Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT CloudGuard SaaS

CLOUDGUARD SAAS: ЗАЩИТА ОБЛАЧНОЙ ПОЧТЫ ОТ КИБЕРУГРОЗ

в 95% атак
нна облачные сервисы
слабым звеном был
пользователь (Gartner)

до 30% угроз
может пропускать
встроенная защита
облачных сервисов
(Check Point, 2020)

в 3 раза
раза вырос ущерб
от атак на облачные
сервисы (IC3)

90% атак
атак на организации
начинаются с почты
(Verizon, 2018)

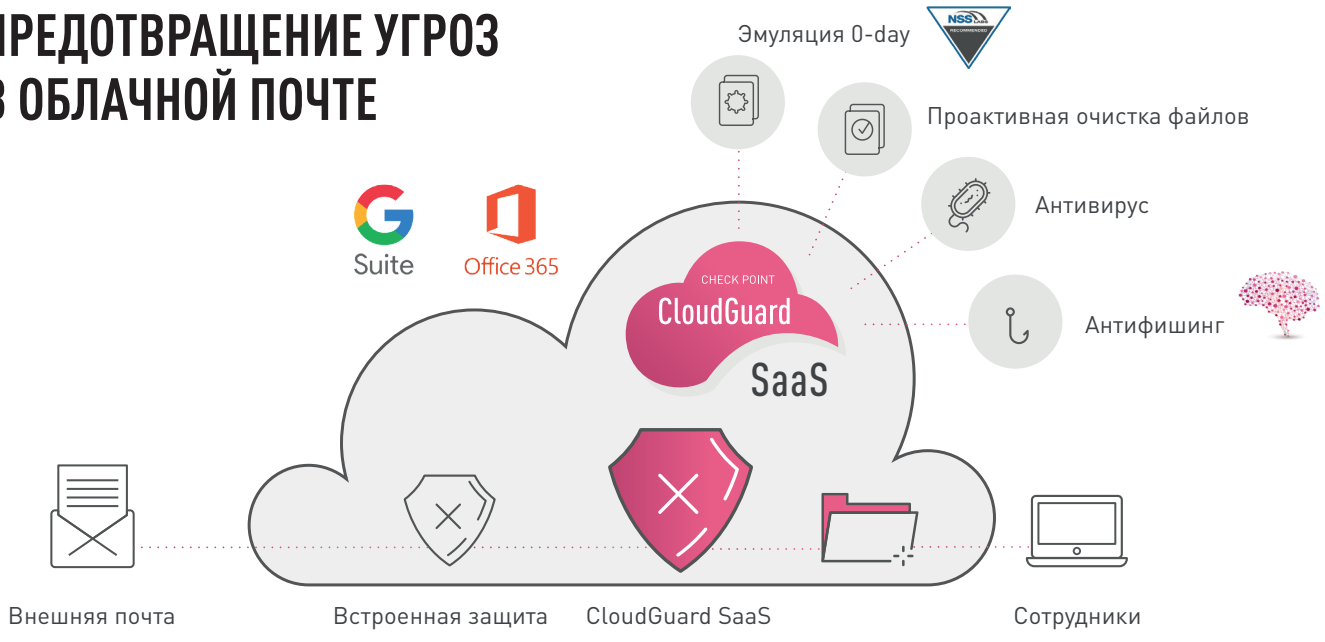
ВСТРОЕННАЯ ЗАЩИТА НЕ СПОСОБНА НАДЕЖНО ПРЕДОТВРАЩАТЬ СОВРЕМЕННЫЕ УГРОЗЫ

Облачные сервисы стремительно входят в нашу жизнь. Почта, развернутая в облаке, удобна тем, что к ней есть доступ отовсюду и с любого устройства; она легко развертывается и быстро масштабируется. Однако, безопасность отстает от удобства, и злоумышленники этим активно пользуются. Вредоносные файлы, в том числе 0-day, социальная инженерия и фишинг — облачные сервисы подвержены тем же угрозам, что и развернутые внутри периметра. Кроме того, добавились и новые: так, кража учетных записей становится важнейшим вектором атаки и приводит к огромному ущербу.

Провайдер отвечает за сохранность данных, за их изолированность, за доступность сервиса, но не за сами данные и их безопасность. Встроенная защита (когда она есть) не способна отразить угрозы на надежном уровне, качество детектирования не подтверждено независимыми тестами. Наши исследования показывают, что до 30% всех вредоносов встроенной защитой пропускаются. Защита от фишинга также ограничена проверкой ссылок, и поэтому бессильна против фишинговых писем, не содержащих ссылок.

Ущерб же от подобных атак может быть колоссальным: прямые потери от нелигитимных транзакций, кража и блокирование данных, потери в результате шантажа, манипулирование акциями, ущерб репутации, штрафы и санкции со стороны регуляторов.

ПРЕДОТВРАЩЕНИЕ УГРОЗ В ОБЛАЧНОЙ ПОЧТЕ



CLOUDGUARD SAAS — ПРОДВИНУТЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ

Надежно предотвращать угрозы, особенно нулевого дня — сложная задача. Для этой цели мы используем проверенные на уровне периметра технологии SandBlast, которые на рынке уже много лет. Они были неоднократно протестированы в независимых сравнениях и доказали свою эффективность.

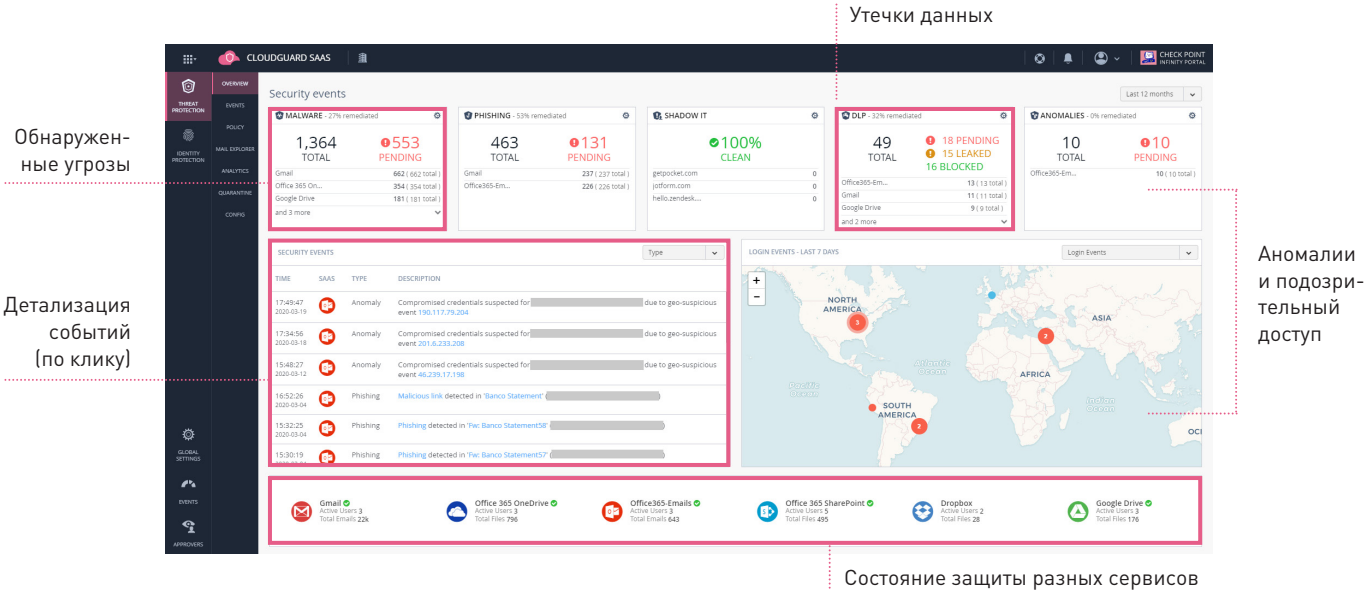
Threat Emulation — позволяет с высокой точностью блокировать вредоносные файлы (100% в тесте NSS Labs 2017 года).

Threat Extraction. Файлы, требующие проверки, будут мгновенно сконвертированы в безопасную форму и доставлены пользователю, что позволяет избежать задержек в работе почты.

Anti-Phishing. Блокировать фишинг очень важно, и для этого мы используем машинное обучение и более 300 различных параметров письма, кроме URL.

В отличие от других решений CloudGuard SaaS для интеграции использует API (а не MTA), что позволяет защититься от распространения угроз внутри организации.

ВИЗУАЛИЗАЦИЯ СОБЫТИЙ И КОНТРОЛЬ БЕЗОПАСНОСТИ



СРАВНЕНИЕ ВОЗМОЖНОСТЕЙ

	CloudGuard SaaS	Встроенная защита
Блокирование с помощью Антивируса	✓	✓
Предотвращение угроз нулевого дня (Threat Emulation)	Да, t = 2min	Частично, t > 10min
Подтвержденный уровень блокирования угроз	✓ 0% пропущенных уг роз в тесте NSS Labs BPS	✗ до 30% пропущенных угроз в тестах Check Point
Проактивная очистка документов (Threat Extraction)	✓	Частично
Защита от несанкционированного доступа Identity Protection	✓	Без проверки конечных устройств
Гибкие политики и детальный анализ обнаруженных угроз	✓	✗
Обнаружение аномалий (Shadow IT, Anomalies Detection)	✓	Отдельная лицензия
Поддержка других сервисов в рамках одной лицензии	O365, GSuite, Box, Dropbox, Salesforce, Slack	O365 или GSuite

АУДИТ БЕЗОПАСНОСТИ ЗА 30 МИНУТ

Начните с регистрации на portal.checkpoint.com. Начальная настройка займет примерно 30 минут. По умолчанию защита начнется в режиме мониторинга. Проверке подвергнутся все входящие сообщения и те, что доставлены за последние 5 дней.

КОНТАКТЫ Check Point Software Technologies
Россия и СНГ
russia@checkpoint.com