

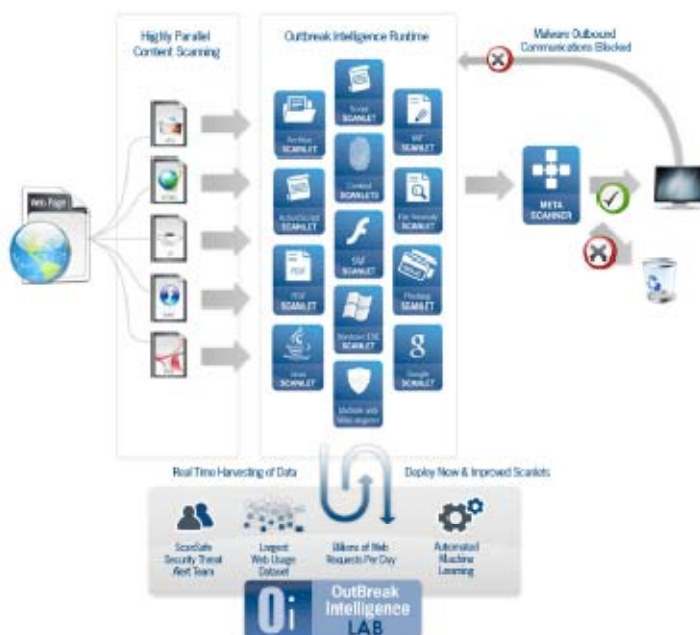
## ТЕХНИЧЕСКОЕ ОПИСАНИЕ ПРОДУКТА

# ScanSafe: решение для обеспечения безопасности web-трафика

По мере развития Интернета из набора статических ресурсов в индустриальную платформу, обеспечивающую двустороннее взаимодействие, увеличивался объем угроз информационной безопасности и вредоносного программного обеспечения, направленных на web-технологии. Хакеры постоянно обнаруживают уязвимости открытой и динамичной среды Интернета, чтобы распространять свое вредоносное программное обеспечение, не создавая специализированных web-сайтов. Заражение вредоносным программным обеспечением при посещении легитимного (но взломанного ранее) web-сайта – это не просто ежедневная реальность, это предпочитаемый хакерами способ атаки. Такое изменение методов атаки существенно снизило эффективность традиционных методов обеспечения информационной безопасности, например, антивирусов, и привело к необходимости разработать альтернативные методы.

### SaaS-решение для обеспечения безопасности web-трафика

Удостоенное множества наград SaaS-решение для обеспечения безопасности web-трафика, предлагаемое ScanSafe, обеспечивает защиту организаций любого размера от уже известных и совершенно новых атак. Решение ScanSafe, основанное на распределенном сетевом сервисе, позволяет повысить уровень защищенности и снизить затраты на 40%, поскольку организации не требуется приобретать, развертывать и поддерживать оборудование, обычно устанавливаемое на территории заказчика.



Решение ScanSafe для обеспечения безопасности web-трафика позволяет организациям создать гибкую глобальную политику обеспечения безопасности web-трафика, включая SSL-трафик. В политике безопасности могут учитываться категории web-сайтов, контент, типы файлов, временные параметры и квоты трафика. Кроме того, политика анализа исходящего трафика позволяет гарантировать, что конфиденциальные данные (например, сведения о заказчиках, номера кредитных карт и т. п.) не могут быть переданы из сети.

### Преимущества SaaS-решения для обеспечения безопасности web-трафика

- Защита конфиденциальной информации и вычислительных ресурсов
- Предотвращение совершенно новых атак на сетевые ресурсы
- Поддержка качественной работы конечных пользователей с интернет-ресурсами
- Снижение совокупной стоимости владения на 40%
- Высвобождение ИТ-специалистов для решения стратегических задач, стоящих перед организацией

Дополнительные сведения:  
[www.scansafe.com](http://www.scansafe.com)

«Некоторые средства обеспечения информационной безопасности лучше реализовывать с помощью распределенных сетевых сервисов. Это дешевле для потребителей и надежнее с точки зрения уровня защищенности.»

Джон Микин (John Meakin)  
Руководитель службы ИБ,  
STANDARD CHARTERED BANK

Решение ScanSafe для обеспечения безопасности web-трафика анализирует каждый запрос к интернет-ресурсам, чтобы проверить вредоносность контента, а также допустимость запроса в соответствии с заданной политикой безопасности. Такой подход позволяет обеспечить надежную защиту от уже известных и совершенно новых атак, которые в противном случае могли бы пройти успешно.

Решение ScanSafe для обеспечения безопасности web-трафика использует ядро Outbreak Intelligence®, реализующее множество технологий обнаружения вторжения, автоматизированных эвристических механизмов обучения и "модулей сканирования". Ядро Outbreak Intelligence формирует детализированное представление каждого web-запроса и оценивает риск безопасности, чтобы гарантировать безопасность пользователей решения ScanSafe.

### Outbreak Intelligence – защита от совершенно новых атак

Модули сканирования ядра Outbreak Intelligence анализируют все элементы web-запроса, включая HTML, JavaScript, Flash и активные скрипты. По результатам анализа формируются различные показатели уровня безопасности каждого конкретного запроса. Каждое ядро сканирования передает результаты своей работы в модуль Meta Scanner, который принимает окончательное решение о безопасности web-запроса.

Ядро Outbreak Intelligence сканирует более миллиарда web-запросов ежедневно, в режиме реального времени, блокируя миллионы экземпляров вредоносного программного обеспечения и защищая тысячи наиболее активных организаций по всему миру. Такой масштаб анализа реального интернет-трафика позволил создать крупнейшую в мире базу данных об использовании интернет-ресурсов, которая позволяет ScanSafe обеспечивать масштабирование в интересах своих заказчиков – способность более оперативного и точного анализа и обнаружения вредоносного программного обеспечения по сравнению с другими поставщиками решений в сфере информационной безопасности.

Эти факторы делают ядро Outbreak Intelligence наиболее эффективным решением для отражения совершенно новых интернет-атак.

### Централизованное управление и формирование отчетов

Решение ScanSafe для обеспечения безопасности web-трафика управляется с использованием интуитивно понятного web-интерфейса, ScanCenter, в который интегрированы все средства управления и формирования отчетов. С помощью ScanCenter администратор может создать глобальную политику безопасности всей организации, а также политики безопасности для конкретных групп пользователей. Все изменения политики распространяются в режиме реального времени.

ScanCenter обеспечивает формирование отчетов, содержащих сводные данные, сведения о трендах и сведения об обнаруженном вредоносном программном обеспечении.

### Высокопроизводительный сервис

Архитектура решения ScanSafe для обеспечения безопасности интернет-трафика обеспечивает высокопроизводительную и безопасную работу с интернет-ресурсами для всех пользователей организации. SaaS-платформа ScanSage, созданная на основе распределенной сети центров обработки данных, архитектуры параллельных вычислений, нескольких высокопроизводительных операторских сетей и расширенных средств резервирования, обеспечивает один из наиболее впечатляющих в отрасли показателей уровня обслуживания: непрерывность работы сервиса составляет 99,999%.

### Надежная защита удаленных сотрудников

Для сотрудников, работающих удаленно, можно обеспечить тот же уровень защищенности, что и для пользователей, расположенных в центральном офисе. Компонент Anywhere позволяет защитить системы, подключенные к Интернету из дома, из отеля или из кафе. Компонент Anywhere автоматически перенаправляет трафик пользователей в ближайший центр обработки данных, чтобы обеспечить высочайший уровень производительности.

### О корпорации ScanSafe

Корпорация ScanSafe является первопроходцем в области SaaS-решений в сфере информационной безопасности и глобальным поставщиком услуг по обеспечению безопасности web-трафика, позволяющих создать защищенную и эффективную интернет-среду для подключения предприятий. Решения ScanSafe препятствуют проникновению вредоносного программного обеспечения в корпоративные сети и позволяют предприятиям контролировать и защищать работу с интернет-ресурсами. SaaS-архитектура позволяет заказчикам существенно снизить совокупную стоимость решения. Многоуровневая система обнаружения угроз Outbreak Intelligence™ позволяет ежемесячно обрабатывать миллиарды web-запросов и миллионы блоков для заказчиков, работающих более чем в 100 странах.

Дополнительные сведения:

[www.scansafe.com](http://www.scansafe.com)

