom CPC, отвечающие всем отраслевым стандартам, предложат вам круглосуточную поддержку и адаптацию политики для защиты ваших приложений и интеллектуальной собственности – без перерывов. Среди особенностей. **TrustCSI™ MAS** проактивное управление событиями безопасности и реагирование на них, мониторинг в режиме реального времени, специализированные политики, отчеты об атаках и круглосуточная поддержка.

ОСНОВНЫЕ ОСОБЕННОСТИ

- Мгновенно приостанавливает атаки на важные веб-приложения и обеспечивает динамическую защиту онлайн-ресурсов
- Гибкие режимы развертывания с минимальными изменениями существующей среды
- (Дополнительная услуга) Регулярные совещания с анализом отчетов экспертами по безопасности
- Полностью управляемое экспертами по безопасности решение с круглосуточным мониторингом в режиме реального времени, поддержкой на местах и службой «горячей линии»
- Механизм комплексного оповещения
- (Дополнительная услуга) Периодическое автосканирование сети в поисках уязвимостей с виртуальным внесением исправлений (патчингом)

Надежный партнер в сфере информационно-коммуникационных технологий

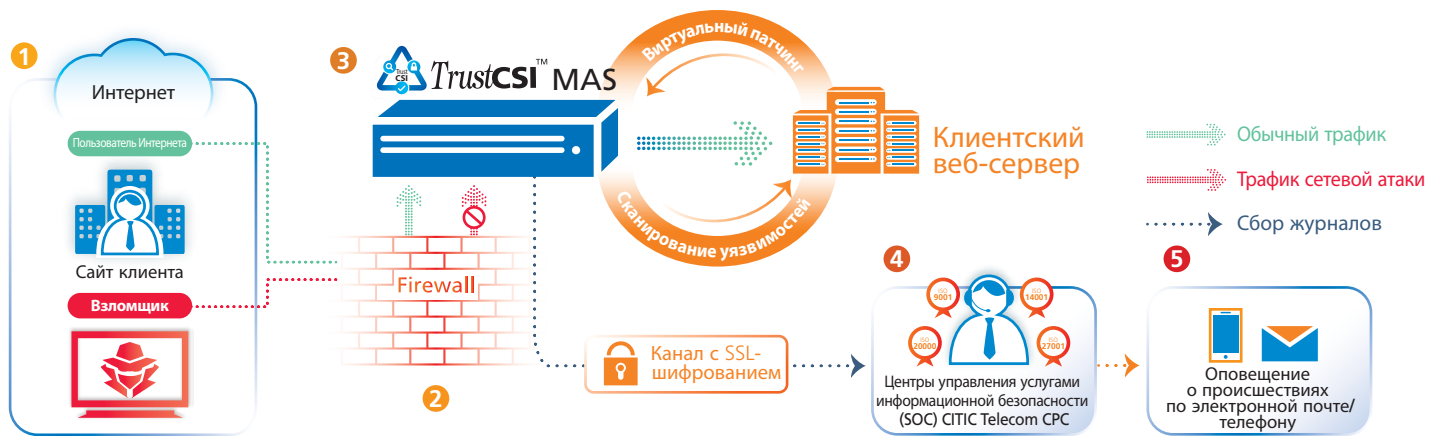


Конкурентные преимущества

Управляемая система безопасности веб-приложений TrustCSI™ – это уникальное инновационное решение от CITIC Telecom CPC, представляющее собой инструмент, призванный стать самым эффективным, надежным, наименее громоздким и лучшим по цене предложением на рынке.

- Мониторинг в режиме реального времени, уведомления и защита важных веб-приложений
- Управление экспертами в сфере безопасности, имеющими необходимые отраслевые сертификаты, с отлаженной по мировым стандартам процедурой реагирования на инциденты
- Защищите свой бизнес, обеспечив его максимальную сохранность и доступность
- Быстрое обнаружение на ранних этапах для защиты от убытков
- Передовые практики в конфигурировании и управлении изменениями
- Гибкие ежемесячные платежи с низкими эксплуатационными расходами без авансовых капитальных вложений

Диаграмма решения TrustCSI™ MAS



- 1 Пользователи и взломщики пытаются получить доступ к веб-серверу клиента через Интернет.
- 2 Сетевой брандмауэр отслеживает и контролирует сетевой трафик, но не может эффективно обнаруживать или защищать веб-серверы от угроз для приложений.
- 3 TrustCSI™ MAS отличается современной системой защиты веб-приложений от кибератак.
- 4 Центры управления услугами информационной безопасности (SOC) CITIC Telecom CPC с профильной командой профессионалов проводят круглосуточный мониторинг в режиме реального времени, принимают меры по устранению проблем и оказывают поддержку, включая модернизацию оборудования и управление исправлениями.
- 5 Сразу же после выявления случаев нарушения безопасности Центры SOC оповестят клиента по электронной почте или телефону.

Преимущества для пользователя

- **Динамическое профилирование** - автоматическое исследование фактического трафика приложения для определения структуры и динамики приложения, что упрощает конфигурирование политики и повышает уровень безопасности. Гарантирует надежную защиту со стороны управляемой системы безопасности веб-приложений TrustCSI™ с первого дня.
- **Виртуальный патчинг** - мгновенное устранение уязвимостей за счет импорта результатов сканирования веб-приложения для блокировки известных уязвимостей, что сразу же снижает вероятность успешной атаки.
- **Обнаружение и защита критической интернет-активности в режиме реального времени** - защита мирового класса в режиме реального времени и блокировка DDoS-атак на приложения на местах, включая угрозы, входящие в первую десятку списка OWASP.
- **Выполнение требования 6.6 стандарта безопасности данных в сфере платежных карт** - торговые организации, принимающие платежи с кредитных карт, должны соответствовать требованиям индустрии платежных карт (PCI), а требование 6.6 обязует организации иметь брандмауэр веб-приложений и проводить регулярную ревизию всех веб-приложений.

CITIC Telecom CPC

- 🌐 Сайт: www.citictel-cpc.com
- ✉ Азиатско-тихоокеанский регион: info@citictel-cpc.com
- ✉ Европа и СНГ: info-eu@citictel-cpc.com

Гонконг: 852 2170 7101
Япония: 81 3 5339 1968
Эстония: 372 622 33 99
Польша: 48 22 630 63 30

Тайвань: 886 2 6600 2588
Малайзия: 603 2280 1500
Латвия: 371 6721 4122
Россия: 7 495 657 9277

Континентальный Китай (бесплатный звонок): 400 880 1222
Сингапур: 65 6220 6606
Литва: 370 5264 4303
Нидерланды: 31 20 567 2000