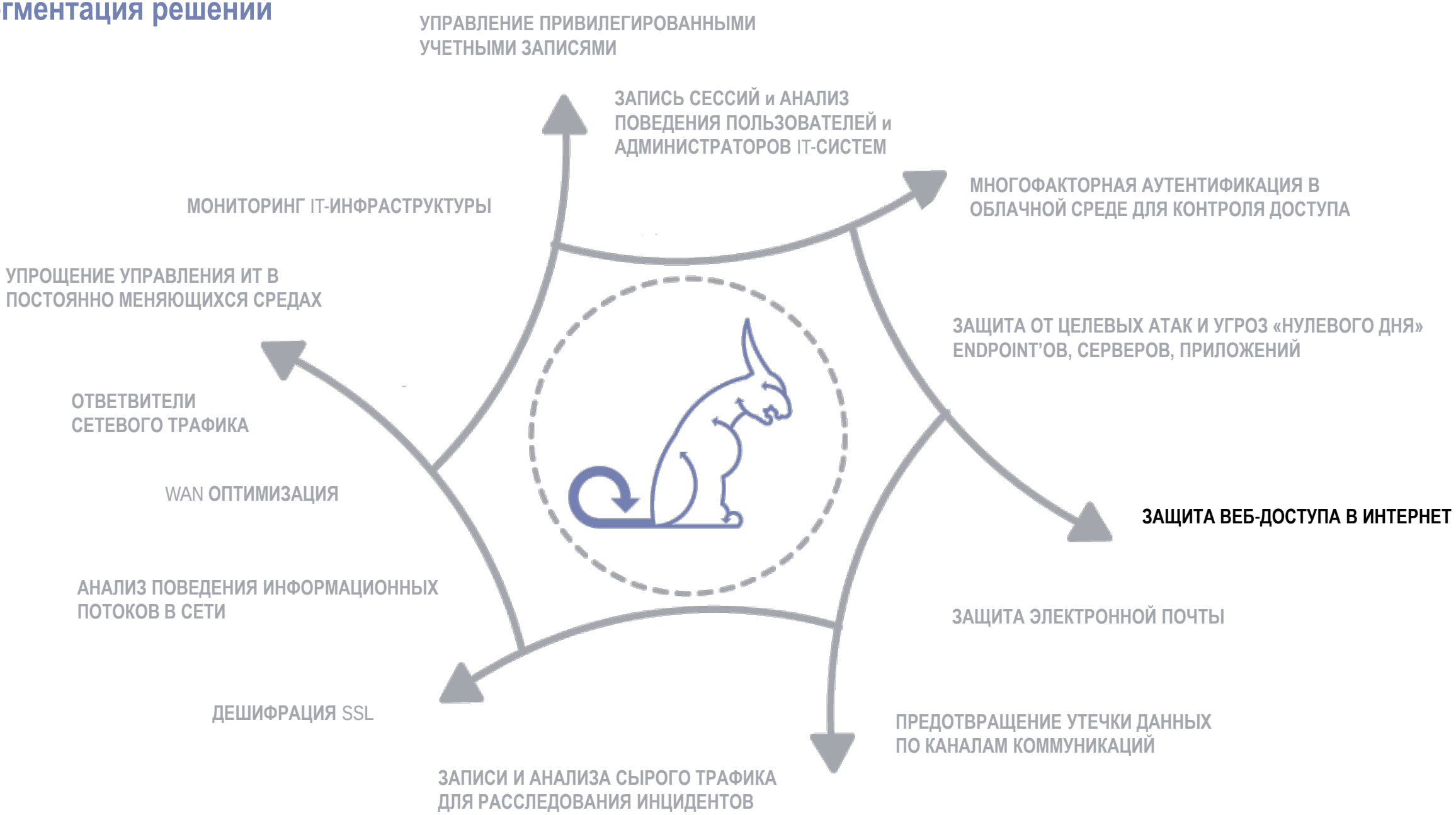
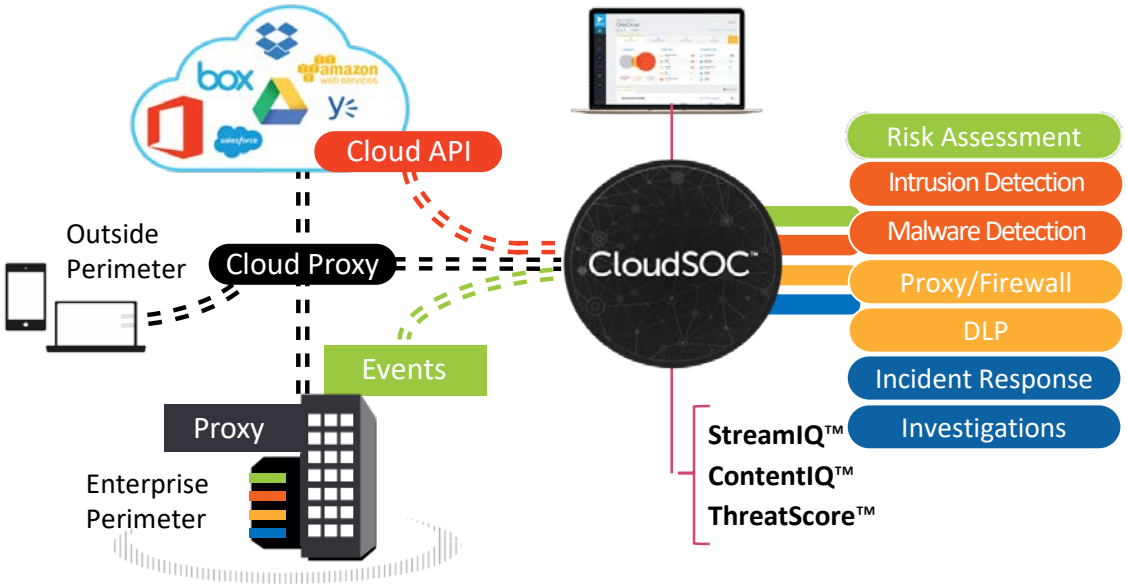
Сегментация решений



Решение от Symantec – Cloud Access Security Broker

КОНТРОЛЬ ПЕРЕДАВАЕМЫХ ДАННЫХ В ОБЛАЧНЫЕ ПРИЛОЖЕНИЯ И СЕРВИСЫ

https://www.symantec.com/products/web-and-cloud-security/cloud-application-security-cloudsoc



- Выявление и контроль конфиденциальной информации в облачных сервисах;
- Применение политик DLP к данным, обезличивание документов;
- Обеспечение безопасности в облачных аккаунтах с помощью *«Оценки угроз поведения»;*
- Проведение исследования в рамках реагирования на инциденты.

1. Шлюз CASB в режиме аудита анализирует журналы доступа пользователей к ресурсам Интернет и обнаруживает облачные приложения и сервисы, которые использовались.
2. Если дальнейшей интеграции CASB с облачным сервисом не предполагается (для детального контроля), то такие облачные сервисы в дальнейшем можно будет мониторить или блокировать (на прокси или файерволле).
3. Если облачный сервис официально используется в компании и требуется детально контролировать взаимодействие пользователей с ним, то **с помощью CASB шлюза** или **соответствующего API-based Securlet** на шлюзе CASB настраивается политика. Трафик пользователей при этом должен проходить через шлюз CASB.
4. CASB развертывается как облачный сервис или ПАК (в части модуля обезличивания данных) в корпоративной сети.
5. CASB интегрируется с файерволлами, прокси, UBA/UEBA и DLP решениями.

CloudSOC Audit – Shadow IT

Выявление Shadow IT - поиск и аудит использования облачных сервисов. Оценка безопасности облачных сервисов. Подробнее https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloudsoc-audit-en.pdf

CloudSOC Security for Cloud Apps – Securlets

Решение включает в себя **Securlets на основе облачных API** для «понимания» действий с данными в **разрешенных** облачных сервисах и **облачный CASB шлюз** для управления взаимодействием с облачными сервисами. Securlets для выбранных организацией облачных сервисов дают возможность узнать, какие данные опубликованы, кем именно и применить политики доступа к документам, расположенным в облаке.
Решение может быть полностью интегрировано с Symantec DLP.
Подробнее https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloudsoc-security-for-saas-en.pdf

CloudSOC CASB Gateway

- Контроль в реальном времени транзакций с санкционированными (разрешенными) и несанкционированными облачными приложениями;
- Управление данными с помощью политик, возможна полная интеграция с Symantec DLP;
- Визуализированная карта активности пользователя для быстрого анализа;
- Защита от угроз, основанная на обширной аналитике поведения пользователей;
- Интеграция с SIEM для реагирования на инциденты и Symantec VIP для надежной аутентификации.

С помощью технологии StreamIQ извлекаются события из трафика облачных приложений в реальном времени. Уникальная технология, основанная на наукоёмких технологиях, обеспечивает глубокую видимость транзакций с широким спектром облачных приложений.
CloudSOC User Behavior Analytics (UBA) использует интеллектуальные средства StreamIQ и машинное обучение для автоматического поддержания индивидуальных профилей пользователей, отображения активности пользователей и компиляции показателя угрозы от пользователя в реальном времени.
Подробнее https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloudsoc-gateway-en.pdf

Cloud Data Protection Gateway

Модуль обезличивания данных. Решение может быть полностью интегрировано с Symantec DLP.
Подробнее https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloudsoc-audit-en.pdf

ProxySG представляет собой масштабируемую прокси-платформу для обеспечения безопасности взаимодействия с ресурсами сети Интернет (web security) и оптимизации работы бизнес-приложений (WAN optimization). **Устройства NGFW не являются заменителями** прокси-решений в виду ограниченных возможностей разбора веб-трафика.

Решение от Symantec – Secure Web Gateway ProxySG

ЗАЩИТА ВЕБ-ДОСТУПА В ИНТЕРНЕТ КАК ОСНОВНОГО ТРАНСПОРТА ДОСТАВКИ ВРЕДОНОСНОГО ПО

https://www.symantec.com/products/web-and-cloud-security/secure-web-gateway-proxy-sg-and-asg

Преимущества решения ProxySG:

Общее

- Высокопроизводительная фирменная операционная система с возможностью перезагрузки на предыдущую версию.
- Возможность функционирования в качестве прозрачного (transparent) и явного (explicit) прокси одновременно. Применяется для обеспечения защиты внутренних пользователей и сетей от шпионского программного обеспечения и фишинговых атак при веб-доступе в Интернет.
- Возможность функционирования в качестве обратного (reverse) прокси. Применяется в составе организованной сети DMZ для исключения возможности прямого доступа извне к веб-серверам организации. Функционал Web Application Firewall - бесплатный.

Протоколы и аутентификация

- Возможность применения для таких протоколов передачи данных как: HTTP/HTTPS, CIFS, SSL, FTP,FTP-over-HTTP, MAPI, P2P, MMS, RTMP, RTSP, QuickTime, TCP-Tunnel, DNS, WCCP.
- Возможность разграничения прав доступа к ресурсам посредством следующих механизмов аутентификации: на основании локальных списков пользователей; IWA (Basic, NTLM, Mirosoft Kerberos), LDAP (Active Directory, eDirectory, SunOne), CA eTrust SiteMinder, Oracle Access Manager, RADIUS; применения сертификатов; поддержка SSO и прозрачной аутентификации, а также последовательной аутентификация в нескольких системах.

SSL

- Аппаратное ускорение SSL-трафика. Контроль параметров SSL-соединений – валидности сертификатов серверов, версий протоколов шифрования SSL/TLS, шифрования и контроля целостности SSL/TLS-соединения (cipher suites).
- Функционал Encrypted TAP позволяет отдать расшифрованный *-over-SSL трафик (HTTPS, IMAPS и т.д.) на анализ во внешнее устройство ИБ (например, “песочницу”) в дешифрованном виде.
- Дешифрация SSL-трафика и SSL off loading

Интеграция

- Поддержка протокола ICAP – для интеграции с DLP или другими системами безопасности.
- Интеграция с другими решениями ИБ позволяет значительно повысить уровень сетевой безопасности.

Надежность и архитектура

- Работа в режиме Active/Active bridging с поддержкой virtual IP для обеспечения функций резервирования и удаленного управления, встроенный сетевой адаптер passthrough
- Поставляется в виде физических устройств (ProxySG и Advanced Security Gateway) и виртуальных образов (virtual appliance) для ESX/ESXi, Hyper-V или Amazon Web Services

Безопасность

- Контроль действий пользователей в сети Интернет. Позволяет блокировать отдельные приложения и действия в этих приложениях (например, загрузку/выгрузку вложений в веб-почте или отправку писем или сообщений в социальных сетях).
- Возможность выполнения контентной фильтрации и категорирования Интернет-ресурсов – BlueCoat WebFilter или BlueCoat Intelligence Services.

Оптимизация

- Повышение производительности сетевой инфраструктуры, веб приложений и веб-сайтов организации по средствам функционала WAN optimization.
- Возможность кэширования данных с учетом результатов антивирусной проверки.
- Возможность управления сетевыми протоколами и полосой пропускания каналов связи.

Управление и отчетность

- Централизованное управление политиками на всех SWG в сети
- Возможность сбора статистической информации и формирования отчетов в отношении протоколов передачи данных (более 60 контролируемых параметров), а также для определения эффективности и активности рабочих мест пользователей.

Отладка и мониторинг

- Широкие возможности по трассировке и отладке используемых политик безопасности
- Контроль доступности для критичных приложений и услуг
- Поддержка SNMP и Syslog.

Решение от Symantec – Content Analysis

ОБНАРУЖЕНИЕ И БЛОКИРОВАНИЕ ПРОДВИНУТЫХ УГРОЗ, С МНОГОУРОВНЕВОЙ ПРОВЕРКОЙ И ДИНАМИЧЕСКОЙ ПЕСОЧНИЦЕЙ

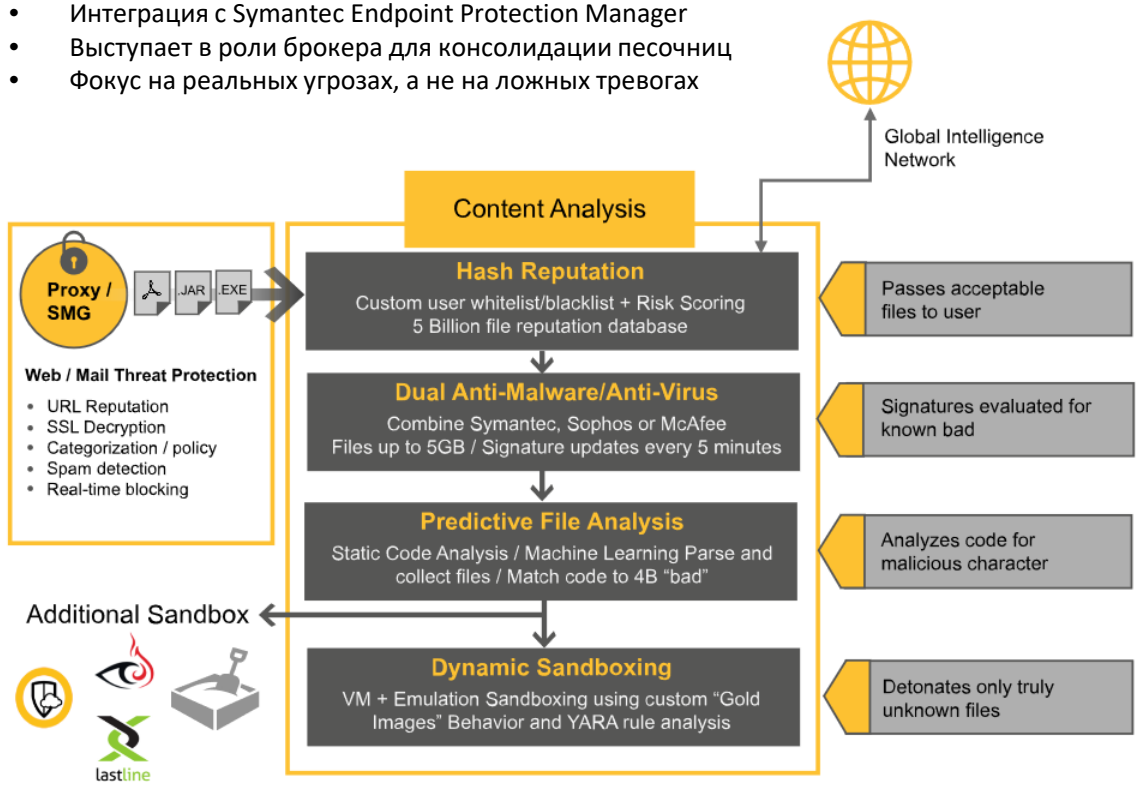
https://www.symantec.com/products/web-and-cloud-security/atp-content-malware-analysis

Используется с Symantec ProxySG. Решение выполняет многоуровневую фильтрацию контента – возможно подключение нескольких антивирусных движков и песочниц для выявления вредоносного поведения и угроз нулевого дня, с возможностью безопасной детонации подозрительных файлов и URL-адресов.

Анализ контента 2.1 включает в себя следующие функции:

1. **Malware и Antivirus сканирование** — Content Analysis поддерживает движки McAfee, Sophos и Kaspersky; все могут использоваться одновременно.
2. **Предиктивный анализ** — службы от Cylance используют передовой механизм искусственного интеллекта для выявления вредоносных программ.
3. **Служба репутации файлов** — анализ содержимого генерирует хэш SHA1 для каждого обрабатываемого файла. Этот хэш сравнивается с облачной системой репутации Symantec для идентификации известных файлов. Служба использует оценки репутации, цифры (1-10), которые указывают, являются ли файлы безопасными или зловредными.
4. **Ручной файловый «Черный» и «Белый» списки**.
5. **Интеграция с внешними песочницами** Symantec Malware Analysis, Lastline или FireEye **и/или активация модуля песочницы на борту** — проверка поведения файлов в фоновом или режиме реального времени.
6. **Интеграция с Symantec Endpoint Protection Manager (SEPM)** — когда песочница обнаруживает вредоносное ПО, Content Analysis может запросить сервер CounterTack Sentinel в вашей сети, чтобы определить, какие пользователи (если они есть) его получили. Когда песочница находит вредоносный файл, уведомляется администратор и предоставляется возможность добавить хэш файла в черный список на SEPM.
7. **Кэшированные ответы** — когда Content Analysis определяет вердикт (чистый и вредоносный) для файла, он кэширует хэши и вердикт файла, чтобы избежать сканирования одного и того же файла при последующих запросах. Анализ контента содержит отдельные кэши для ответов от каждой из своих служб: антивируса, репутации файлов, интеллектуального анализа и песочницы (угрозы и чистые).
8. **Global Intelligence Network (GIN)** — крупнейшая глобальная сеть сенсоров, собирающих данные о ландшафте угроз (от сообщества безопасности + 5млн. аккаунтов-приманок + 8млрд. сообщений/мес.)

- Блокирует все известные угрозы, идентифицированные через Global Intelligence Network
- Оптимизированный многоэтапный анализ для проверки только подозрительных файлов
- Детонирует неизвестные файлы с помощью встроенной или выделенных песочниц
- Интеграция с Symantec Endpoint Protection Manager
- Выступает в роли брокера для консолидации песочниц
- Фокус на реальных угрозах, а не на ложных тревогах



Multi-layer threat inspection, detection and sandboxing uncover the unknowns

Решение от Symantec – Malware Analysis

ОБНАРУЖЕНИЕ И БЛОКИРОВАНИЕ ПРОДВИНУТЫХ УГРОЗ, С МНОГОУРОВНЕВОЙ ПРОВЕРКОЙ И НАСТРАИВАЕМОЙ ПЕСОЧНИЦЕЙ

https://www.symantec.com/products/web-and-cloud-security/atp-content-malware-analysis

Решение Malware Analysis обнаруживает и анализирует неизвестные, передовые, и целенаправленные вредоносные программы с использованием уникального подхода двойного обнаружения. Безопасно детонирует в песочнице корпоративного класса в средах с высокой реалистичностью подозрительные файлы и URL-адреса, выявляет вредоносное поведение и угрозы нулевого дня. Объединяет динамические, статические и репутационные методы анализа для точного выявления вредоносных программ. Предоставляет подробные отчеты и информацию об угрозах. Интегрируется с Symantec Content Analysis, Symantec Mail Threat Defense и Symantec Security Analytics.

Ключевые особенности Malware Analysis

- **Высокая эффективность выявления злонамеренного поведения** за счет функционала Emulation и Virtualization Sandbox
- **Множественные методы обнаружения**, используется комбинация методов статического и динамического анализа, в которых используются стандартные, настраиваемые и открытые шаблоны YARA с открытым исходным кодом. Обнаруживаются упакованные вредоносные программы и VM-образы, которые изменяют поведение в искусственной среде, а также вредоносное ПО, которое пытается подождать анализ любой песочницы, используя короткие или длинные спячки.
- **Инструменты для противодействия анти-анализу**
- **Взаимодействие с вредоносными программами** путем кликов в диалоговых окнах и инсталляторах ПО
- **Создание более релевантных результатов** путем репликации нескольких пользовательских сред
- **Адаптивный интеллект для изменяющихся угроз** - гибкие шаблоны предназначены для обнаружения полиморфных файлов, одноразовых целевых вредоносных программ и быстро изменяющихся доменов веб-сайта
- **Подробная информация об инциденте** для быстрого реагирования – предоставляется полная карта ущерба, включая хостовые и сетевые индикаторы компрометации
- **Защита от 0-day угроз** средствами крупнейшей глобальной сети сенсоров Global Intelligence Network, собирающих данные о ландшафте угроз (от сообщества безопасности + 5млн. аккаунтов-приманок + 8млрд. сообщений/мес.)

Возможности Malware Analysis

- Emulated и Virtual среда анализа песочницы для реализации подхода двойного обнаружения.
- Настраиваемые профили Windows 8/7/XP для соответствия производственным системам.
- Виртуализированная песочница Android обнаруживает мобильные угрозы.
- Обнаружение на основе шаблонов вредоносных файлов и URL-адресов, включая полиморфные, уникальные и целевые угрозы.
- Поддержка любого формата файла ПК.
- Переходы по диалоговым окнам и установщикам для выявления интерактивных вредоносных программ, требующих взаимодействия с пользователем.
- Блокирует вредоносное VM-ПО, обходит вызовы сна и обнаруживает основные эксплойты, такие как «heap sprays».
- Настраиваемые шаблоны, параметры анализа и оценки рисков.
- Автоматические обновления шаблонов для постоянной защиты от быстроразвивающихся угроз.
- Поддержка централизованного управления устройствами для развертывания на предприятии
- Формирует детализированные вердикты и информацию для анализа инцидентов.
- Интегрируется с Symantec Content Analysis, Symantec Mail Threat Defense и Symantec Security Analytics.

Emulation Sandbox
Реплицированная компьютерная среда для ПК, эмулирует системы Windows для обнаружения вредоносных программ, которые иначе не будут взорваться в виртуализованной среде.

Virtualization Sandbox
Пользовательские профили анализа реплицируют фактические производственные среды Windows, вплоть до приложений и версий, используемых для быстрого обнаружения аномалий и поведенческих различий, которые раскрывают методы анализа, сна и других усовершенствованных методов уклонения. Виртуализированная Android-песочница обнаруживает и анализирует мобильные угрозы, проходящие через корпоративные сети.

Решение от Symantec – Advanced Secure Gateway

ПРОКСИ И КОНТЕНТНАЯ ФИЛЬТРАЦИЯ В ОДНОМ УСТРОЙСТВЕ

https://www.symantec.com/products/web-and-cloud-security/secure-web-gateway-proxy-sg-and-asg

К Secure Web Gateway относятся и ProxySG, и Advanced Secure Gateway

Прокси для endpoint

- Перехват и дешифрация трафика
- Эмуляция всех типов устройств
- Извлечение содержимого для проверки
- Интеграция аутентификации

Управление Веб и облачными сервисами

- Обнаружение и контроль Shadow IT
- Блокировка веб-угроз
- Применение политик доступа
- Аудит использования веб и облачных ресурсов

Повышенная производительность

- Оптимизация видеотрафика
- Интеллектуальное кэширование контента
- Оптимизация по протоколам

Предотвращение угроз и управление контентом

- Фильтрация перед песочницей и расширенная проверка контента
- Пересылка контента в DLP, песочницу и прочие системы ИБ
- Открытая интеграционная архитектура для быстрого добавления новых сервисов

Advanced Secure Gateway (ASG) в себе сочетает возможности ProxySG (SGOS 6.6) + Content Analysis (CAS 1.3)

Ограничения: песочницы on-box и интеграции с SEP'ом в ASG нет!

Единое управление доступом

Аутентификация, применение политик, журналирование
Обнаружение и контроль теневого (shadow) IT

Извлечение и управление файлами

Дешифрация SSL, извлечение документов
Передача файлов на проверку по ICAP
Запрет доставки на основе вердикта
Потоковые дешифрованные данные для расследования инцидентов

Проверка файлов для предотвращения вредоносных программ и продвинутых угроз

Белый / Черный список
Двойные AV сигнатуры
Анализ статического кода
Фильтрация перед песочницей

Поддерживается интеграция с песочницами Symantec Malware Analysis, Lastline или FireEye AX.
Примечание: интеграция с FireEye NX не поддерживается

Решение от Symantec – SSL Visibility

ПЕРЕДАЧА РАСШИФРОВАННОГО SSL НА АНАЛИЗ СИСТЕМАМ ИБ

https://www.symantec.com/products/information-protection/encrypted-traffic-management/ssl-visibility-appliance

Просто развертывается. Высокая производительность. Универсальность решения.

- Обеспечивается видимость всего трафика SSL/TLS для всех портов и приложений
- Нет сложных сценариев и конфигураций
- Одновременное использование активных и пассивных устройств

Высокое качество шифрации и дешифрации

- Всесторонняя, лидирующая в отрасли поддержка наборов шифров (RSA, DHE, ECDHE, ChaCha, Camilla и т.д.)
- Поддерживаются версии TLS 1.1 - 1.3 и механизмы handshake
- Не снижается уровень безопасности для пользовательских сеансов

Повышение рентабельности всей инфраструктуры безопасности

- Снижение затрат на обновление аппаратного обеспечения от 3 до 5 раз, часто требуемых решениями безопасности для проверки SSL
- Получение требуемой видимости в зашифрованном трафике, что критически важно для разбора инцидентов ИБ
- Расширение возможностей имеющихся инструментов за счет подачи расшифрованного SSL/TLS трафика

Конфиденциальность и избирательная дешифрация

- Широкий спектр применения политики
- Централизованное управление политикой

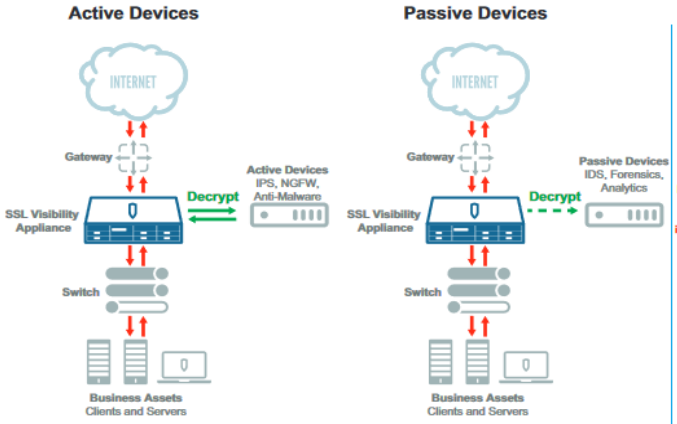


Figure 1: SSL visibility appliances decrypt SSL traffic and feed multiple active and passive devices

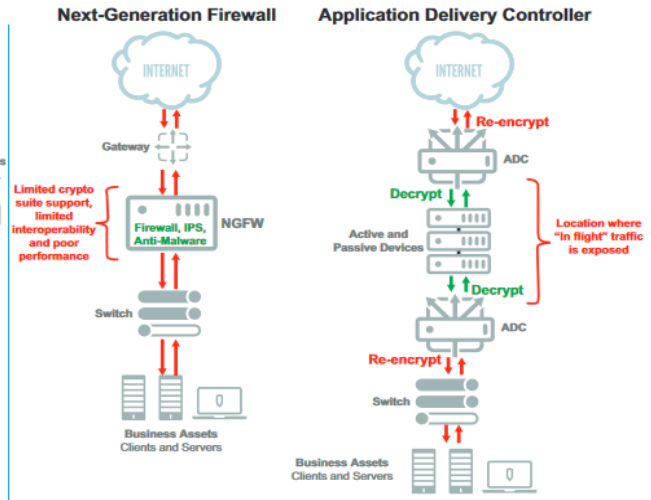


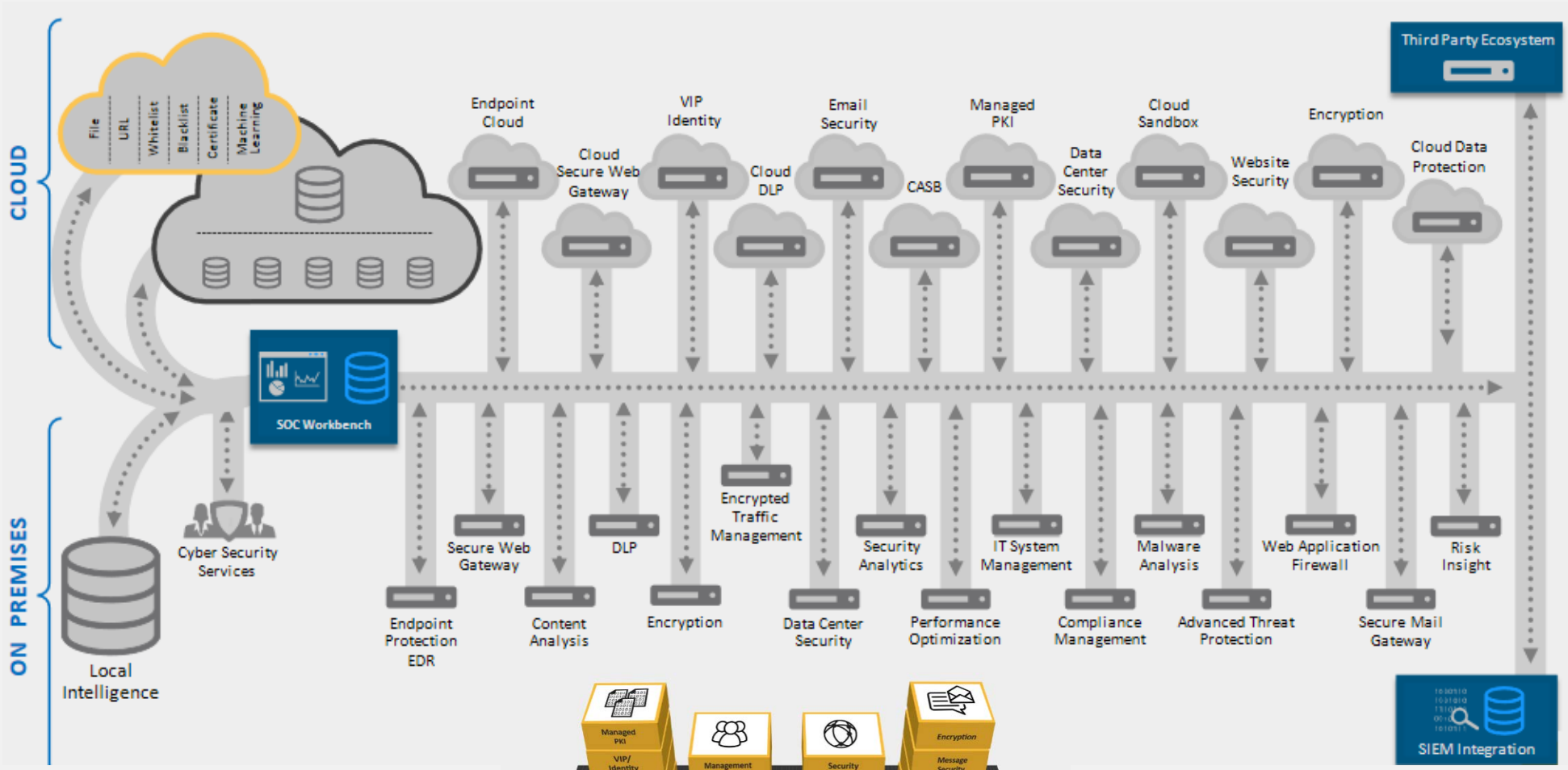
Figure 2: NGFWs and ADCs can decrypt SSL traffic, but NGFWs can't share data with other active devices, and decrypted traffic between ADCs is exposed and vulnerable to modification.

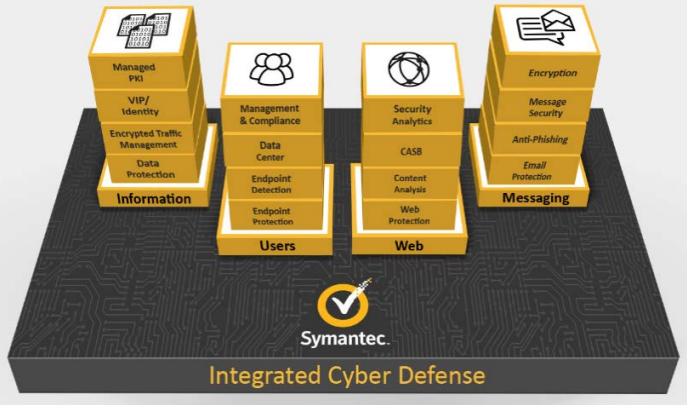
Лицензирование ex Blue Coat.

Наименование	Краткое описание	Самая свежая информация о решении	Принцип лицензирования
Решение от Symantec – Cloud Access Security Broker	Контроль передаваемых данных в облачные приложения и сервисы	https://www.symantec.com/products/web-and-cloud-security/cloud-application-security-cloudsoc	По модулям, модули наполняются по пользователям: • Elastica CASB Audit - App Visibility, Analytics and Control, Add Users • Elastica CASB Gateway - All Gatelets with Detect, Investigate and Protect, Add Users • Pack - Cloud App API, Detect, Investigate and Protect - Advanced Edition • Add Users, Blue Coat Cloud Data Protection Communication Server • Blue Coat Cloud Data Protection Communication Server, Subscription • Symantec Cloud Data Protection for AppService • Blue Coat Cloud Data Protection Server Subscription, Development Environment per App
Решение от Symantec – Secure Web Gateway	Защита веб-доступа в интернет как основного транспорта доставки вредоносного по	https://www.symantec.com/products/web-and-cloud-security/secure-web-gateway-proxy-sg-and-asg	Стоимость решения формируется из следующих составляющих: модель апплайса, кол-во пользователей, модули безопасности, модули управления и отчетности, подписка на модули и доп.оборудование
Решение от Symantec – Content Analysis	Обнаружение и блокирование продвинутых угроз, с многоуровневой проверкой и динамической песочницей	https://www.symantec.com/products/web-and-cloud-security/atp-content-malware-analysis	Стоимость решения формируется из следующих составляющих: модель апплайса, кол-во пользователей, модули безопасности, модули управления и отчетности, подписка на модули и доп.оборудование **Антивирусные движки** по числу пользователей доступны Kaspersky, McAfee, Panda, Sophos; пары Kaspersky+McAfee, Kaspersky+Sophos, Sophos+McAfee
Решение от Symantec – Malware Analysis	Обнаружение и блокирование продвинутых угроз, с многоуровневой проверкой и настраиваемой песочницей	https://www.symantec.com/products/web-and-cloud-security/atp-content-malware-analysis	Стоимость решения формируется из следующих составляющих: модель апплайса, Software Upgrade

Лицензирование ex Blue Coat.

Наименование	Краткое описание	Принцип лицензирования
Решение от Symantec – Advanced Secure Gateway	Прокси и контентная фильтрация в одном устройстве https://www.symantec.com/products/web-and-cloud-security/secure-web-gateway-proxy-sg-and-asg	**Апплайнсы** S200-30 для 1000/2500 пользователей, S200-40 для 1000/2500 пользователей, Cold Standby for ASG-S200-30 and ASG-S200-40 S400-20 для 1000/2500/5000 пользователей, S400-30 для 5000/10000/15000 пользователей, S400-40 для 10000/15000/25000 пользователей Cold Standby for ASG S400-20, S400-30, S400-40 S500-10 для 10000/15000/25000 пользователей S500-20 для 25000/35000/50000 пользователей Cold Standby for ASG S500-10, S500-20 **Лицензии** Upgrade from Cold Standby to Production Encrypted Tap License Flash Proxy License Подписки на модули
Решение от Symantec – SSL Visibility	Управление и дешифрация SSL трафика	https://www.symantec.com/products/information-protection/encrypted-traffic-management


CLOUD
ON PREMISES
File
URL
Whitelist
Blacklist
Certificate
Machine Learning
Local Intelligence
Cyber Security Services
SOC Workbench
Third Party Ecosystem
Endpoint Cloud
Cloud Secure Web Gateway
VIP Identity
Cloud DLP
Email Security
CASB
Managed PKI
Data Center Security
Cloud Sandbox
Website Security
Encryption
Cloud Data Protection
Endpoint Protection EDR
Secure Web Gateway
Content Analysis
DLP
Encryption
Encrypted Traffic Management
Data Center Security
Security Analytics
Performance Optimization
IT System Management
Compliance Management
Malware Analysis
Advanced Threat Protection
Web Application Firewall
Secure Mail Gateway
Risk Insight
SIEM Integration


Managed PKI
VIP/ Identity
Encrypted Traffic Management
Data Protection
Information
Management & Compliance
Data Center
Endpoint Detection
Endpoint Protection
Users
Security Analytics
CASB
Content Analysis
Web Protection
Web
Encryption
Message Security
Anti-Phishing
Email Protection
Messaging
Symantec.
Integrated Cyber Defense