CITIC TELECOM CPC

TrustCSI™ ATP Усовершенствованная защита от угроз

Защитите свое предприятие с помощью TrustCSI™ ATP

Принимая во внимание рост изощренных угроз и атак на приложения и данные, современные предприятия действуют в условиях беспрецедентного риска. Решение **TrustCSI™ ATP** обеспечивает комплексную защиту вашего предприятия от развитых устойчивых угроз (ATP – advanced persistent threats) на конечных устройствах, серверах (файловых и интернет-серверах) и в сетях. Управляемая система ATP от CITIC Telecom CPC предоставляет вашей организации все преимущества круглосуточного ИТ-отдела мирового класса без каких-либо административных и накладных расходов.

ОСНОВНЫЕ ОСОБЕННОСТИ

- Комплексное, полностью управляемое решение по безопасности обеспечивает эффективную защиту от угроз.
- Эффективно борется с широким спектром угроз во всей инфраструктуре, обеспечивая мониторинг в режиме реального времени, упреждая оповещения и устраняя угрозы.
- Активно обнаруживает и блокирует новые возникающие угрозы и атаки неизвестного типа, с которыми не справляются другие, менее совершенные решения в области безопасности.
- Элементы системы активно взаимодействуют друг с другом для обеспечения единой согласованной защиты в режиме реального времени.
- Непрерывно действующая система многоуровневой безопасности включает в себя унифицированное управление угрозами (UTM), брандмауэр веб-приложений (WAF), защищенный почтовый шлюз (SEG), изолированную среду и круглосуточно управляемые услуги по обеспечению безопасности (MSS).

Надежный партнер в сфере информационно-коммуникационных технологий

中信國際電訊(信息技術)有限公司
CITIC TELECOM INTERNATIONAL CPC LIMITED
Представитель
CITIC TELECOM INTERNATIONAL

TrustCSI™ ATP

Усовершенствованная защита от угроз

TrustCSI™ ATP воплощает в себе новый подход к защите вашего предприятия путем сочетания нескольких механизмов обеспечения безопасности с инфраструктурой и профессиональными услугами мирового класса от CITIC Telecom CPC. TrustCSI™ ATP представляет собой комплексное решение для защиты сетей от продуманных атак.

Конкурентные преимущества

Индивидуализированное комплексное решение по безопасности

TrustCSI™ ATP будет настроена и развернута с учетом ваших потребностей, инфраструктуры и ресурсов.

Модули взаимодействуют друг с другом для более надежной защиты

Интеграция различных защитных механизмов для выявления подозрительной деятельности и обеспечения взаимодействия систем безопасности и отсутствия слабых мест. Усовершенствованные модули UTM, WAF и SEG интенсивно обмениваются информацией с модулем изолированной зоны, который обновляет сигнатуры угроз при обнаружении новых.

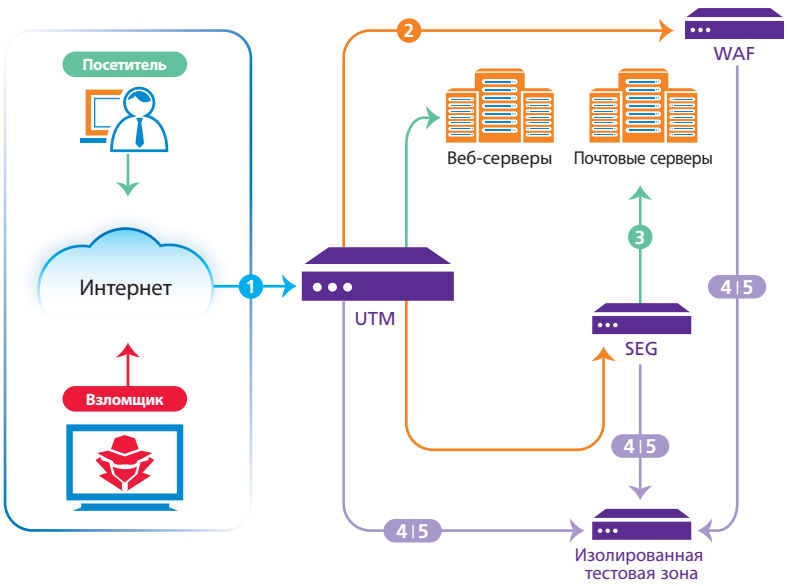
Круглосуточный мониторинг и консультации по вопросам безопасности

Ваше предприятие получит круглосуточную помощь специалистов по безопасности, оповещение о нештатных ситуациях и рекомендации экспертов по устранению проблем.

Глубокое понимание тенденций в сфере угроз безопасности

В Центрах SOC используется исследовательская платформа для анализа тенденций в развитии угроз вашим цифровым ресурсам с еженедельным предоставлением отчетов о работе модулей UTM, WAF и SEG.

Диаграмма решения TrustCSI™ ATP



1. Когда посетители просматривают веб-сайты, веб-трафик поступает в модуль UTM, который укрепляет периметр сети, контролируя все типы поступающего трафика.
2. Трафик веб-приложения передается в модуль WAF для анализа поведения и сигнатур. Разрешенный трафик отправляется обратно в модуль UTF, в то время как известный вредоносный трафик блокируется.
3. Электронная почта передается в модуль SEG, который сканирует содержимое и приложения. Сеть и пользователи защищаются от спама и вредоносного ПО.
4. Неизвестные и подозрительные файлы отправляются в карантинную зону. Эти файлы исполняются в эмулированной и изолированной среде.
5. При обнаружении вредоносного или подозрительного файла модуль изолированной среды отправит уведомление соответствующему модулю и автоматически примет защитные меры.

Пять основных компонентов системы TrustCSI™ ATP

YYY — Унифицированное управление угрозами: высокоэффективный шлюз безопасности, обеспечивающий всестороннюю защиту от комплексных угроз на уровне сети, контента и приложений.

БВ — Брандмауэр веб-приложений: использует передовые технологии для двусторонней защиты от сложных угроз для веб-приложений, включая внедрение SQL-кода и межсайтовый скриптинг.

ЗПШ — Защищенный почтовый шлюз: защищает от различных угроз почтовой безопасности, включая фишинг и вредоносные вложения.

ИЗОЛИРОВАННАЯ ТЕСТОВАЯ ЗОНА — Изолированная тестовая зона: исполняет подозрительные файлы в виртуальной среде для определения их истинной сути и уровня риска. Борьба с угрозами автоматизирована путем интеграции с другими компонентами системы безопасности.

УУБ — Управляемые услуги безопасности: услуги по предотвращению, обнаружению и устранению угроз, а также круглосуточный мониторинг и оповещение в режиме реального времени. При помощи исследовательской платформы анализируются уязвимости и обнаруживаются реальные угрозы.

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

STA1802EN