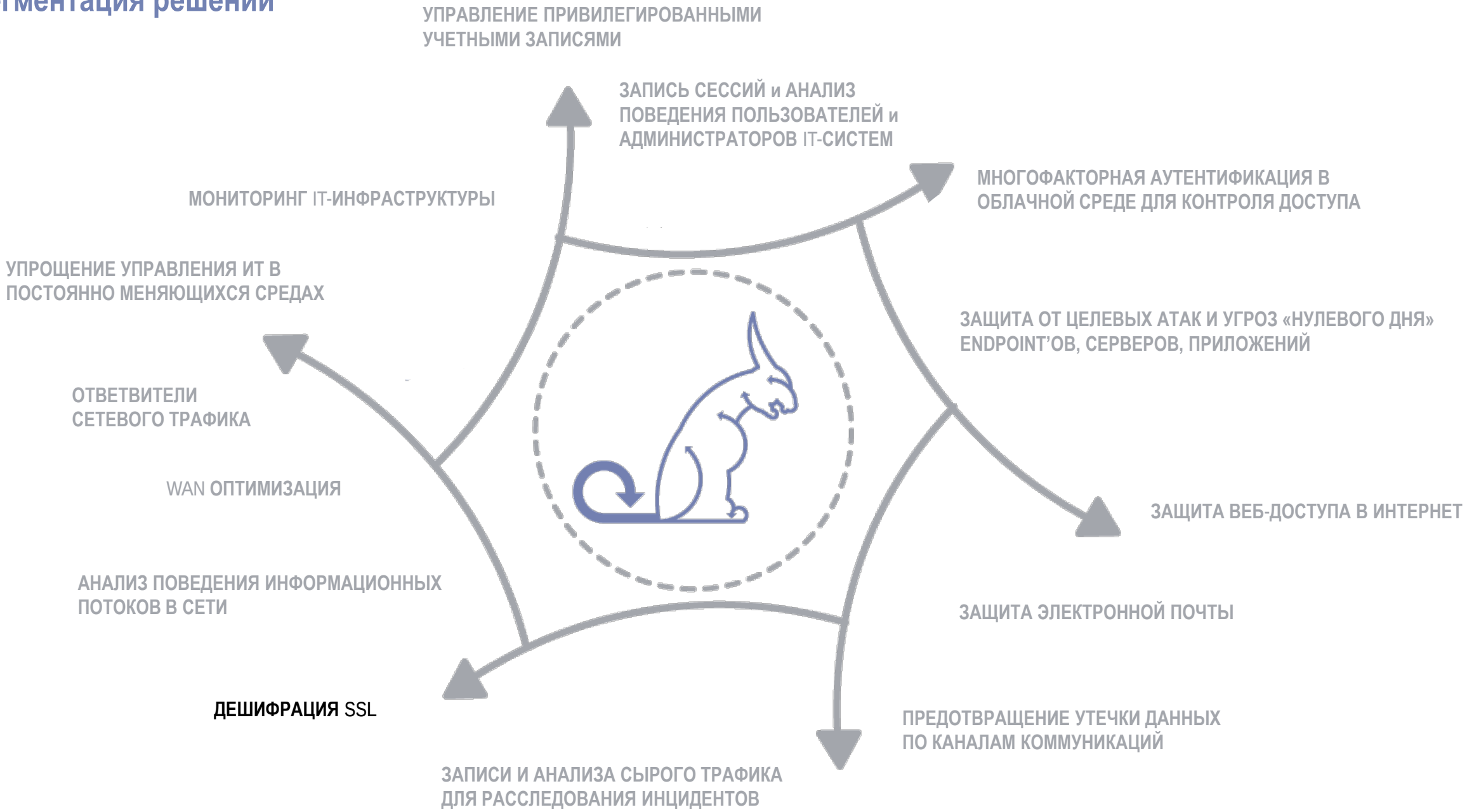
Сегментация решений



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

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

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

Конфиденциальность и избирательная дешифрация

- Широкий спектр применения политики
- Централизованное управление политикой

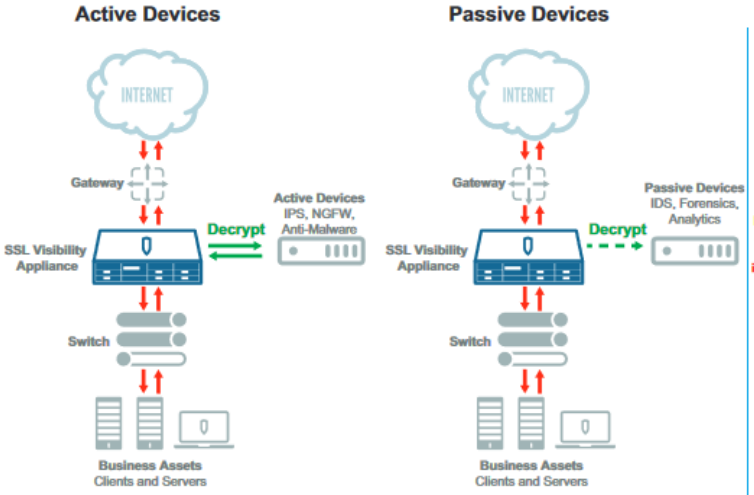


Figure 1: SSL visibility appliances decrypt SSL traffic and feed multiple active and passive devices

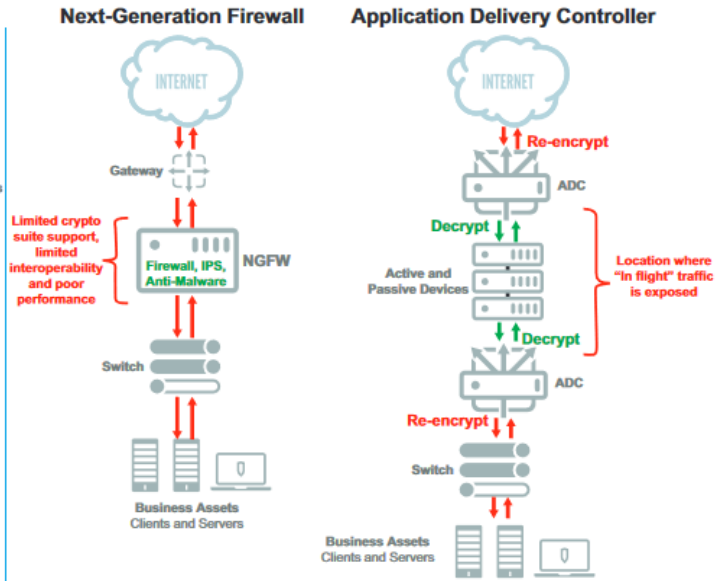


Figure 2: NGFWs and ADCs can decrypt SSL traffic, but NGFWs can't share data with other active devices, and decrypted traffic between ADCs is exposed and vulnerable to modification.

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 – 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

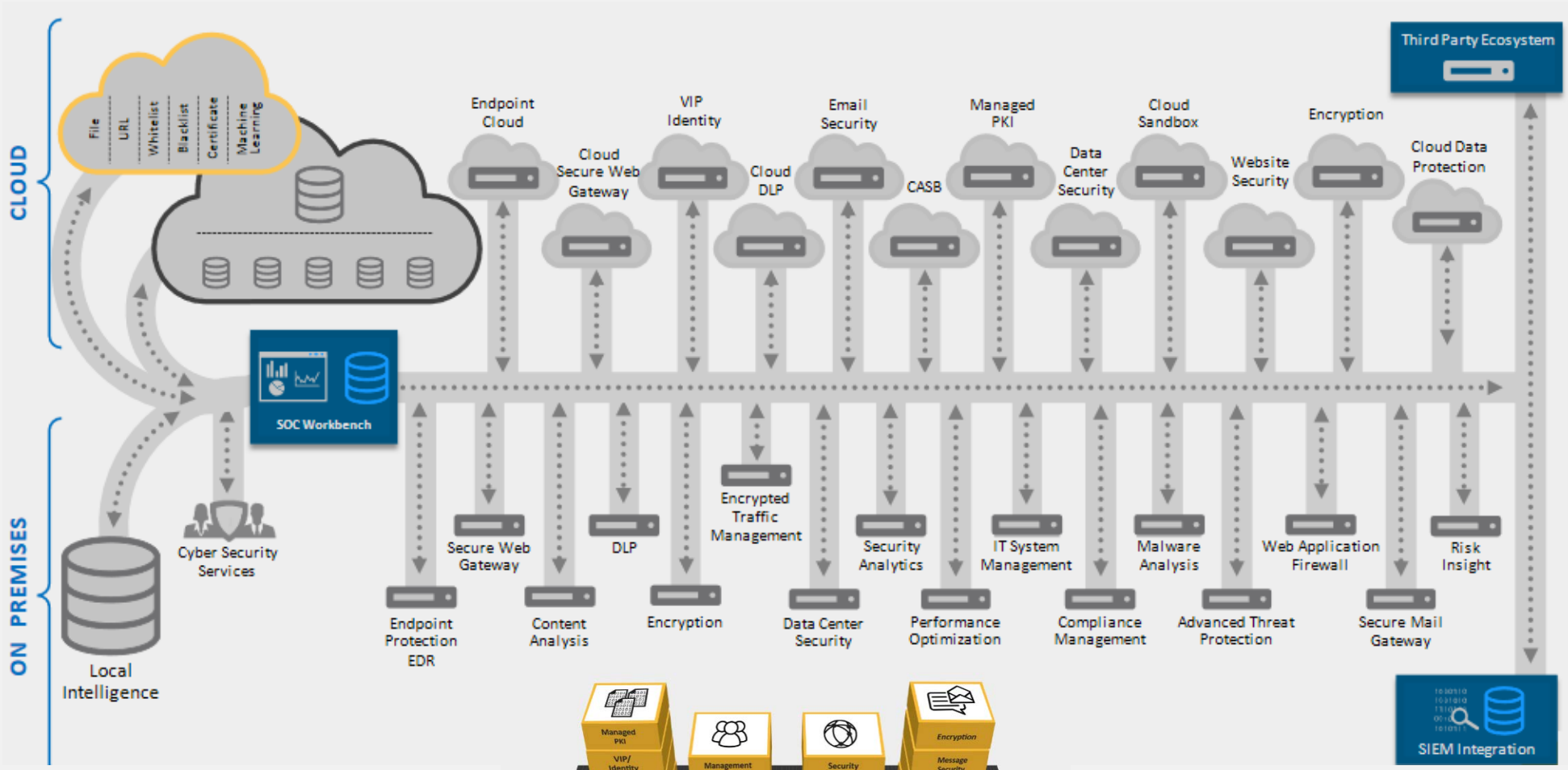
Проверка файлов для предотвращения вредоносных программ и продвинутых угроз

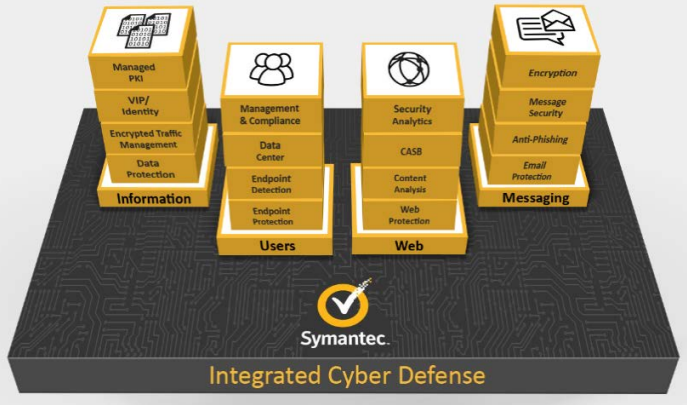
Белый / Черный список
Двойные AV сигнатуры
Анализ статического кода
Фильтрация перед песочницей

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

Лицензирование ex Blue Coat.

Наименование	Краткое описание	Самая свежая информация о решении	Принцип лицензирования
Решение от Symantec – SSL Visibility	Управление и дешифрация SSL трафика	https://www.symantec.com/products/information-protection/encrypted-traffic-management	Стоимость решения формируется из следующих составляющих: оборудование, Software Upgrade, модуль Host Categorization for SSL Visibility Appliance
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 – 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


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