IMPERVA®

Межсетевой экран веб-приложений Imperva SecureSphere

DATASHEET

Защитите ваши критичные веб-приложения и данные

Веб-приложения являются для кибератак целями номер один, так как они открыты для доступа и представляют собой легкий путь к ценным данным. Для борьбы с кибератаками организации должны защищать свои веб-сайты и приложения от существующих и вновь возникающих киберугроз без ущерба для производительности приложений или их доступности.

Все больше организаций полагаются именно на решение компании Imperva для защиты своих критичных веб-приложений. Решения Imperva для безопасности веб-приложений идеально встраиваются в физические, виртуальные и облачные центры обработки данных и предоставляют наиболее совершенные средства безопасности веб-приложений, постоянно получающие аналитическую информацию об угрозах, подготовленную исследователями из всем известного Центра Защиты Приложений Imperva (Application Defense Center).

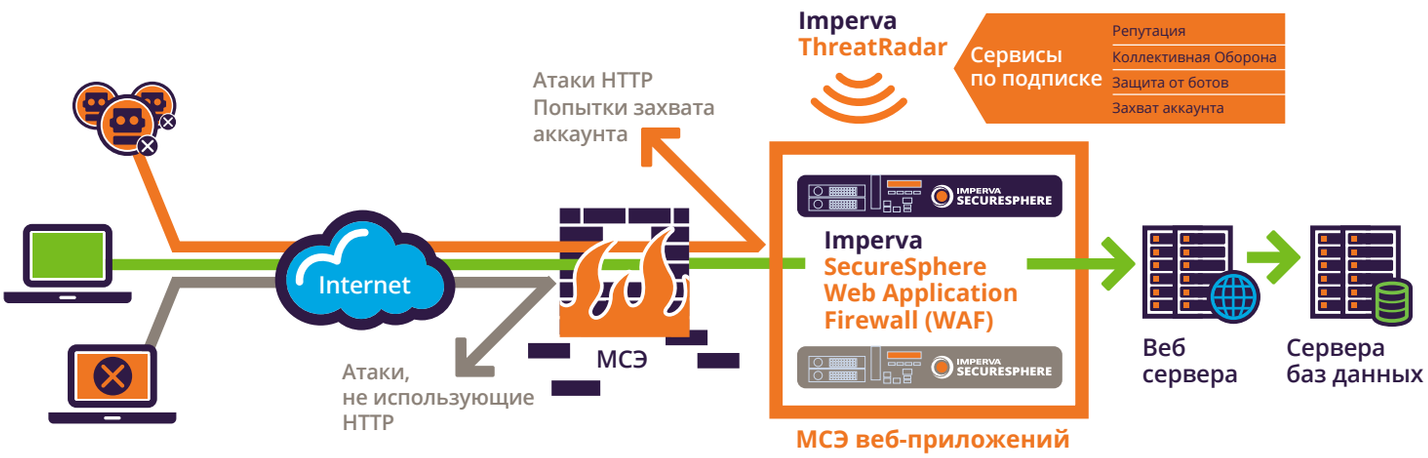
SecureSphere Web Application Firewall анализирует весь доступ пользователей к критичным для вашего бизнеса приложениям и защищает ваши приложения и данные от кибератак.

Межсетевой экран веб-приложений Imperva SecureSphere

МСЭ веб-приложений SecureSphere Web Application Firewall анализирует весь доступ пользователей к критичным для вашего бизнеса приложениям и защищает ваши приложения и данные от кибератак. SecureSphere Web Application Firewall динамически обучается понимать «нормальное» поведение ваших приложений и коррелирует его с аналитической информацией об угрозах, собранной по всему миру и обновляемой в реальном времени для создания наилучшей защиты.

Лидирующий в индустрии[1] МСЭ веб-приложений SecureSphere идентифицирует и реагирует на угрозы, содержащиеся в безобидно выглядящем трафике – трафике, который может легко преодолеть традиционные средства защиты. Это позволяет предотвратить атаки на уязвимости приложений, такие как SQL инъекции, межсайтовый скриптинг и удаленную вставку файлов; атаки на бизнес-логику, такие как сбор данных с сайта и спам-комментарии; ботнеты и атаки DDoS; а также попытки завладеть учетной записью до того момента, когда мошенничество сможет быть реализовано.

[1] Gartner's Magic Quadrant для межсетевых экранов веб-приложений, 15 июля 2015



Доступны следующие аналитические сервисы ThreatRadar:

- **Репутационный сервис** – фильтрует трафик на основании последних данных о репутации источника, полученных в реальном времени;
- **Коллективная оборона** – использует в качестве дополнительного источника аналитической информации данные от сообщества пользователей решений Imperva;
- **Защита от ботов** – обнаруживает клиентов ботнетов и атаки «распределенный отказ в обслуживании» на приложения;
- **Защита от захвата аккаунта** – защищает учетные записи пользователей на веб-сайтах от атак и захвата;
- **Предотвращение мошенничества** – упрощает внедрение лучших в своем классе решений партнеров по защите от мошенничества.

Возможности решения Imperva SecureSphere

Автоматизированное обучение поведению пользователей и приложений

Для точного обнаружения атак МСЭ веб-приложений должен понимать структуру приложения, его элементы и ожидаемое поведение пользователя. Запатентованная компанией Imperva технология Динамического Профилирования (Dynamic Profiling) позволяет автоматизировать этот процесс путем создания профилей защищаемых приложений и построения «базового уровня» или «белого списка» допустимого поведения пользователей. Также система автоматически обучается тому, что время от времени приложение изменяется. Динамическое Профилирование позволяет исключить ручное конфигурирование и обновление многочисленных атрибутов приложения: URL, параметров, куки и методов.

Политики безопасности как результат исследований

Используя Центр Защиты Приложений Imperva (Application Defense Center, ADC) - всемирно признанную исследовательскую организацию по безопасности, SecureSphere предлагает наиболее полный набор сигнатур приложений и доступных политик. Imperva ADC изучает уязвимости, анонсируемые Bugtraq, CVE®, Snort® и подпольными форумами, а также проводит собственные исследования в целях выработки наиболее современной и исчерпывающей аналитической информации и методов защиты от атак на приложения.

Гибкие схемы развертывания

Решение SecureSphere может быть развернуто в виде физического устройства, виртуального устройства, в среде Amazon Web Services или как гибрид вышеуказанного. Варианты размещения отличаются чрезвычайной гибкостью, в том смысле что SecureSphere может быть развернуто в прозрачном режиме, практически не требуя внесения изменений в сеть. Кроме того, детализированные настройки политик позволяют с высочайшей точностью и беспрецедентным контролем соответствовать требованиям специфической политики безопасности организации.

Глубокий анализ угроз

Для защиты от хорошо подготовленных современных киберпреступников жизненно необходимо располагать передовой системой оповещения, которая распознает и защищает от постоянно эволюционирующих веб-атак. Система Imperva ThreatRadar[2] постоянно снабжает МСЭ веб-приложений SecureSphere Web Application Firewall аналитической информацией об угрозах, полученной в реальном времени от различных источников во всем мире и обработанной в Центре Защиты Приложений. ThreatRadar предоставляет наилучшую защиту, увеличивает точность МСЭ веб-приложений и повышает эффективность работы команды безопасности за счет проактивной фильтрации трафика от известных «плохих» источников, что позволяет специалистам по безопасности сконцентрироваться на том, что действительно является важным.

Виртуальные «заплатки»

SecureSphere может устанавливать виртуальные «заплатки» для ваших веб-приложений путем интеграции со сканером уязвимостей. Вместо того чтобы оставлять веб-приложение открытым для атак на недели и месяцы, ожидая модификации кода после обнаружения уязвимости в нем, виртуальные «заплатки» активно защищают веб-приложения от атак, уменьшая «окно доступности» и снижая затраты на внеплановые циклы обслуживания до момента, когда вы сможете установить штатные «заплатки».

Защита протокола HTTP, платформы и XML

SecureSphere контролирует соответствие протокола HTTP стандарту для предотвращения эксплуатации его уязвимостей и использования технологий обхода защиты. Детальные политики позволяют администраторам следить за строгим соответствием протокола стандартам RFC или допускать минимальные отклонения от них. Используя более 8000 сигнатур, SecureSphere защищает всю инфраструктуру, включая приложения и ПО веб-сервера. Гибкие и автоматизируемые политики безопасности XML защищают веб-сервисы, SOAP, веб-сокеты HTML 5 и приложения Web 2.0.

Точные политики корреляции снижают уровень ложных тревог

SecureSphere различает атаки от необычного, но легитимного поведения путем корреляции веб-запросов на всех уровнях безопасности в различные моменты времени. Функционал SecureSphere Correlated Attack Validation исследует многие атрибуты, такие как соответствие протокола HTTP стандартам, нарушения профиля, сигнатуры, специальные символы и репутацию пользователя, для того чтобы выдать точное оповещение или блокировать атаку с минимальным в индустрии уровнем ложных срабатываний. В качестве атрибута также могут применяться данные ThreatRadar, для того чтобы быть уверенными в использовании самой последней информации о ландшафте угроз.

Кастомизируемые отчеты по соответствию и криминалистике

Богатые возможности по предоставлению отчетов SecureSphere помогают клиентам легко оценить состояние безопасности и соответствие регулирующим требованиям. SecureSphere предоставляет как предопределенные, так и полностью кастомизируемые формы отчетов. Это позволяет вам легко понять состояние вашей защиты и упростить демонстрацию соответствия требованиям PCI, SOX, HIPAA и FISMA, а также другим стандартам.

Мониторинг для глубокого анализа атак

Сигналы оповещения могут быть легко найдены, отсортированы и непосредственно привязаны к соответствующим правилам безопасности. Функционал SecureSphere по мониторингу и отчетности дает возможность непосредственно увидеть широкую картину безопасности, соответствия регулирующим требованиям и проблемам доставки контента. Панель реального времени предоставляет высокоуровневый взгляд на состояние системы и события безопасности.

[2] Информация от ThreatRadar доступна на базе годовой подписки

Киберзащита Imperva SecureSphere

Imperva SecureSphere – это целостная интегрированная платформа безопасности, включающая в себя решения SecureSphere по безопасности веб, баз данных и файлов, масштабируемая для соответствия требованиям центров обработки данных даже крупнейших организаций. Ее развитие обеспечивается исследовательской организацией по безопасности мирового класса - Центром Защиты Приложений (Imperva Application Defense Center), которая поддерживает продукт на передовом крае защиты от постоянно эволюционирующих угроз.

IMPERVA SECURESPHERE

ПРОДУКТЫ ДЛЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ	
SecureSphere Web Application Firewall	Точная, автоматизированная защита от онлайн-угроз
SecureSphere ThreatRadar	Глобальная аналитическая информация в реальном времени для обнаружения, фильтрации и блокирования известного «плохого» трафика
ПРОДУКТЫ ДЛЯ ЗАЩИТЫ БАЗ ДАННЫХ	
Database Activity Monitor	Полный аудит и обзор использования данных в БД
Database Firewall	Мониторинг активности и защита в реальном времени для критичных БД
Database Assessment	Оценка уязвимости, управление конфигурациями и классификация данных для БД
User Rights Management for Databases	Пересмотр и управление правами доступа пользователей к критичным БД
ADC Insights	Предустановленные отчеты и правила по безопасности и соблюдению требований для SAP, Oracle EBS и PeopleSoft
ПРОДУКТЫ ДЛЯ ЗАЩИТЫ ФАЙЛОВ	
File Activity Monitor	Полный аудит и обзор использования данных в файлах
File Firewall	Мониторинг активности и защита в реальном времени для критичных данных в файлах
User Rights Management for Files	Пересмотр и управление правами доступа пользователей к критичным файлам
Directory Services Monitor	Аудит, оповещения и отчеты об изменениях, сделанных в Microsoft Active Directory
ПРОДУКТЫ ДЛЯ ЗАЩИТЫ SHAREPOINT	
SecureSphere for SharePoint	Обзор и анализ прав доступа и использования данных в SharePoint, а также защита от веб-угроз
ПРОДУКТЫ ДЛЯ УПРАВЛЕНИЯ	
MX Management Server	Единый интерфейс для управления, мониторинга и отчетности по активности на множестве шлюзов SecureSphere
Manager of Managers	Объединяет в федерацию мультидоменные и многоклиентские среды, развернутые с множеством серверов управления MX