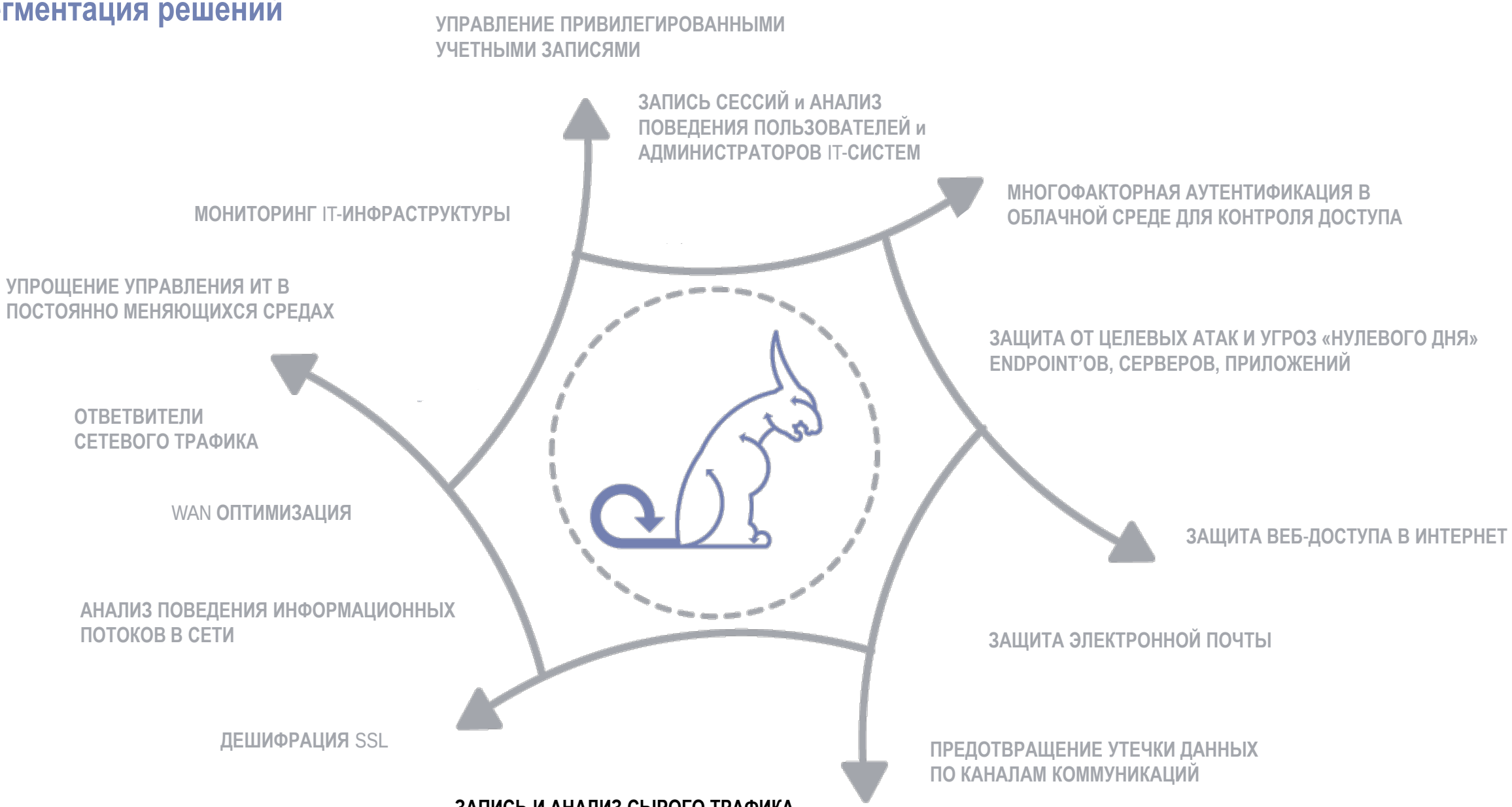
Сегментация решений



Решение от Symantec – Security Analytics

СИСТЕМА ЗАПИСИ И АНАЛИЗА СЫРОГО ТРАФИКА ДЛЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

https://www.symantec.com/theme/security-analytics-key-features

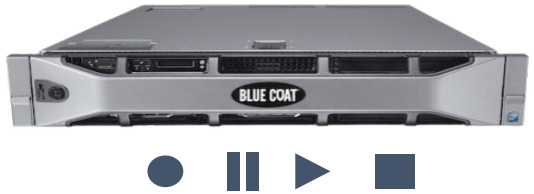
Symantec Security Analytics Appliances являются частью наших решений для реагирования на инциденты и судебной экспертизы. Предварительно настроенные устройства «под ключ» используют программное обеспечение Symantec Security Analytics для сбора, индексирования, классификации и обогащения всего сетевого трафика (включая полные пакеты) в режиме реального времени. Эти данные хранятся в оптимизированной файловой системе для быстрого анализа, мгновенного поиска и полной реконструкции сессий для поддержки всех ваших действий по реагированию на инциденты. Апплайнсы могут быть развернуты в любой точке сети: по периметру, в ядре, в магистрали 10 GbE или на удаленном канале, чтобы обеспечить четкий, эффективный интеллект для быстрой реакции и разрешения инцидентов в режиме реального времени.

Ключевые возможности

- Обнаружение и предотвращений угроз в сетевом трафике
- Обнаружение аномалий в сетевом трафике
- Классификация приложений
- Плотная интеграция с существующей инфраструктурой (DLP, SIEM, NGFW, песочницы и прочие)
- Высокая производительность и масштабируемость
- Развертывание «под ключ»

- Аналитика на сетевых уровнях 2-7
- Различные инструменты аналитики
- Полная реконструкция сеанса
- Визуализация данных
- Исследователь корневой причины
- Анализ временной шкалы
- Восстановление файлов и объектов
- IP-геолокация
- Анализ тенденций

«Камера наблюдения» в вашей сети



24/7 без потерь записи целых пакетов
Интеллектуальная обогащенная система записи
Трафик за дни, недели или месяцы
Устройство, программное обеспечение, или VM

Подробное описание возможностей Security Analytics см. на следующей странице

TOP-10 возможностей Symantec Security Analytics

1) Панель мониторинга предупреждений
На панели представлена гистограмма активности и новые «предупреждающие карты», отфильтрованные по оценкам угроз. На этой странице вы можете фильтровать свои оповещения по IP, по индикатору или по уровню угрозы.
Обнаружение аномалий
Функция обнаружения аномалий выполняет статистический анализ ваших перехваченных данных и предупреждает вас об аномальном поведении. Вы можете увидеть, когда произошла аномалия, как часто и какие другие конечные точки были задействованы.

2) SCADA
Промышленные системы управления (ICS) являются привлекательными объектами для кибер-атаки и, как и остальная часть сети, требуют полной видимости. Security Analytics поддерживает анализ протокола SCADA в промышленных средах управления. Также, выполняется контроль протоколов Modbus и DNP3, которые используются в работе на ядерных объектах, очистных сооружениях, электростанциях, нефтеперерабатывающих заводах, производственных объектах и многих других отраслях. Использование индикаторов, правил (уведомлений) и обнаружения аномалий возможно по индексированным атрибутам SCADA.

3) Динамическая фильтрация
Не весь аномальный трафик в равной степени вреден. Команды реагирования на инциденты могут исключить из анализа трафик, который они не рассматривают как угрозу и определить приоритетность доступных хранилищ для оптимизации расхода ресурсов. С помощью Security Analytics вы можете выборочно фильтровать и «не» собирать пакеты на основе правил (устранить потоковое видео/музыку, видеоконференции). Это позволит сосредоточиться на наиболее критичных задачах.

4) Режим «Capture Only»
В случае, когда требуется очень быстро перехватывать сырой трафик без необходимости обогащения его метаданными, выборочно отключите обогащение данных. При этом значительно повышается эффективность захвата трафика на одном устройстве.

5) Активные отчеты
Определите эксплойты и вредоносное ПО с отчетами Symantec Security Analytics, в которых представлена подробная картина сетевого трафика. Отчеты являются ключевой навигационной точкой, помогая с низкими трудозатратами быстро и точно находить нужные данные. Отчеты распределяются по категориям: applications, DNS, email activity, encryption, files, geolocation, network packets, social personas, threat intelligence, web activity.

6) Извлечение артефактов
Самым мощным функционалом для ситуационной осведомленности является способность Security Analytics реконструировать сетевой трафик, как будто он был передан вам как обычно, по сети. По перехваченным пакетам интуитивно понятно производится обнаружение, восстановление и доставка файлов в их исходном формате. Смотрите веб-страницу такой, как ее видел пользователь. Просмотр сообщений чата и электронной почты. Реконструирование PDF-файлов, документов Word, PPT-презентация, электронных таблиц Excel и многое другое в их исходном формате. Вы получаете возможность просматривать документы, а не только набор пакетов.
Хронологическая гистограмма сетевых артефактов помогает специалистам по реагированию на инциденты быстро визуализировать последовательность событий и значительно улучшает производительность поиска артефактов.

7)Классификация приложений
Symantec Security Analytics классифицирует более 2800 приложений в вашей сети; распознаются и индексируются тысячи атрибутов для удобного поиска. Вы не только можете определить конкретные приложения в сетевом трафике, вы можете искать атрибуты метаданных, такие как To, From, Subject Line, Protocol, Tunnel Initiator, обозначенный и детектированный MIME-тип и многое другое в сетевых потоках.

8) Сервис репутации / Обогащение данных
Аналитика безопасности обеспечивает проверку репутации по требованию нескольких доверенных поставщиков угроз, включая: Symantec ThreatExplorer, Domain Age, RobText, Team Cyrmu, YARA, WHOIS

9) Symantec Intelligence Services
Весь трафик, который был захвачен на устройстве Symantec Security Analytics, анализируется на предмет известных вредоносных сетевых, почтовых и файловых угроз. Security Analytics использует службы Symantec Global Intelligence Network, где собрана информация об угрозах от 175 миллионов конечных точек, сообщающих о миллиардах веб-угроз и URL-адресов.

10) Интеграция с другими средствами ИБ
Symantec Security Analytics может интегрироваться по REST API. Комплексное решение позволяет использовать такие технологии, как HP ArcSight, Splunk, IBM Qradar, Guidance, Countertack, Symantec ATP, песочницы и многое другое. Оптимизируйте рабочий процесс реагирования на инциденты и получите полные сведения об источнике и масштабе атаки.

Прочие возможности решения

11) Анализатор пакетов
Security Analytics включает полнофункциональный анализатор пакетов прямо на устройстве. Нет необходимости передавать огромные файлы по сети, чтобы определить, что пакеты, которые вы искали, там отсутствуют. Используйте синтаксис фильтра Wireshark и проведите свой глубокий анализ, не выходя из интерфейса Security Analytics. Отфильтрованные результаты будут легко доступны.

12) Панель мультимедиа
Панель мультимедиа позволяет быстро просматривать и анализировать все изображения и аудиофайлы, чтобы точно видеть, что видел пользователь. Фильтровать по файлу, расширению или размеру и связанным с ним метаданным, таким как: URL, IP-адрес источника / получателя, размер или тип MIME. Картинка порой заменяет тысячи слов, поэтому при расследовании инцидентов может стать ценным свидетельством несанкционированной деятельности.

13) Производительность / масштабируемость
Symantec Security Analytics способны захватывать весь трафик, попадающий в вашу сеть. Это дает вам полную запись сетевой активности. Устройства Security Analytics удовлетворяют жесткие требования крупнейших правительственных и корпоративных сетей, быстро восстанавливают и предоставляют реальные файлы из терабайтов сырых пакетных данных.
Варианты развертывания варьируются от небольших до специализированных устройств высокой плотности 10 Гбит с расширяемым хранилищем. Подходят для самых быстрых сетей на сегодняшний день. Symantec Security Analytics предоставляет вам возможность развертывания виртуального устройства. Крупные клиенты с обширными сетями выбрали Security Analytics как уникальное решение, способное удовлетворить их потребности в реагировании на инциденты.
Пассивно получая трафик от TAP или SPAN, Security Analytics невидима для остальной части вашей сети, захватывая трафик с линейными скоростями без добавления задержки.

14) Централизованное управление
Central Manager обеспечивает единую точку управления для Security Analytics 2G, 10G, VMs и высокоплотных хранилищ. Он обеспечивает централизованный доступ ко всем сенсорам Security Analytics для направленного, агрегированного поиска и управления. Благодаря поддержке более 200 сенсоров, Central Manager позволяет командам реагирования на инциденты проводить эффективные и всесторонние расследования по всей сети.

15) Сравнительная отчетность
Сравните захваченный сетевой трафик с предыдущими периодами, чтобы выявить признаки ненорм и установить базовую линию, а затем выделить и оповестить, когда происходят отклонения. Со сравнительной отчетностью вы понимаете тенденции с течением времени и определяете необходимость дальнейшего расследования.

16) Индикаторы / Правила
Индикаторы используют структурированный язык для наблюдения и идентификации конкретной деятельности. Используйте встроенные атрибуты метаданных, автоматически обновляемые данные сторонних индикаторов или используйте пользовательские обновления практически из любого источника.
Правила позволяют автоматизировать оповещения и общие действия для дополнительного анализа на основе любого показателя. Например, автоматически экспортируйте данные в PCAP, обогатите сохраненные метаданные или отправьте их в общий доступ к файлам, проанализируйте сторонними инструментами, такими как DLP.

17) Исследователь корневых причин
Быстрый переход к первопричине атаки с автоматической трассировкой цепей перенаправления HTTP. Проводник корневой причины коррелирует соответствующую информацию электронной почты, IM и HTTP для быстрого анализа и обнаружения того, как угроза попала в сеть и последующие действия. Как заявил один из пользователей: «Вы сделали одну из самых трудоемких функций для моей работы так же просто, как нажатие кнопки ... Это было просто!»

18) Импорт PCAP
Вы можете оптимизировать хранилище Security Analytics, экспортируя захваченный сетевой трафик как PCAP на внешнее хранилище для последующего импорта и анализа по мере необходимости.

19) Воспроизведение
Проигрывая ранее собранный трафик с обновленными инструментами анализа, вы можете определить, были ли вы заражены до того, как была классифицирована новая угроза.

20) Фильтр и воспроизведение трафика
Применение нескольких фильтров с возможностью запуска и остановки фильтров в любое время, продолжая фиксировать трафик. Это обеспечивает гибкость захвата трафика, который вы считаете наиболее важным для ваших исследований.

21) Расширенное хранение метаданных
Оптимизируйте хранилище, доступное на вашем устройстве Symantec Security Analytics, и создавайте независимые распределения хранилищ для метаданных и полных пакетов. Это позволяет сохранять и анализировать более длительные периоды метаданных и пакетов - недели, месяцы или более.

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

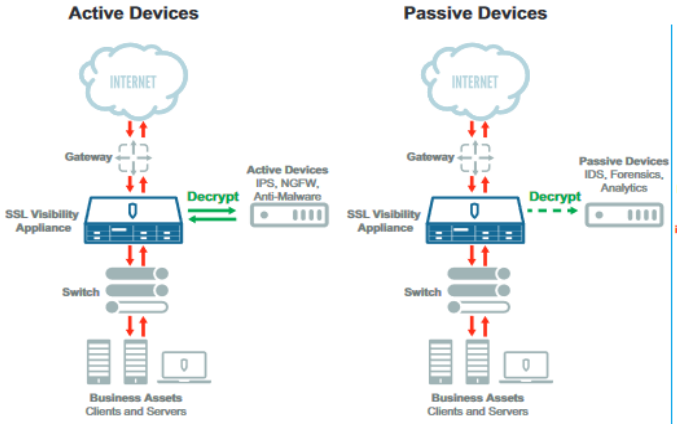


Figure 1: SSL visibility appliances decrypt SSL traffic and feed multiple active and passive devices

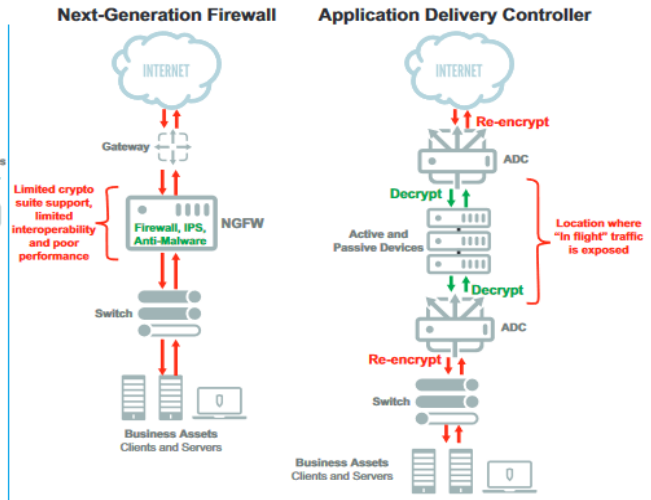
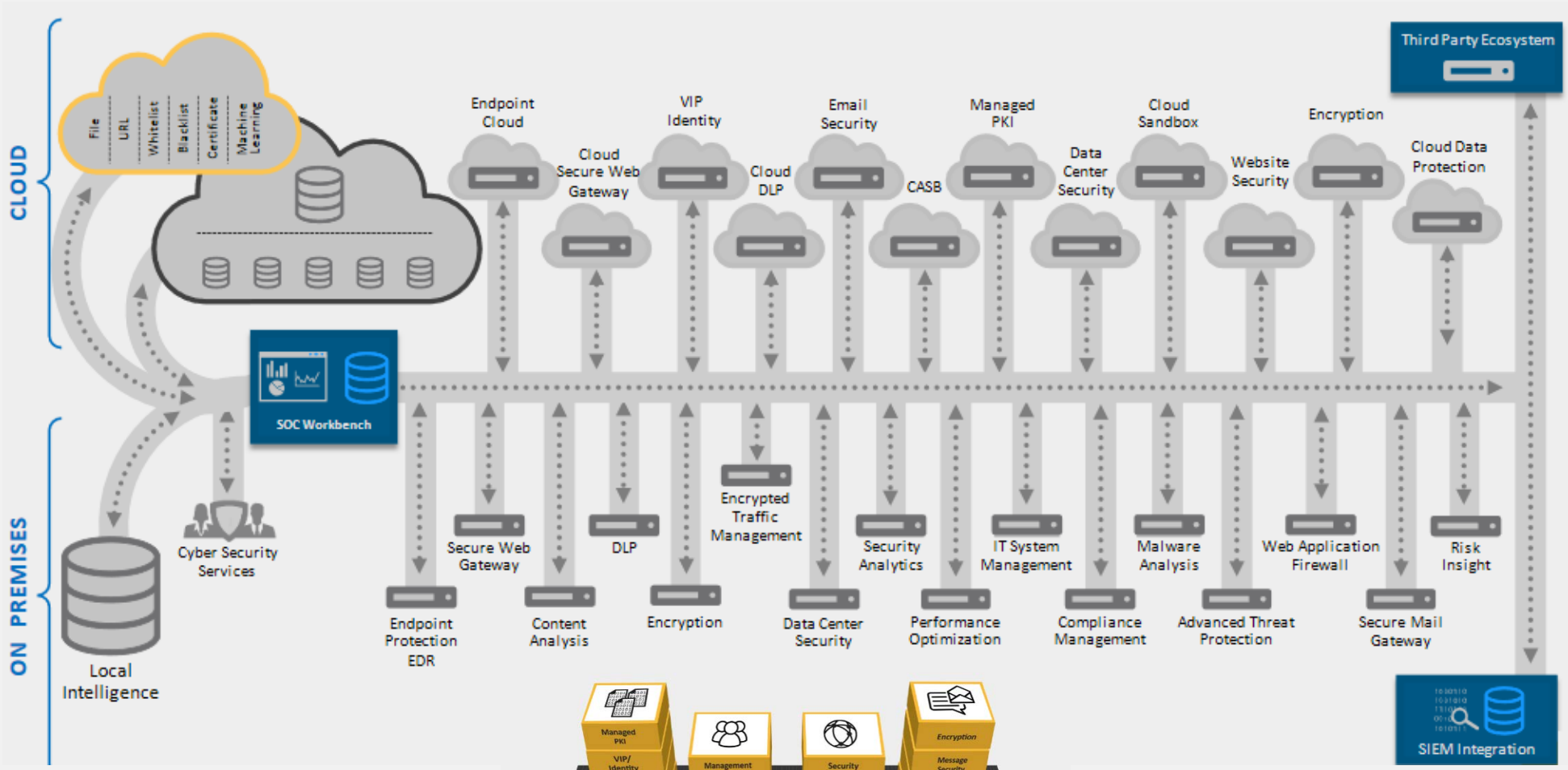
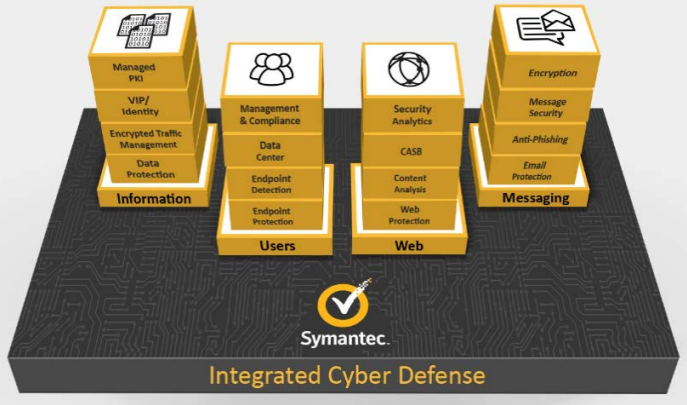


Figure 2: NGFWs and ADCs can decrypt SSL traffic, but NGFWs can't share data with other active devices, and decrypted traffic between ADCs is exposed and vulnerable to modification.

Лицензирование ex Blue Coat.

Наименование	Краткое описание	Принцип лицензирования
Решение от Symantec – SSL Visibility	Управление и дешифрация SSL трафика	https://www.symantec.com/products/information-protection/encrypted-traffic-management
Решение от Symantec – Security Analytics	Система записи и анализа сырого трафика для расследования инцидентов https://www.symantec.com/products/web-and-cloud-security/network-forensics-security-analytics	**Оборудование** Security Analytics 2/10 G Appliance Gen 6, Security Analytics 2/10 G Appliance Gen 6 Cold Standby, Security Analytics 10G-HD Appliance Fiber Channel Gen 6, Security Analytics 240TB (Raw) Storage Module Fiber Channel Gen 6, Security Analytics Central Manager Appliance Gen 6, Security Analytics Central Manager Appliance Gen 6 Cold Standby, Blue Coat Security Analytics J5300 40T Direct-Attached Storage (includes storage license), Cold Standby Unit Blue Coat Security Analytics J5300 40T Direct-Attached Storage, Security Analytics 240TB (Raw) Storage Module Fiber Channel Gen 6 (Includes Storage License), Security Analytics 240TB (Raw) Storage Module Fiber Channel Gen 6 Cold Standby **Лицензии** Upgrade from Cold Standby/TAB to Production Intelligence Services for Security Analytics (Enables ThreatBLADES) 2G/10G/10G-HD Sensor Appliance Security Analytics Storage Expansion License, per TB per System Service, Security Analytics Storage Expansion License, per TB per System Upgrade Kit


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