Обеспечение безопасности веб-приложений

Защита критичных веб-приложений

Обеспечение защиты веб-приложений от угроз в Интернете

Веб-приложения — основная мишень интернет-атак, поскольку они широко доступны и обеспечивают доступ к ценным данным. Чтобы противостоять сложным и распределенным атакам, предприятия должны обеспечить защиту своих веб-сайтов от постоянно возникающих угроз, не снижая при этом производительность и доступность приложений.

Все больше организаций доверяют защиту своих критичных приложений компании Imperva. Imperva Web Application Security эффективно интегрируется в физические, виртуальные и облачные центры обработки данных и обеспечивает самую продвинутую защиту, адаптируясь к изменяющимся угрозам благодаря исследованиям и аналитике больших данных.

Imperva SecureSphere

Передовое решение SecureSphere Web Application Firewall принципиально изменило концепцию защиты бизнес-приложений за счет внедрения автоматических процессов обеспечения безопасности в Интернете, а также гибкого и прозрачного развертывания. Комплексная защита и низкие административные расходы — вот что делает SecureSphere идеальным решением для защиты ценных веб-ресурсов и соблюдения требований стандартов PCI. Imperva SecureSphere доступно в виде физических или виртуальных устройств, а также в Amazon Web Services.

Продукты

SecureSphere Web Application Firewall

ThreatRadar Reputation Services

ThreatRadar Fraud Prevention

DDoS Protection Service

Imperva Incapsula

Соответствие стандартам PCI 6.6

- SecureSphere Web Application Firewall помогает тысячам предприятий выполнять требования стандартов PCI 6.6.
- Постоянная автоматическая защита.
- Предустановленные и настраиваемые формы отчетов для соблюдения требований регуляторов.
- Виртуальный патчинг уязвимостей для обеспечения надежной защиты.
- Соблюдение требований стандартов PCI в сфере аудита и контроля прав доступа пользователей с помощью Database Firewall.

Возможности решений Imperva SecureSphere

Автоматическое изучение приложений и действий пользователей систем

Чтобы точно определять атаки, межсетевой экран веб-приложений должен понимать структуру и элементы приложения, а также ожидаемые действия пользователей. Запатентованная технология динамического профилирования Imperva выполняет эти операции автоматически, создавая профили защищаемых приложений и формируя эталон, или «белый список», допустимых действий пользователей. Она также автоматически запоминает изменения, которые в разное время вносятся в приложения. Механизм динамического профилирования исключает необходимость настраивать и обновлять вручную огромное число URL-адресов, параметров, файлов cookie и процедур приложений.

Политики безопасности на основе данных исследований

SecureSphere предлагает самый полный набор сигнатур и политик приложений благодаря эффективному применению базы знаний Imperva Application Defense Center — международного исследовательского центра по вопросам обеспечения безопасности. Специалисты ADC изучают отчеты Bugtraq, CVE®, Snort®, информацию с форумов и проводят первичные исследования, предоставляя самые актуальные комплексные решения для защиты от интернет-атак.

Адаптируемая защита от крупномасштабных автоматических атак

Дополнительный сервис ThreatRadar Reputation Services — это эффективный инструмент защиты от автоматических атак и ботнетов. ThreatRadar оперативно собирает данные об известных источниках атак, бот-сетях, фишинговых страницах и анонимайзерах и блокирует вредоносный трафик еще до попытки совершения атаки. Используя актуальные данные системы геопозиционирования, организации могут ограничивать доступ в зависимости от географического положения.

Дополнительный сервис ThreatRadar Community Defense предоставляет ценную информацию для защиты от угроз, полученную на основе анализа данных атак, поступающих от других устройств SecureSphere Web Application Firewall.

Защита от DDoS-атак

Хотя SecureSphere Web Application Firewall предотвращает DDoS –атаки на уровне приложений, массированные флад-атаки, совершаемые на уровне сети, могут парализовать работу сайтов и существенно снизить пропускную способность. Именно поэтому блокировать этот тип угроз следует в облаке — прежде, чем они смогут достигнуть сеть предприятия. DDoS Protection Service for SecureSphere — это надежный высокопроизводительный сервис, обеспечивающий защиту организаций от разрушительных DDoS-атак. Сервис быстро развертывается, а благодаря возможности масштабирования может справляться с массированными мультигигабитными атаками.

Виртуальный патчинг с помощью интеграции со сканерами уязвимости

SecureSphere обеспечивает моментальный патчинг уязвимостей приложений, при помощи импорта результатов анализа уязвимостей, полученных из WhiteHat, IBM, Cenzic, NT OBJECTives, Qualys и других систем сканирования, а также дает возможность создания кастомных политик для блокировки известных уязвимостей. Применение «виртуальных заплаток», или виртуальный патчинг, значительно снижает риск утечки данных и расходы на исправление и тестирование исправлений.

Защита от мошенничества, совершаемого с помощью вредоносного ПО

ThreatRadar Fraud Prevention, дополнительный сервис для SecureSphere Web Application Firewall, позволяет организациям быстро разворачивать и управлять инструментами защиты от мошенничества без необходимости обновлять веб-приложения. Благодаря интеграции с ведущими решениями защиты от мошенничества, SecureSphere может обнаруживать и блокировать мошеннические операции. Этот сервис также предоставляет широкие возможности для мониторинга и контроля, которые помогают организациям централизованно управлять WAF и политиками защиты от мошенничества.

Защита трафика HTTP и XML

SecureSphere проверяет HTTP-трафик на соответствие стандартам, предотвращая применение эксплоитов и техники обхода. Тонкая настройка политик защиты позволяет администраторам либо обеспечить строгое выполнение требований RFC, либо допустить незначительные отклонения от них. Благодаря базе, включающей более 8 000 сигнатур, SecureSphere может надежно защитить всю инфраструктуру приложений, включая программное обеспечение приложений и веб-серверов. Гибкие и оперативно обновляемые политики защиты XML обеспечивают эффективную защиту веб-служб, приложений SOAP и Web 2.0.

Детальные политики корреляции при минимальных ложных результатах

SecureSphere способна отличать атаки от необычного, но легитимного трафика с помощью механизма корреляции веб-запросов на всех уровнях защиты в течение длительного времени. Технология Correlated Attack Validation анализирует большое число атрибутов (таких, например, как параметры HTTP-протокола, нарушения параметров профиля, сигнатуры атак, специальные символы и репутационная оценка источников запросов) для точного обнаружения или блокировки атак, обеспечивая самый низкий в отрасли уровень ложных срабатываний.

Настраиваемые отчеты для соблюдения требований и расследования инцидентов

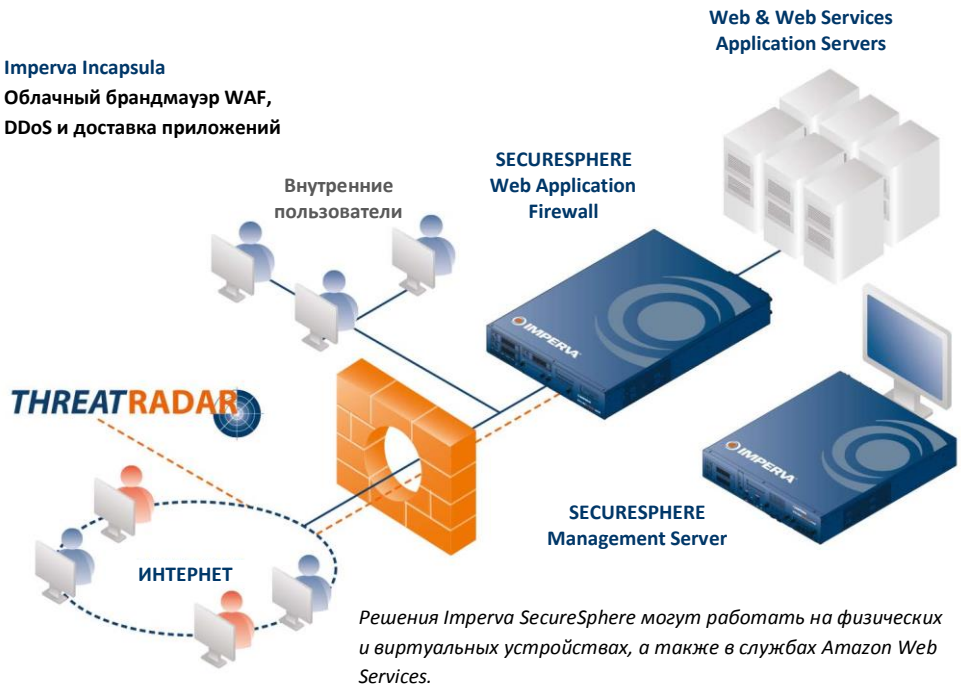
SecureSphere обладает широкими возможностями для создания отчетов, позволяя заказчикам легко оценивать уровень защиты и соблюдать нормативные требования. Система содержит как предустановленные, так и настраиваемые формы отчетов. Можно просматривать отчеты в любое время, либо настроить их отправление по электронной почте по графику: ежедневно, еженедельно или ежемесячно.

Мониторинг и глубокий анализ атак

Интерфейс SecureSphere позволяет с легкостью находить, сортировать и сопоставлять оповещения об атаках с соответствующими политиками защиты. Механизмы мониторинга и создания отчетов обеспечивают мгновенный анализ уровня защиты, соответствия стандартам безопасности и проблем с доставкой контента. Панель мониторинга в реальном времени позволяет получить общую картину о состоянии системы и событиях безопасности.

Imperva Incapsula

Imperva Incapsula — это простое и экономичное решение, которое включает Web Application Firewall, сертифицированный по стандартам PCI, средства защиты от DDoS-атак, балансировки нагрузки и отказоустойчивости для работы в глобальной сети доставки контента. Imperva Incapsula не требует установки дополнительного оборудования, программ или настройки приложений. Подразделения или организации могут использовать это решение без необходимости привлечения ИТ-отдела или специалистов по безопасности. Внеся незначительные изменения в параметры DNS, они могут быть уверены в безопасности своих веб-приложений и данных.



Решения Imperva SecureSphere могут работать на физических и виртуальных устройствах, а также в службах Amazon Web Services.

Варианты развертывания SecureSphere

- **Transparent Layer 2 Bridge.**

  Блокировка вредоносного трафика и лучшая в отрасли производительность.

- **Reverse Proxy and Transparent Proxy.**

  Изменение контента, например, подписывание файлов cookie и перезапись URL-адресов.

- **Non-inline Monitor.**

  Мониторинг и расследование инцидентов безопасности с нулевым риском.

- **High Availability.**

  Интерфейсы IMPVHA, VRRP, Fail-Open, существующие варианты резервирования, развертывание в качестве внешнего компонента (non-inline).

Imperva SecureSphere для защиты центров обработки данных

Imperva SecureSphere — это комплексная, интегрированная платформа безопасности, в состав которой входят компоненты SecureSphere для защиты веб-приложений, баз данных и файлов. Она масштабируется в соответствии с требованиями безопасности центров обработки данных и подходит для использования в самых крупных средах, а обновление данных и политик, осуществляемое специалистами международного исследовательского центра Imperva Application Defense Center, обеспечивает защиту от угроз с помощью самых передовых средств.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

Web Application Firewall

Надежная автоматизированная защита от интернет-угроз.

ThreatRadar Reputation Services

Эффективный механизм репутационной защиты, обеспечивающий блокировку доступа для злоумышленников и предотвращающий автоматические атаки.

ThreatRadar Community Defense

Ценная информация для защиты от угроз, полученная от пользователей, работающих с продуктами SecureSphere по всему миру.

ThreatRadar Fraud Prevention

Быстрый и эффективный способ блокировки вредоносного ПО и предотвращения взломов учетных записей.

Incapsula SaaS WAF и DDoS Protection

Передовые средства защиты веб-приложений и доставки контента-услуги.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ БАЗ ДАННЫХ

Database Activity Monitor

Комплексный аудит и мониторинг работы пользователей с базами данных.

Database Firewall

Отслеживание действий и защита критичных баз данных в реальном времени.

Database Assessment

Оценка уязвимости, управление конфигурациями и классификация информации для баз данных.

User Rights Management for Databases

Анализ и контроль прав доступа пользователей к критичным базам данных.

ADC Insights

Встроенные отчеты и правила для соблюдения требований стандартов безопасности и защиты бизнес-приложений SAP, Oracle EBS и PeopleSoft.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ФАЙЛОВ

File Activity Monitor

Комплексный аудит и мониторинг работы пользователей с файлами.

File Firewall

Отслеживание действий и защита критичных файловых данных.

User Rights Management for Files

Анализ и контроль прав доступа пользователей к критичным файлам.

Directory Services Monitor

Аудит изменений в Microsoft Active Directory, оповещение и составление отчетов по ним.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ИНФРАСТРУКТУРЫ SHAREPOINT

SecureSphere for SharePoint

Мониторинг и анализ прав доступа и использования данных в системе SharePoint, а также защита от интернет-угроз.

IMPERVA

NETWELL
Официальный дистрибьютор

115114, Москва,
1-й Дербеневский пер., д. 5
Тел.: +7 (495) 66 239 66
www.netwell.ru