websense®

РЕШЕНИЯ WEBSENSE® TRITON™

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ ДЛЯ ИНТЕРНЕТА, ЭЛЕКТРОННОЙ ПОЧТЫ, ДАННЫХ И МОБИЛЬНЫХ УСТРОЙСТВ

TRITON БЛОКИРУЕТ БОЛЬШЕ УГРОЗ. МЫ ГОТОВЫ ЭТО ДОКАЗАТЬ.

websense
TRITON®

ПЕРЕДОВАЯ И ДИНАМИЧНАЯ ЗАЩИТА ОТ ПЕРЕДОВЫХ И ДИНАМИЧНЫХ УГРОЗ

Угрозы безопасности, которым вынуждены противостоять современные корпорации, постоянно развиваются и усложняются. Привычные методы защиты не смогут обезопасить вас от угроз будущего. Эффективные решения безопасности должны быть столь же передовыми и интеллектуальными, как и сами угрозы. Таковы решения на базе архитектуры Websense® TRITON™.

Архитектура TRITON стала результатом активной многолетней научно-исследовательской работы в области современного изменчивого ландшафта угроз. Решения TRITON сочетают в себе передовые технологии безопасности для Интернета и электронной почты, а также технологии предотвращения потери данных (DLP), образуя единую систему информационной безопасности, которая защищает вашу организацию от полного спектра угроз повышенной сложности.

ЛУЧШАЯ В СВОЕМ КЛАССЕ БЕЗОПАСНОСТЬ НА БАЗЕ ЕДИНОЙ АРХИТЕКТУРЫ

Решения безопасности TRITON обеспечивают мгновенную защиту благодаря встроенным средствам Websense ACE (Advanced Classification Engine), действующим в реальном времени. Эта подсистема ACE объединяет семь аспектов оценки безопасности в комплексную модель количественной оценки на базе упреждающего анализа. Эффективную работу этих непревзойденных средств защиты в режиме реального времени обеспечивает крупнейшая в мире сеть аналитики безопасности Websense ThreatSeeker® Intelligence Cloud, а также профессионализм и опыт международной исследовательской команды Websense Security Labs™.

ВСТРОЕННАЯ В ЯДРО ТЕХНОЛОГИЯ DLP.

В отличие от предложений конкурентов технология DLP встроена прямо в ядро решений TRITON . Эта технология используется в архитектуре TRITON в целях защиты и соблюдения нормативных требований. Шлюзы электронной почты защищены с помощью встроенных в ядро средств Websense TruEmail DLP™. А наш самый передовой веб-шлюз обеспечивает комплексное управление политиками Websense TruWeb DLP™, защиту целостности и такие уникальные возможности, как оптическое распознавание символов в изображении. В криминалистических отчетах доступны всеобъемлющие передовые методы для сбора сведений и данных об инцидентах безопасности, которые можно легко просмотреть на панели мониторинга угроз. Функции защиты рабочих станций DLP могут работать автономно, без подключения к серверу и используют цифровые отпечатки на рабочих станциях с ОС Windows и Mac OS. Технологии шифрования портативных устройств защищают данные с рабочих станций на USB-устройствах и съемных носителях.

СВОБОДА ВЫБОРА И ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ.

В зависимости от размера вашей организации вы можете развернуть ПО, АПК, облачные службы или гибридное решение. Развертывание системы для защиты от угроз в веб, электронной почте, а также решение для защиты данных возможно выполнить на одной платформе. Благодаря гибридному развертыванию облачного решения и АПК, вы сможете обеспечить одинаково надежную защиту офисов и удаленных пользователей.

ЭКОНОМИЧНЫЙ ПАКЕТ СЕЙЧАС — НЕОГРАНИЧЕННЫЙ РОСТ ВАШЕГО БИЗНЕСА В БУДУЩЕМ

Вместе с любым вариантом решения TRITON вы приобретаете возможность укреплять и расширять защиту интернет-трафика, электронной почты и конфиденциальных данных в будущем. Если вашей компании требуется лучший на рынке веб-шлюз с прокси-сервером, встроенная технология предотвращения утечки информации (DLP) для обеспечения безопасности сети и соответствия законодательным нормам, а также передовые системы блокировки вредоносного ПО и «песочницы» для определения вредоносного кода, не нужно искать эти решения у отдельных поставщиков. Websense предоставит вам единую систему безопасности на основе архитектуры TRITON, которая обеспечивает интеграцию компонентов, защиту от новейших атак и снижение затрат.

TRITON БЛОКИРУЕТ БОЛЬШЕ УГРОЗ. МЫ ГОТОВЫ ЭТО ДОКАЗАТЬ.

ОБЪЕДИНЕННЫЕ ФУНКЦИИ АНАЛИЗА И АНАЛИТИЧЕСКОЙ БЕЗОПАСНОСТИ

УНИКАЛЬНОСТЬ WEBSENSE: ACE

Благодаря комплексной количественной оценке рисков и предиктивной аналитике подсистема ACE обеспечивает самую эффективную встроенную контекстную защиту для веб траффика, электронной почты и данных в режиме реального времени. ACE гарантирует целостность информации, анализируя входящий и исходящий трафик с помощью интеллектуальных методов защиты от кражи данных. С помощью классификаторов для безопасности в режиме реального времени, анализа данных и контента, разработанных за многие годы исследований, подсистема ACE ежедневно обнаруживает гораздо больше угроз, чем традиционные антивирусные ядра (доказательства см. на стр. www.websense.com/proveit). Технология ACE — это основная система защиты во всех решениях TRITON, которая функционирует на базе облака ThreatSeeker Intelligence Cloud.

THREATSEEKER INTELLIGENCE CLOUD: КРУПНЕЙШАЯ В МИРЕ СИСТЕМА ВЕБ-МОНИТОРИНГА

Облако ThreatSeeker Intelligence Cloud под управлением компании Websense Security Labs предоставляет совокупные данные аналитики безопасности для всех продуктов безопасности Websense. Эта система, объединяющая в себе свыше 900 млн рабочих станций, получает данные от Facebook и технологии Defensio™. Вместе со средствами безопасности ACE она ежедневно анализирует 3–5 млрд запросов. Благодаря столь обширным сведениям об угрозах безопасности облако ThreatSeeker Intelligence Cloud предлагает обновления безопасности в режиме реального времени, которые блокируют угрозы повышенной сложности, вредоносное ПО, фишинговые атаки, мошеннические ресурсы и сайты-приманки, предоставляя наиболее актуальные веб-рейтинги. Система ThreatSeeker Intelligence Cloud не имеет себе равных по масштабу и использованию методов защиты ACE в реальном времени для анализа совокупных входных данных.

WEBSENSE SECURITY LABS: КРУГЛОСУТОЧНАЯ ИНФОРМАЦИЯ ОТ МИРОВЫХ ЭКСПЕРТОВ

Websense Security Labs стимулирует исследования в сфере безопасности, обнаруживая, расследуя и освещая угрозы повышенной сложности, которые невозможно обнаружить с помощью традиционных методов исследования безопасности. Будучи признанным мировым лидером в сфере исследований безопасности, Websense Security Labs круглосуточно публикует результаты деятельности в своем заслужившем широкое признание блоге, который посещают сотни представителей отраслевых партнеров, поставщиков, информационных агентств, военных и других организаций во всем мире. Свыше 100 мировых экспертов по угрозам трудятся в команде Websense Security Labs в различных странах Америки, Европы, Ближнего Востока, Африки и Азиатско-Тихоокеанского региона. Они постоянно отслеживают новые угрозы, в том числе те, которые появляются в Интернете, распространяются по сети, электронной почте, через мгновенные сообщения и пиринговый обмен файлами.

СЕМЬ ЭТАПОВ ПОВЫШЕННОЙ АТАКИ

ЕДИНЫЕ ТЕХНОЛОГИИ ДЛЯ ЗАЩИТЫ ОТ УГРОЗ В ИНТЕРНЕТЕ И ЭЛЕКТРОННОЙ ПОЧТЕ, А ТАКЖЕ ДЛЯ ПРЕДОТВРАЩЕНИЯ ПОТЕРЬ ДАННЫХ

В едином интерфейсе решений TRITON сочетаются возможности управления и отчетов для технологий Websense, обеспечивающих безопасность в веб, электронной почте, а также защиту от утечек данных. Этот интерфейс задает новые стандарты прозрачности, контроля и простоты управления. В едином веб-интерфейсе Websense TRITON можно задавать политики, управлять инцидентами, создавать отчеты и выполнять задачи администрирования независимо от модуля решения (веб-безопасность, безопасность данных или электронной почты) или платформы (облачной или локальной). При этом все решения TRITON имеют единую архитектуру и оснащены едиными возможностями аналитики безопасности, политик и отчетов.

Websense® Web Security

(ВЕБ-БЕЗОПАСНОСТЬ)

Целевые атаки и кражи данных — вот два фактора, формирующих современный ландшафт веб-безопасности. Антивирусные программы и URL-фильтры уже не способны обеспечить всеобъемлющую защиту информации. Для защиты от современных атак повышенной сложности необходимы встроенные методы защиты в режиме реального времени и инновационные технологии защиты от утечек данных (DLP). Ведь эти атаки могут включать любые из семи этапов вредоносной деятельности, ведущих к краже данных. Продукты веб-безопасности TRITON оснащены инновационными возможностями, такими как панели мониторинга угроз, криминалистические отчеты и сбор данных для ведения расследований, анализ вредоносного ПО в изолированной среде («песочнице») и интеллектуальные методы защиты, которые обеспечивают целостность важной информации. Для удобного управления всеми этими возможностями используется единая консоль TRITON.

Websense® Email Security

(БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ)

Угрозы, распространяемые по электронной почте, совершенствуются ежедневно, чего нельзя сказать о типичных решениях безопасности для этого вида коммуникации. В большинстве из них используются устаревшие методы, которые были эффективны в прежние времена, когда хакеры просто рассылали вирусы в виде вложений в письма. Такие методы бессильны перед смешанными угрозами, использующими для заражения сразу и электронную почту, и веб ресурсы, а также неспособны обнаружить действия сотрудников, которые могут привести к утечке конфиденциальной информации. Благодаря встроенным технологиям веб-безопасности и безопасности данных продукты для защиты электронной почты TRITON обеспечивают передовую защиту от угроз повышенной сложности. И независимо от метода их развертывания — облако, АПК или гибридный вариант — ими можно с легкостью управлять из консоли TRITON.

Websense® Web Security

(БЕЗОПАСНОСТЬ ДАННЫХ)

Опороченная репутация бренда, падение прибыли, сужение рынка сбыта и даже административные штрафы — негативное влияние уязвимостей данных не только очевидно, но и представляет значительную опасность для компаний в современной деловой среде. Даже один инцидент утечки данных может подорвать конкурентное преимущество и уверенность клиентов в компании, привести к штрафам или взысканиям от регулятивных органов. Еще больше усугубляет проблему повсеместное распространение периферийных устройств и общедоступность ПО для обмена файлами. Традиционные решения для защиты от утечек данных стоят дорого и довольно сложны в эксплуатации. Аналогичные возможности Websense развернуть очень легко: вы сможете сразу извлекать из них выгоду, не усложняя себе работу и без излишних затрат. Решения для защиты данных Websense эффективно предохраняют организации всех размеров от множества сценариев утечки конфиденциальных данных. Они образуют единую платформу, которая предотвращает утечки данных в сети и на рабочих станциях и распознает конфиденциальные данные.

НАБОРЫ РЕШЕНИЙ TRITON

Клиентам предлагаются два набора решений TRITON. Оба набора включают технологии веб-защиты, защиты электронной почты и предотвращения потери данных (DLP).

WEBSENSE TRITON ENTERPRISE

Самое комплексное решение для защиты информации, Websense TRITON Enterprise, сочетает в гибридном развертывании «АПК+облако» такие технологии, как Websense Web Security Gateway Anywhere, Websense Email Security Gateway Anywhere и Websense Data Security Suite, эффективно защищая офисных и удаленных сотрудников от новейших угроз. Добавив сервисы Websense CyberSecurity Intelligence™ (CSI), вы получите доступ к «интернет-песочнице» для вредоносного ПО и возможность прямого взаимодействия с исследователями угроз Websense Security Labs.

WEBSENSE TRITON SECURITY GATEWAY ANYWHERE

Websense TRITON Security Gateway Anywhere сочетает в гибридном развертывании «АПК+облако» такие технологии, как Websense Web Security Gateway Anywhere и Websense Email Security Gateway Anywhere, а также встроенные возможности защиты от потери данных, эффективно защищая офисных и удаленных сотрудников от новейших угроз. Добавив сервисы CSI, вы получите доступ к «интернет-песочнице» для вредоносного ПО и возможность прямого взаимодействия с исследователями угроз Websense Security Labs.

МОДУЛИ РЕШЕНИЙ TRITON

Два набора решений TRITON состоят из следующих модулей, которые можно приобрести по отдельности или в различных комбинациях в зависимости от потребностей организации:

WEBSENSE WEB SECURITY GATEWAY ANYWHERE

Websense Web Security Gateway Anywhere, наш флагманский веб-шлюз, работает на гибридной локально-облачной архитектуре и включает возможности защиты от утечек данных. Благодаря комплексным встроенным средствам защиты в реальном времени Web Security Gateway Anywhere эффективно защищает офисных и удаленных сотрудников от новейших угроз. В этом решении предлагаются средства защиты от угроз повышенной сложности, панель мониторинга угроз, криминалистические отчеты, функции сбора данных и защиты их целостности.

WEBSENSE EMAIL SECURITY GATEWAY ANYWHERE

Websense Email Security Gateway Anywhere обеспечивает высочайший уровень защиты от традиционных и современных угроз, предоставляет возможности развертывания средств защиты от утечек данных. Технология TrueHybrid позволяет использовать две платформы развертывания -- локальную и облачную. В модуле Email Security Gateway Anywhere интегрированы функции аналитики веб-безопасности и безопасности данных. Именно они обеспечивают непревзойденный уровень прозрачности и защиты от современных угроз в электронной почте. Важно отметить, что в модуле используется та же технология, что и в нашем ведущем корпоративном специализированном продукте с функциями защиты от утечек данных для электронной почты.

WEBSENSE WEB SECURITY GATEWAY

Модуль Websense Web Security Gateway — это локальный веб шлюз с панелью мониторинга угроз повышенной сложности. Он обеспечивает комплексную встроенную защиту от современных угроз повышенной сложности в режиме реального времени, криминалистические отчеты для расследования инцидентов безопасности и интеграцию с SIEM. А контроль приложений позволяет продуктивно и безопасно работать в социальных сетях, не подвергая компанию риску и не нарушая принятых правил пользования.

WEBSENSE EMAIL SECURITY GATEWAY

Websense Email Security Gateway развертывается на АПК Websense V-Series™, обеспечивая встроенную защиту от традиционных и отличающихся повышенной сложностью угроз, а также кражи и утечки данных.

WEBSENSE DATA SECURITY SUITE

Websense Data Security Suite — это единый набор возможностей защиты от потери данных для шлюзов, рабочих станций и процессов обнаружения. Data Security Suite включает три модуля: Data Security Gateway, Data Discover и Data Endpoint, с помощью которых вы сможете минимизировать риск потери данных от действий злоумышленников или случайного несанкционированного использования. Для каждого модуля можно приобрести отдельную лицензию, начав с одной возможности и наращивая их число по мере надобности.

TRITON MOBILE SECURITY

Websense TRITON Mobile Security — это единственное облачное решение безопасности, которое позволяет распространить действующие в компании политики безопасности на мобильные устройства. Эта возможность позволяет защитить ваши данные, снизить риски и активизировать работу бизнеса, облегчая сотрудникам работу в любой ситуации. TRITON Mobile Security обеспечивает эффективную веб-безопасность, защиту от вредоносного кода для мобильных платформ, контроль приложений и отчетность для мобильный устройств. Благодаря ему ваши сотрудники смогут пользоваться мобильными устройствами в рабочих целях, не беспокоясь о вредоносном ПО для мобильных платформ,, веб-угрозах, фишинговых атаках, спуфинге и многом другом.

ПОДДЕРЖКА РАЗЛИЧНЫХ ПЛАТФОРМ

Решения TRITON обеспечивают клиентам свободу выбора: вы сможете установить их на одну или несколько различных платформ с учетом своих потребностей.

АПК СЕРИИ V: МОЩНЫЕ, РАСШИРЯЕМЫЕ И ПРОСТЫЕ

Наши предварительно настроенные АПК серии V сразу готовы к работе: вы получаете мощную, гибкую и одновременно простую в развертывании платформу безопасности. Теперь вам не придется вручную подбирать совместимое оборудование, устанавливать ПО, настраивать ОС или проводить предварительное тестирование.

ОБЛАЧНОЕ РАЗВЕРТЫВАНИЕ: СЭКОНОМЬТЕ НА УСТАНОВКЕ И ПОДДЕРЖКЕ ОБОРУДОВАНИЯ И ПО

Облачное развертывание позволяет быстро и эффективно предоставить функции защиты от угрозы в Интернете и электронной почты для всех пользователей независимо от их местонахождения. Вам не придется обслуживать локальное оборудование, и вы сможете упростить сетевую инфраструктуру, а также снизить совокупную стоимость владения. А наши глобальные центры обработки данных операторского класса сертифицированы по стандарту ISO 27001 и обеспечивают работоспособность в размере 99,999 %, зафиксированную в соглашениях об уровне обслуживания.

РАЗВЕРТЫВАНИЕ TRUHYBRID: ТОЛЬКО ЛУЧШЕЕ

Развертывание TruHybrid — позволит использовать лучшее из двух подходов — локальные АПК и облачные технологии. Вы получаете уникальные преимущества локальных и облачных технологий защиты информации и сможете управлять всей системой из единой консоли.

Развертывание TruHybrid решает сразу несколько ключевых проблем веб-безопасности:

- Высокопроизводительные АПК или масштабируемое ПО для нужд крупных компаний. .
- Облачная защита филиалов, где недостаточно ресурсов для технической поддержки оборудования.
- Облачная защита удаленных пользователей без возврата трафика в центральный офис для инспекции.

Развертывание TruHybrid дает преимущества и в сфере безопасности электронной почты:

- Основная масса входящего трафика фильтруется в облаке, снижая нагрузку на локальное оборудование.

ПОДРОБНЫЕ СВЕДЕНИЯ МОЖНО ПОЛУЧИТЬ В КОМПАНИИ WEBSENSE

www.websense.com

websense

websense TRITON