

## Общее описание продукта

Splunk - это универсальная поисковая система, позволяющая осуществлять сбор, хранение и аналитическую обработку данных, представленных на всех уровнях ИТ инфраструктуры - физическом, виртуальном и 'облачном'.

ИТ данные являются одним из важнейших информационных ресурсов для бизнеса, аккумулируя сведения о транзакциях пользователей, операционной деятельности ИТ (включая профили активности пользователей и показатели производительности ИТ-систем), создавая индикаторы угроз безопасности и потенциального мошенничества и т.п. Большая часть этой информации зачастую представлена в динамически меняющемся, неструктурированном формате, при этом составляя основной объем данных в организации.

Компаниям редко удается получить реальную отдачу от владения громадными объемами ИТ данных. Существующие средства анализа, управления и мониторинга не предназначены для обработки больших объемов динамически меняющейся неструктурированной информации.

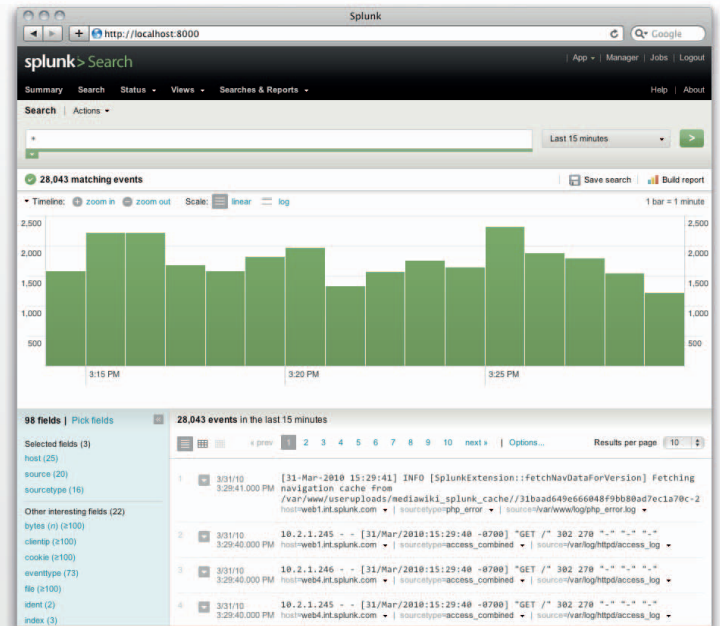
Основатели Splunk ставили задачу создания единого универсального средства для обработки всего объема данных, генерируемых ИТ-системами, на основе сбора, индексации и хранения этих данных в виде последовательности событий, снабженных метками времени. Splunk осуществляет поиск, мониторинг и анализ проиндексированных данных из единой точки в режиме реального времени, что позволяет оперативно получать информацию о состоянии дел в ИТ, и не только в ИТ.

Splunk можно также использовать как средство визуализации и аналитической обработки данных. Устранение неисправностей и расследование инцидентов безопасности с помощью Splunk занимает всего несколько минут вместо нескольких часов или дней, что позволяет существенно повысить уровень обслуживания клиентов, избежать непроизводительных простоев вследствие сбоев в ИТ-инфраструктуре, обеспечить соответствие требованиям регуляторов и получить новый уровень "видения" вашего бизнеса.

## Возможности Splunk

**Индексация любых данных, полученных из любого источника.** Splunk позволяет индексировать данные, полученные из любого источника в любом формате. Это могут быть данные, генерируемые приложениями собственной разработки, web-серверами, базами данных, сетевыми устройствами, операционными системами, и а также многое другое. Вне зависимости от формата источника, Splunk индексирует все данные единым образом, что исключает необходимость разработки специализированных парсеров/коннекторов, а также их последующей поддержки и модификации в случае изменения исходных форматов. Splunk индексирует данные очень быстро и легко масштабируется до решения корпоративного уровня, обрабатывающего 100% вашей ИТ информации. Ни один продукт, предназначенный для поиска и индексации данных, не обладает подобной гибкостью и быстродействием. Делаем выводы.

**Поиск и анализ "чего-угодно".** Splunk позволяет осуществлять поиск по данным реального времени и историческим данным из единого центра и отслеживать транзакции, проходящие через множество различных ИТ систем. Система позволяет осуществлять поиск по специфическим полям и шаблонам данных и использовать логические операции для уточнения области поиска. Мощный механизм статистической обработки и формирования отчетов позволяет обновлять данные о транзакциях, вычислять метрики и отслеживать изменение параметров с непрерывным отображени-



ем результатов на панели мониторинга. Встроенный помощник облегчает построение поисковых запросов, в зависимости от контекста, предлагая наиболее часто используемые варианты.

### Анализ результатов поиска в режиме реального времени.

Путем расширения/сужения временных границ поиска, Splunk позволяет легко обнаруживать тренды, пики и аномалии в ИТ данных. Итеративный поиск "вглубь" реализуется простым нажатием кнопки мыши, позволяя в считанные секунды убрать шумовые эффекты и найти "иголку в стоге сена", не тратя утомительные часы на обращения в другие подразделения компании за необходимой информацией. Поиск в режиме реального времени означает, что вы можете выполнять корреляцию, анализ ИТ данных и реагировать на события без задержки. Это позволяет отслеживать транзакции и текущую активность пользователей, оперативно обнаруживать угрозы и реагировать на них, а также осуществлять мониторинг параметров SLA.

**Извлечение знаний.** Splunk автоматически извлекает необходимую информацию из ваших ИТ данных непосредственно во время поиска, что позволяет начать использовать новый источник данных немедленно. Вы также можете добавить контекст к вашим данным путем именованной и тегирования полей и различных элементов данных. Добавив информацию из внешних источников - баз данных учета информационных ресурсов, управления конфигурациями ИТ систем, а также пользовательских каталогов - вы можете сделать представление данных более "понятным" для широкой аудитории.

**Мониторинг и оповещения.** Вы можете преобразовать результат поиска в оповещение в режиме реального времени, которое автоматически запускает действия типа отправки почтового сообщения или запуска скрипта для устранения неисправности. Оповещения могут также генерировать SNMP-сообщения для различных систем управления и регистрировать запросы на обслуживание в службе поддержки. Вы можете формировать оповещения на основе пороговых данных, условиях, базирующихся на выявленных трендах, а также разнообразных сценариях, как например, атака с посредством подбора пароля или различные варианты компьютерного мошенничества.

**Отчетность и аналитика.** Мастер отчетов Splunk позволяет быстро строить диаграммы, графики и информационные панели, отражающие основные тренды, пороговые значения и частотные

характеристики ИТ данных, что позволяет создавать информационно-наполненные отчеты “с нуля”, без каких-либо дополнительных знаний о расширенных возможностях языка поисковых запросов. При этом вы можете “провалиться вглубь” из любого места диаграммы, чтобы получить непосредственный доступ к исходным данным. Вы можете сохранить отчет, интегрировать его в панель мониторинга, или рассылать его на периодической основе для распространения полученной информации среди менеджмента, бизнес-пользователей и других заинтересованных лиц.

**Панели мониторинга и представление данных.** Создайте свою собственную панель мониторинга всего несколькими нажатиями кнопки мыши с использованием встроенного редактора. Панели могут включать несколько диаграмм и различных вариантов отображения ИТ данных в реальном времени в соответствии с требованиями различных пользователей. Вы можете персонализировать панели для менеджмента, бизнес-аналитиков и специалистов по ИБ, аудиторов, разработчиков ПО и системных администраторов.

**Приложения Splunk.** Splunk предоставляет широкие возможности для создания специализированных приложений, использующих функционал базовой платформы. Они воплощают практический опыт множества пользователей для различных ролей и случаев использования Splunk. Создав приложение, Вы можете сделать его доступным для других категорий пользователей внутри вашей организации, а также поделиться им с остальной частью сообщества Splunk. Постоянно увеличивающееся число приложений доступно для скачивания с сайта сообщества Splunk ([www.splunkbase.com](http://www.splunkbase.com)) и включает в себя разработки членов сообщества, партнеров и самой компании. Приложения покрывают широкий спектр областей применения, и ИТ-платформ и технологий, таких как Windows, Linux, Unix, средства виртуализации, сетевые устройства и др.

**Масштабирование до размера ИТ инфраструктуры предприятия.** Splunk легко масштабируется с инсталляции на одном “обычном” сервере Windows, Linux или Unix, до решения, индексирующего данные нескольких центров обработки данных (ЦОД), расположенных в различных географических зонах и генерирующих десятки терабайт данных в день. Архитектура Splunk базируется на технологии MapReduce, позволяющей линейно масштабировать решение с использованием стандартного оборудования для обработки неограниченных объемов данных.

**Ограничение доступа к данным.** Для ограничения доступа к данным Splunk использует механизм ролей, определяющих пространство поиска, доступное пользователю. Так, например, пользователям в конкретных регионах доступны ИТ данные только своего региона, в то время как пользователи глобального уровня могут анализировать информацию, полученную из ЦОД, расположенных в любой точке мира. Splunk позволяет каждому авторизованному пользователю получать данные, которые ему необходимы для решения конкретной прикладной задачи - начиная от расследования инцидентов, мониторинга и отчетности, анализа и улучшения операционной деятельности ИТ до предоставления значимой информации для бизнеса.

**Защищенный доступ к данным и Single Sign-on.** В основу Splunk заложена надежная модель безопасности данных. Каждая транзакция Splunk обладает уникальным идентификатором, будь то внутренняя активность системы, активность веб-пользователей или интерфейсы командной строки. Splunk легко интегрируется с LDAP-совместимыми каталогами и Active Directory для использования корпоративных политик безопасности. Интеграция с широко распространенными SSO-решениями обеспечивает сквозную аутентификацию пользователей. Поскольку все необходимые для расследования инцидентов и обеспечения соответствия требованиям регуляторов данные сохраняются в Splunk, вы можете существенно ограничить доступ к критичным информационным ресурсам.

**Splunk – это программа.** Splunk – это программное обеспечение корпоративного уровня, с которым легко работать. Скачайте и установите его на свой компьютер всего за 5 мин. Начав таким образом использовать Splunk, вы можете затем легко масштабировать его до размеров корпоративного ЦОД. И вот вы уже готовы использовать мощный поисковый движок Splunk через удобный и интуитивный веб-интерфейс.

## Бесплатная версия Splunk

Скачайте бесплатную версию Splunk сайта компании-производителя [www.Splunk.com](http://www.Splunk.com) – и вы автоматически получите весь функционал корпоративной версии на период до 60 дней, а также сможете индексировать до 500 Мб данных ежедневно. После 60 дней или ранее, вы можете изменить лицензию на бесплатную бессрочную или приобрести корпоративную лицензию, чтобы продолжать пользоваться расширенным функционалом продукта, позволяющим работать в многопользовательском режиме.

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	500MB	Unlimited (based on license)
Universal, real-time indexing	✓	✓
Real-time and historical search	✓	✓
Reporting	✓	✓
Knowledge mapping	✓	✓
Dashboards	✓	✓
Monitoring and alerting		✓
Distributed search		✓
Data forwarding and receiving	✓	✓
Role-based access controls		✓
Single sign-on		✓
Developer APIs	✓	✓
Community Apps	✓	✓
Enterprise Apps		✓
Standard support	✓	✓
Enterprise support		✓

## Требования к системе

### Server Operating System

- **Unix:** Linux (kernel version 2.6x and above (x86, 32- and 64-bit); AIX 5.2 and 5.3; HO-UX 11iv2 (11.22) and 11iv3 (11.31) (PA-RISC or Itanium); Solaris 9,10 (x86 SPARC); FreeBSD 6.1 and 6.2 (x86, 32- and 64-bit)
- **Windows:** XP (32-bit); Vista (32-bit and 64-bit); Windows 7 (32-bit and 64-bit); Windows Server 2003 (64-bit), Windows Server 2008 (64-bit)
- **Mac:** MacOSX 10.5 (32-bit and 64-bit); MacOSX 10.6 (32-bit mode)

### Server Hardware

- 2x quad-core Xeon, 3GHz, 8GB RAM (recommended)

### Storage

- 12-48% of raw data size depending on indexing density/data source

### Supported Browsers

- Firefox 2.0+ / Windows, Linux and Mac OSX; IE 6+/Windows; Safari 4

## Контакты

Адрес во всемирной паутине: [www.splunk.com](http://www.splunk.com)

Штаб-квартира: 250 Brannan St, San Francisco, CA, USA, 94107

Адрес электронной почты: [emea-sales@splunk.com](mailto:emea-sales@splunk.com)

Телефон: +1 866-438-7758 | +1 415-848-8400

Бесплатная версия программы: [www.splunk.com/download](http://www.splunk.com/download)