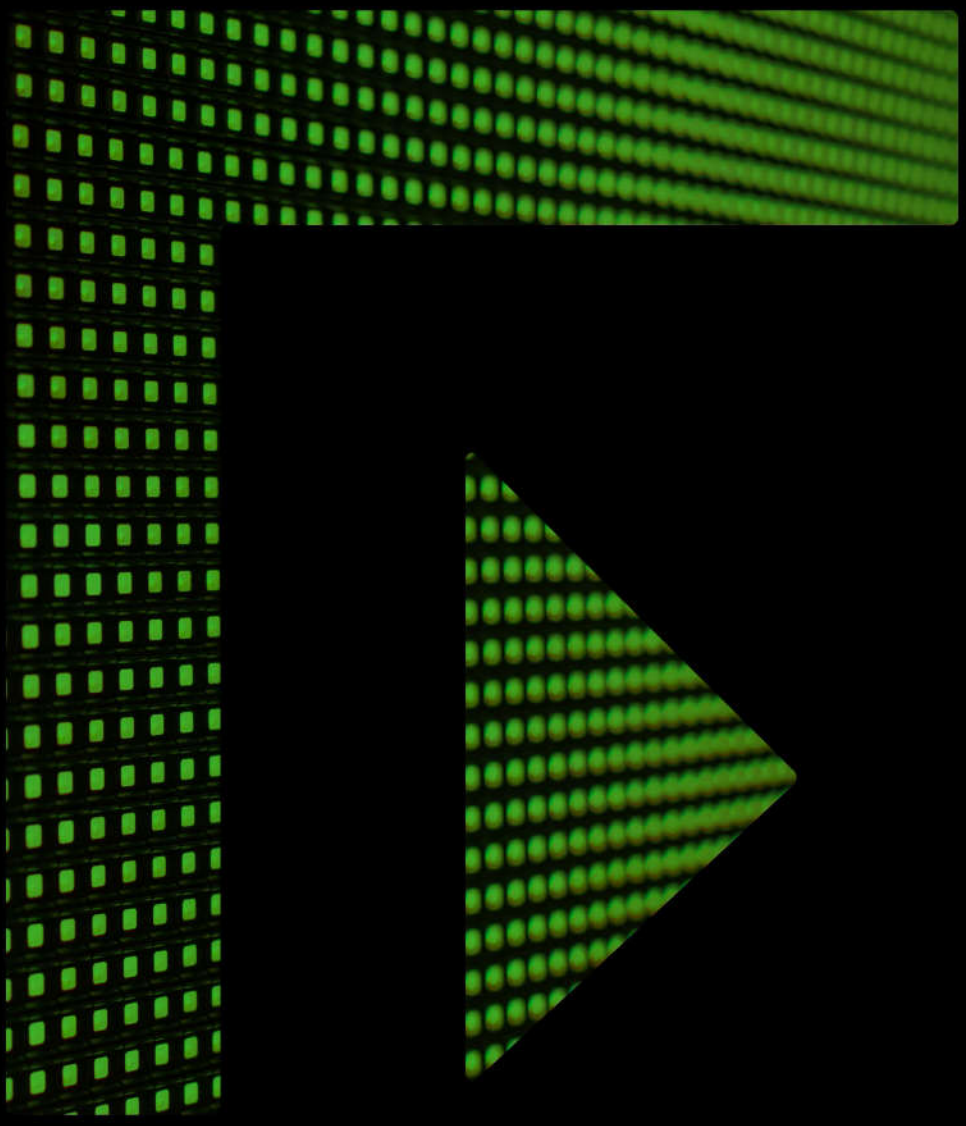


Forcepoint Email Security

БЕЗОПАСНОСТЬ ЛОКАЛЬНОЙ И ОБЛАЧНОЙ ЭЛЕКТРОННОЙ ПОЧТЫ ОТ КОМПАНИИ FORCEPOINT

FORCEPOINT
POWERED BY Raytheon

Forcepoint Email Security

БЕЗОПАСНОСТЬ ЛОКАЛЬНОЙ И ОБЛАЧНОЙ ЭЛЕКТРОННОЙ ПОЧТЫ ОТ КОМПАНИИ FORCEPOINT.

Большинство широкомасштабных кибератак начинаются через электронную почту, используя изощренные и скоординированные тактики, такие как социально привлекательные приманки и целенаправленный фишинг. Поскольку такие многоэтапные угрозы соединяют в себе элементы Интернет и электронной почты, существует «убийственная цепочка» возможностей остановить их до того, как будет пробита брешь в защите.

Максимальное использование и безопасность электронной почты.

ПО Forcepoint Email Security определяет целевые атаки, пользователей с высоким уровнем риска и внутренние угрозы, а также расширяет возможности мобильных работников и безопасное внедрение новых технологий, таких как Office 365 и Box Enterprise.

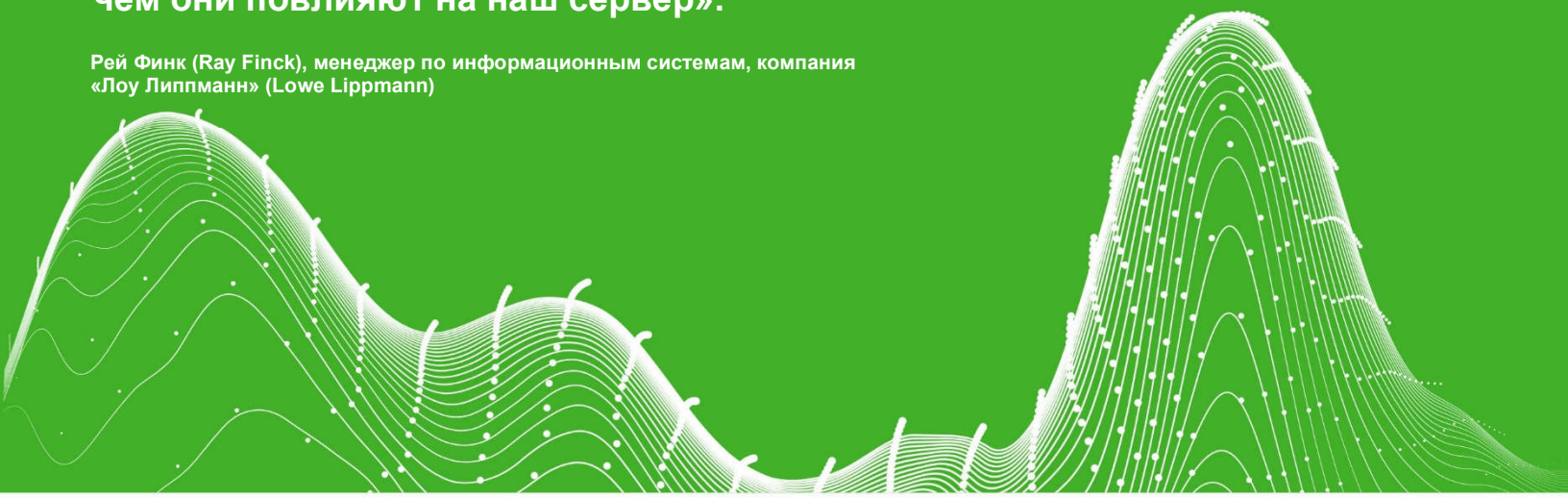
Начиная с попытки входящей атаки и заканчивая попыткой кражи исходящих данных или попыток отправки сообщений ботнетом, ПО Forcepoint Email Security защищает смешанные среды, используя учитывающую контент защиту, защищая сообщения электронной почты как часть полнофункциональной системы защиты от продвинутых устойчивых угроз (APT) и других видов продвинутых угроз.

Проблемы безопасности электронной почты.

- Продвинутые устойчивые угрозы обычно используют электронную почту на ранних стадиях своих атак.
- Система электронной почты должна предпринимать больше усилий для устранения краж данных и внутренних угроз.
- Компании все чаще используют Office 365 и другие облачные сервисы в целях расширения и конкуренции.
- Рискованные пользовательские привычки легко могут привести к нарушениям безопасности и потере данных.

«В конечном итоге, мы очень довольны продуктами компании Forcepoint. ПО Forcepoint Email Security делает свою работу и решает любые проблемы прежде, чем они повлияют на наш сервер».

Рей Финк (Ray Finck), менеджер по информационным системам, компания «Лоу Липпманн» (Lowe Lippmann)



Функциональность ПО Forcepoint Email Security

ОСТАНАВЛИВАЕТ ПРОДВИНУТЫЕ УСТОЙЧИВЫЕ УГРОЗЫ И ИНЫЕ ПРОДВИНУТЫЕ ЦЕЛЕВЫЕ УГРОЗЫ

Система классификации Advanced Classification Engine (ACE) компании Forcepoint лежит в основе всех решений компании Forcepoint. Система ACE выявляет вредоносные приманки, пакеты эксплоитов, новые угрозы, сообщения ботнетов и другие действия продвинутых угроз в «убийственной цепочке». Это позволяет ПО Forcepoint Email Security определять ранние этапы атаки. Он может даже идентифицировать вредоносные угрозы нулевого дня, используя мощные оценочные возможности, которые включают полностью интегрированную файловую поведенческую песочницу.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ОТ ВНЕШНИХ АТАК И ВНУТРЕННИХ УГРОЗ

Чтобы подготовиться к вредоносной внутренней угрозе или потенциально успешной кибератаке, очень важно контролировать исходящие сообщения. Это также необходимо как для требований к краже данных, так и для бизнес-требований. Только компания Forcepoint предоставляет технологию для прекращения проникания и кражи исходящих данных с помощью таких возможностей, как:

- Сканирование с использованием технологии OCR (оптическое распознавание символов) для определения конфиденциальных данных, скрытых в файлах изображений, таких как отсканированные документы или копии экрана.
- Обнаружение зашифрованных файлов для распознавания пользовательских зашифрованных файлов, предназначенных для нарушения процедуры идентификации.
- Мониторинг предотвращения утечки данных (DLP) для определения небольших утечек конфиденциальных данных с течением времени.
- Расширенный анализ вредоносных файлов и макросов, обычно встраиваемых в файлы MS Office.

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ, ПОДОБНЫХ OFFICE 365 И BOX ENTERPRISE С ОДНОВРЕМЕННОЙ ПОДДЕРЖКОЙ МОБИЛЬНОЙ РАБОЧЕЙ СИЛЫ

ИТ-отделы изо всех сил поддерживают действующие системы, в то же время поддерживая также все увеличивающиеся количество мобильных сотрудников, а также требования к внедрению новых технологий, таких как Office 365. ПО Forcepoint Email Security предоставляет лидирующие в отрасли возможности и использует систему и другую информацию для управления обменом сообщениями, например, для предотвращения всеобщего доступа к конфиденциальным вложениям электронной почты на уязвимых мобильных устройствах и при этом обеспечивая полный доступ на полностью защищенных портативных компьютерах. Такая защита входящих и исходящих сообщений поддерживается в Office 365.

ОПРЕДЕЛЕНИЕ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ ВЫСОКОГО РИСКА И ОБУЧЕНИЕ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ УСИЛЕНИЯ ИХ ОСВЕДОМЛЕННОСТИ

Богатые коллекции данных ПО Forcepoint Email Security компании используются рядом политик для сообщения о системах, требующих особого внимание ИТ специалистов, а также идентификации таких систем. Они создают отчет о показателях компромисса для обнаружения зараженных систем и проактивные отчеты о подозрительном поведении, в том числе о потенциальных внутренних угрозах, например, о деятельности «недовольных сотрудников». Возможности обратной связи с пользователями обучают сотрудников по мере возникновения ошибок, помогая им лучше учиться и понимать передовые методы безопасного обмена электронными письмами.

Модули расширенной защиты.

ДОПОЛНИТЕЛЬНОЕ РАЗВЕРТЫВАНИЕ В ГИБРИДНОМ ОБЛАКЕ	**Использование глобальных облачных служб компании Forcepoint для повышения производительности и способности к масштабированию.** Объединение локальной защиты от угроз с облачными, предварительно фильтрующими службами для сохранения пропускной способности с помощью ведущих отраслевых антиспамовых соглашений об уровне услуг (SLA). Гибридный модуль добавляет функциональность песочницы URL и обучения фишингу в решение Email Security.
СИСТЕМА ЗАЩИТЫ ОТ УТЕЧЕК ДАННЫХ (DLP) В ЭЛЕКТРОНОЙ ПОЧТЕ	**Блокирование краж данных посредством DLP корпоративного класса на основе контента.** Подготовка к внутренней угрозе и краже данных вредоносными программами, достижение целей соответствия и дальнейшее смягчение рисков для персональной информации или IP-адреса. Передовая функциональность обнаруживает кражу данных, скрытых в файлах изображений или пользовательских зашифрованных файлах, даже если они передаются малыми объемами в течение длительного периода времени с целью не быть обнаруженными.
ОБЛАЧНАЯ ПЕСОЧНИЦА	**Интегрирование поведенческой песочницы для автоматического и ручного анализа вредоносных файлов.** Дополняет аналитику системы ACE компании Forcepoint интегрированной файловой песочницей с целью дополнительного глубокого исследования. Использует преимущества поведенческого анализа в виртуальной среде для выявления вредоносного поведения нулевого дня и других продвинутых вредоносных программ. Автоматическое или ручное тестирование файлов для получения подробных криминалистических данных.
ШИФРОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ	**Обеспечение конфиденциальности закрытых сообщений.** Модуль Forcepoint Email Encryption является технологией, управляемой политиками, которая обеспечивает безопасную доставку сообщений электронной почты. Он устраняет традиционные ценовые барьеры и сложности, предлагая удобное администрирование без сложного управления ключами или дополнительного аппаратного обеспечения.
АНАЛИЗ ИЗОБРАЖЕНИЙ	**Определение откровенных изображений для обеспечения приемлемого использования и соответствия.** Модуль Forcepoint Image Analysis позволяет работодателям принимать проактивные меры по мониторингу, обучению и обеспечению соблюдения стратегии электронной почты компании в отношении откровенных или порнографических изображений в виде вложений.

« ПО Forcepoint Email Security привлекло тем, что избавило нас от издержек управления безопасностью электронной почты и дало нам даже больше чем мы ожидали с точки зрения работоспособности и простоты использования. В целом, ПО Forcepoint Email Security дало нам возможность предоставить нашим пользователям более отказоустойчивый, профессиональный и рентабельный сервис ».

— Мартин Лоу (Martin Law), руководитель отдела информационных технологий, компания NCP

Возможности решений компании Forcepoint.

СИСТЕМА КЛАССИФИКАЦИИ ACE

Система ACE компании Forcepoint обеспечивает облачную встроенную, контекстуальную защиту в реальном времени для Интернет, электронной почты, данных и мобильных устройств, используя комбинированную систему оценки рисков и аналитику для обеспечения максимально эффективной защиты. Система также предоставляет сдерживание угроз путем анализа входящего и исходящего трафика, обеспечивая лидирующую в отрасли степень защиты данных от краж. Классификаторы для обеспечения безопасности в реальном времени, анализа данных и контента, которые были получены после многолетних исследований и разработок, позволяют системе ACE обнаруживать больше угроз, чем традиционные антивирусные системы (доказательство обновляется ежедневно по ссылке http://securitylabs.forcepoint.com). Система ACE является основной защитой всех решений компании Forcepoint и поддерживается системой Forcepoint ThreatSeeker Intelligence.

ИНТЕГРИРОВАННЫЙ НАБОР ОЦЕНКИ ВОЗМОЖНОСТЕЙ ЗАЩИТЫ В ВОСЬМИ КЛЮЧЕВЫХ ОБЛАСТЯХ

- Доступны 10 000 аналитических функций для выполнения глубокого анализа
- Предиктивная система безопасности предвидит несколько будущих событий,
- Встроенные средства защиты не только отслеживают, но и блокируют угрозы.

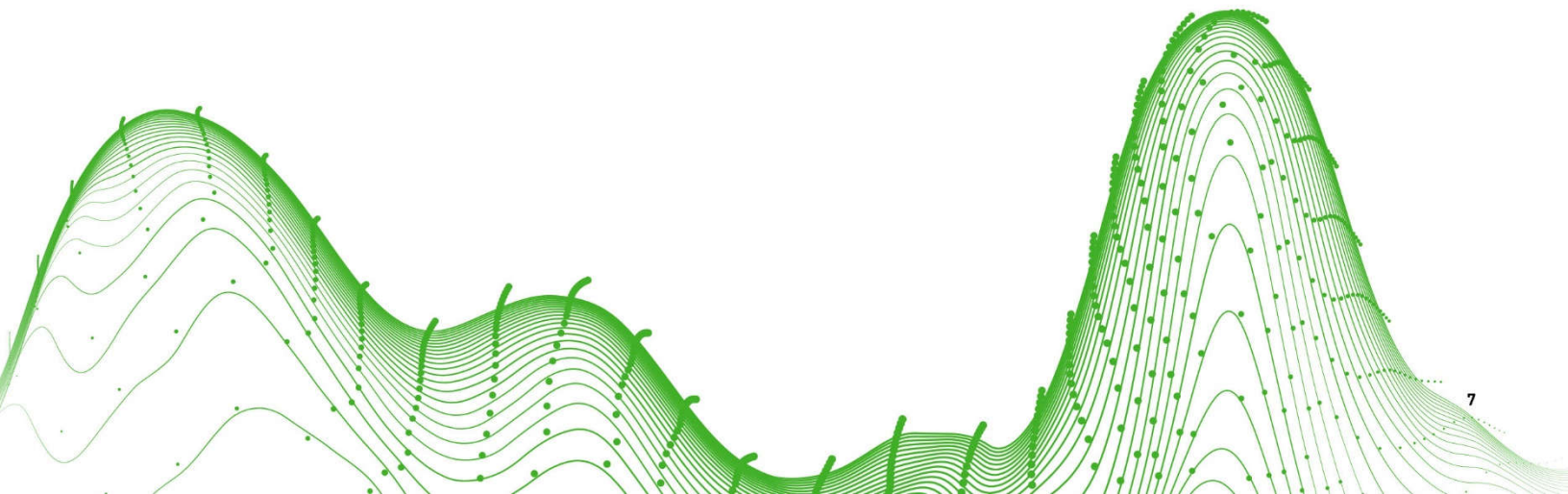
ПО Forcepoint ThreatSeeker Intelligence

ПО Forcepoint ThreatSeeker Intelligence, разработанное лабораторией Security Labs компании Forcepoint, предоставляет базовые общие аналитические возможности для всех продуктов безопасности компании Forcepoint. Оно объединяет более 900 миллионов конечных устройств, включая входные данные от Facebook, а с помощью системы ACE компании Forcepoint анализирует до 5 миллиардов запросов в день.

Такая широкая осведомленность об угрозах безопасности позволяет Forcepoint ThreatSeeker Intelligence предлагает обновления безопасности в реальном времени, которые блокируют изощренные угрозы, вредоносные программы, фишинг-атаки, приманки и мошенничества. Кроме того, ПО также предоставляет последние веб-рейтинги. Forcepoint Intelligence ThreatSeeker не имеет себе равных по размеру и использованию системы ACE в режиме реального времени для анализа общих входных данных. (При обновлении до уровня Web Security, ПО Forcepoint ThreatSeeker Intelligence помогает снизить подверженность веб-угрозам и краже данных).

Архитектура TRITON

Обладая лучшей в своем классе безопасностью и унифицированной архитектурой, архитектура TRITON предлагает мгновенную защиту на основе встроенной защиты в реальном времени, обеспечиваемой системой Forcepoint ACE. Непревзойденная защита, обеспечиваемая в реальном времени системой ACE, поддерживается ПО Forcepoint ThreatSeeker Intelligence и опытом исследователей лаборатории Security Labs компании Forcepoint. В результате получена единая архитектура с одним унифицированным интерфейсом пользователя и единой системой сбора информации для обеспечения защиты.



КОНТАКТНАЯ ИНФОРМАЦИЯ
www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_EMAIL_SECURITY_EN]

FORCEPOINT
POWERED BY Raytheon