FORCEPOINT
POWERED BY Raytheon

Спецификация

# SureView® Analytics
# Операции по обеспечению безопасности

## КОРПОРАТИВНОЕ ПРИЛОЖЕНИЕ С НИЗКОЙ СОВОКУПНОЙ СТОИМОСТЬЮ ВЛАДЕНИЯ, СПОСОБНОЕ РЕАГИРОВАТЬ НА ИНЦИДЕНТЫ ПОСРЕДСТВОМ АНАЛИТИЧЕСКОГО ИССЛЕДОВАНИЯ И БЫСТРО МИНИМИЗИРОВАТЬ ИЗДЕРЖКИ И РИСКИ БРЕШЕЙ В БЕЗОПАСНОСТИ

### СВОЙСТВА И ПРЕИМУЩЕСТВА

- **Интегрированный поиск обеспечивает** доступность актуальной информации по всей компании при исследовании бреши в защите. Аналитики могут искать информацию на всех серверах баз данных, во всех документах, файловых системах, веб-страницах, серверах электронной почты и иных сторонних источниках данных.
- **Виртуальное хранилище данных** устраняет издержки и трудности хранения большого набора повторяющихся данных и стимулирует обмен информацией между отделами. Вопросы прав владения данными исключены благодаря контролю владельцем доступа к данным.
- **Независимый от платформы,** инструмент графического анализа используется для проверки соединений, закономерностей работы системы, тенденций, ассоциаций и скрытых сетей в любом количестве и типе источников данных. Данные представлены графически, что раскрывает глубинные связи и закономерности в аналитическом процессе.
- **Использование собственных ресурсов** при быстром реагировании на брешь в защите. Оперативный поиск для оценки влияния инцидента по всей инфраструктуре безопасности выполняется быстро и легко посредством разработанной интегрированной поисковой структуры, автоматизированной технологии поиска данных и передовых аналитических алгоритмов.
- **Предоставление руководству** ежедневных аналитических обзоров по безопасности с целью формирования целостного представления о корпоративной безопасности путем интегрирования исследовательской аналитики в имеющийся комплект аналитических систем безопасности.

### ЗАДАЧА

Сложность задачи устранения долгой задержки перед избавлением от брешей безопасности растет экспоненциально из года в год благодаря многим неуправляемым факторам. Мы наблюдаем существенное увеличение числа киберпреступников по всему миру. Целеустремленные хакеры превратились в хорошо оплачиваемый ресурс для транснациональных киберпреступных сетей, движимых финансовыми мотивами. Необходимость обработки больших объемов данных в процессе определения и исследования бреши защиты является одновременно преимуществом и трудностью. Более важным является то, что компания постоянно имеет дело с таким чрезвычайно искусным врагом, как хакеры, которые, оттачивают мастерство со временем во время своих атак. Также как перед сотрудниками службы безопасности стоит проблема необходимости постоянного участия в многочисленных расследованиях преступлений, мы параллельно используем компоненту, соответствующую ожиданиям корпорации о том, что служба безопасности обеспечит быструю реакцию на инцидент. Необходимость проводить операции по обеспечению безопасности своевременно, эффективно и результативно сейчас как никогда высока. Сотрудники службы безопасности ищут технологию, которая, с одной стороны, могла бы быстро преобразовать большие объемы данных в действенную аналитику безопасности для минимизации издержек и рисков атак, с другой стороны, обеспечивала бы низкую совокупную стоимость владения для компании.

### ПО SUREVIEW ANALYTICS

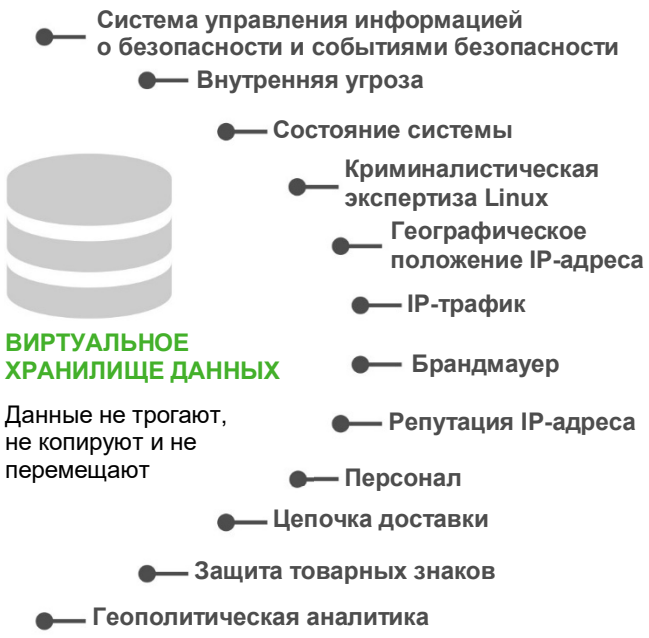
ПО SureView Analytics является комплексным приложением для борьбы с киберугрозами для быстрого снижения рисков и издержек брешей безопасности. Интегрированная поисковая технология ПО SureView Analytics' быстро обрабатывает огромные объемы информации корпорации и за доли секунды извлекает соответствующие результаты в виде понятных изображений. ПО SureView Analytics обеспечивает передовую аналитическую


Рисунок 1: Интегрированный поиск по всему массиву данных компании в сочетании с инструментами автоматического обнаружения и исследовательской аналитикой позволяет создать программы управления средствами защиты, которые предлагают быстрое реагирование на атаки на основе аналитических данных.

среду, которая предоставляет возможности всеобъемлющей визуализации данных и взаимодействия специалистов разного профиля, ускоряет реагирование на изощрённые атаки
(рисунок 1).

## ПОИСК ПО SUREVIEW ANALYTICS

**Интегрированный поиск легко соединяет локальные и удаленные источники данных, чтобы создать окончательное виртуальное хранилище данных, реализующее мгновенный доступ аналитиков ко всем данным, необходимым для** формирования цельной картины ситуации. ПО SureView Analytics не тратит много времени на получение внутренних разрешений на доступ к информации от различных подразделений корпорации, поскольку поиск происходит незаметно из-за отсутствия обработки огромных объемов данных в одном центральном местоположении. ПО SureView Analytics не копирует источники данных, но запрашивает нужные данные из нескольких источников, выполняя незаметным образом, безопасно и параллельно, извлечение ключевой информации по всей компании. При этом требования к существующей ИТ-инфраструктуре или воздействие на нее минимальны.




- **Мгновенный поиск** рабочих данных во внутренних и внешних БД, веб-сайтах, электронной почте или офисных документах гарантирует технология интегрированного поиска
- **Избавление от любых дорогостоящих запросов на хранение больших объемов данных** посредством концепции уникального виртуального хранилища данных, используемого при агрегации данных. Технология повторяет архитектуру традиционного хранилища данных, но при этом сохраняется контроль, безопасность и физическое владение данными в оригинальном источнике (данные не копируются и не перемещаются).
- **Соблюдение конфиденциальности данных и ограничений безопасности** посредством использования встроенного менеджера безопасности, определение параметров с уникальными полномочиями для отдельных пользователей или групп.
- **Быстрое выполнение поисковых запросов при минимальном взаимодействии с пользователем посредством функциональности, автоматизирующей повторяющиеся поисковые операции.**

**Настраивание типов результата,** который возвращает поисковая система при полнотекстовом индексировании, разработанном с учетом фонетических средств и синонимов

## РАБОЧИЙ ПРОЦЕСС ПО SUREVIEW ANALYTICS

Благодаря передовым возможностям визуализации система раскрывает нужную информацию управлению средствами защиты. Аналитический рабочий процесс ПО SureView Analytics' спроектирован для быстрого выделения соединений, которые могли сформировать зараженные сообщения, установления связей с подозрительным поведением системы и выявления закономерностей, тенденций и аномалий в данных. Платформа оптимизирует производительность модулей посредством автоматизированного поиска данных, функциональности оповещения и интегрированной аналитической БД для облегчения понимания больших объемов сложных данных и ускорения быстрого реагирования на атаки.

**Простое определение зараженных и других потенциально инфицированных узлов сети** посредством анализа связей, который обнаруживает передачу подозрительных сообщений в сети компании.

**Быстро выделяет подозрительную модель поведения или необычное поведение системы,** для которого необходимо дальнейшее исследование путем трассирования на протяжении длительного промежутка времени.

**Простое создание ежедневных информационных обзоров и обмен ситуационной осведомленностью о состоянии корпоративной безопасности на основе встроенных инструментов формирования отчетов.** Отчеты легко воспринимаются, поскольку функции *чертежей, маркировок, легенды* и *импорта изображений* общедоступны для настройки отчета.

**Обнаружение важных геопространственных корреляций бреши защиты** благодаря интегрированию ее географического положения со средствами геопространственной визуализации.

**Быстрое обнаружение данных** посредством многофункциональных инструментов поиска, использующих навигационный поиск дополнительно к прямому поиску для уменьшения шума.

**Обогащение данных посредством инструментов трансформации метаданных,** которые гармонизируют данные за счет их смыслового значения в реальном мире.

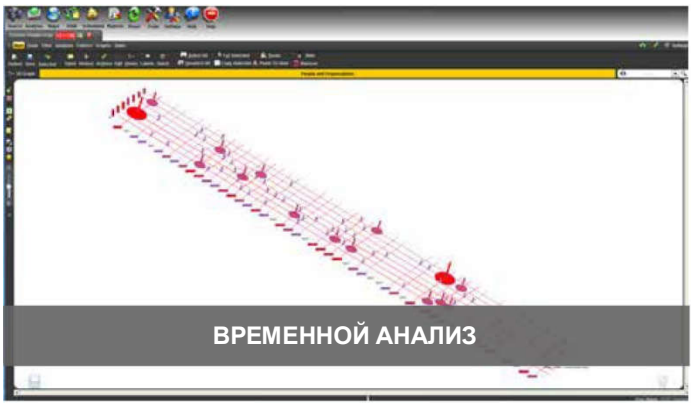



Рисунок 3: Временной анализ. Быстро выделяет подозрительную модель поведения или необычное поведение системы, для которого необходимо дальнейшее исследование путем трассирования на протяжении длительного промежутка времени.

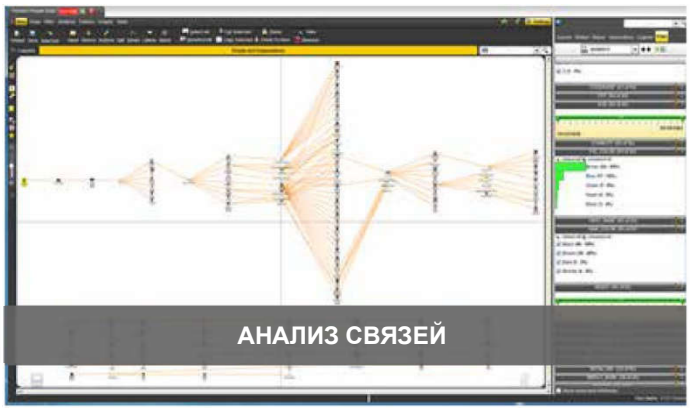



Рисунок 4: Анализ связей. Понимание передвижения предположительно зараженных сообщений по компании.

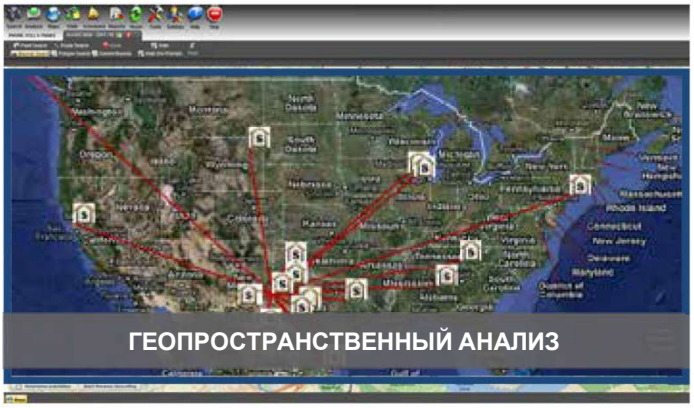



Рисунок 5: Геопространственный анализ. Обнаружение неизвестных взаимосвязей или важности информации благодаря географической корреляции или местоположению посредством интегрирования с геопространственной визуализацией.

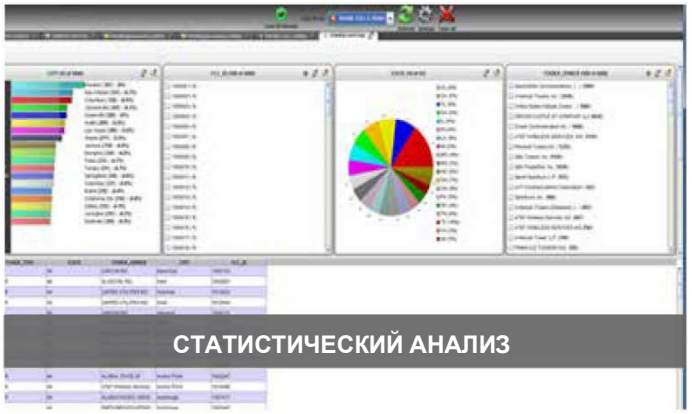
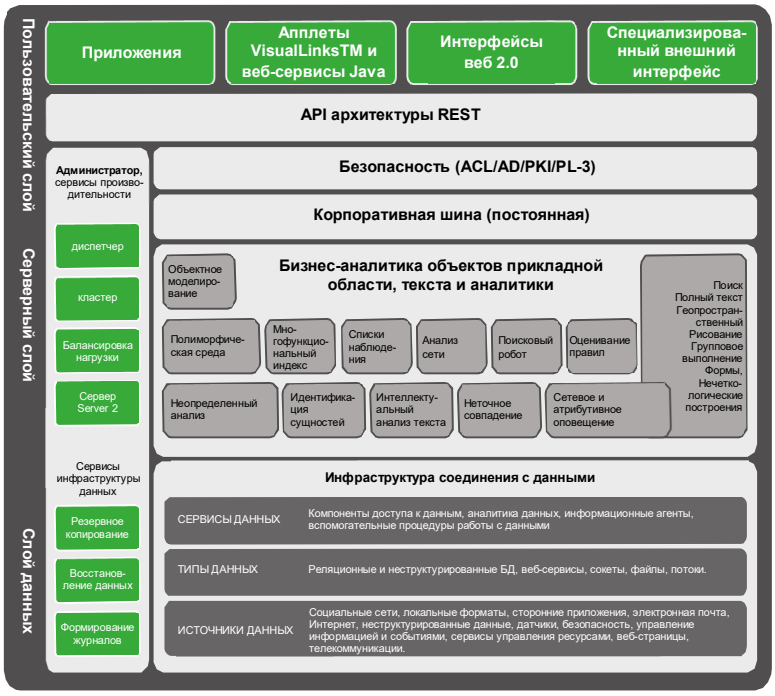



Рисунок 6: Статистический анализ. Обнаружение неожиданных всплесков активности или значений со статистическими представлениями из нескольких источников данных.




- **Минимальное воздействие на существующую ИТ-инфраструктуру.**
- **Создание виртуального хранилища данных.**
- **Клиент-серверное приложение, которое использует готовое аппаратное обеспечение.**
- **Дополнительный постоянный кэш.**
- **Выполняется на виртуальной машине.**
- **Простое интегрирование с существующими приложениями.**

Рисунок 7: Платформа SureView Analytics. Интегрированный поиск данных по всему предприятию в сочетании с инструментами автоматического обнаружения и исследовательской аналитики для быстрого реагирования на изощренные атаки.

## КОРПОРАТИВНОЕ ПРИЛОЖЕНИЕ С НИЗКОЙ СОВОКУПНОЙ СТОИМОСТЬЮ ВЛАДЕНИЯ

Платформа Forcepoint™ SureView Analytics имеет низкую совокупную стоимость владения и оказывает минимальное воздействие на существующую ИТ-инфраструктуру. Технология, являющаяся уникальной для своей отрасли, напрямую подключается к хранилищам оперативных данных и создает «виртуальное» хранилище данных, тем самым устраняя необходимость для ИТ отдела в поддержании еще одного хранилища данных большего объема, поскольку данные никогда не копируются и не перемещаются. ПО SureView Analytics является клиент-серверным приложением, использующим коммерческое готовое аппаратное обеспечение. Приложение имеет дополнительный постоянный кэш, который позволяет ему публиковать контент любой базы данных без опасения транзакционной нагрузки. Приложение может выполняться на виртуальной машине и просто интегрируется с другими приложениями.

## КОНТАКТНАЯ ИНФОРМАЦИЯ

**www.forcepoint.com/contact**

## О компании FORCEPOINT


[DATASHEET_SUREVIEW_ANALYTICS_SECURITY_OPS_EN] 100042.011416