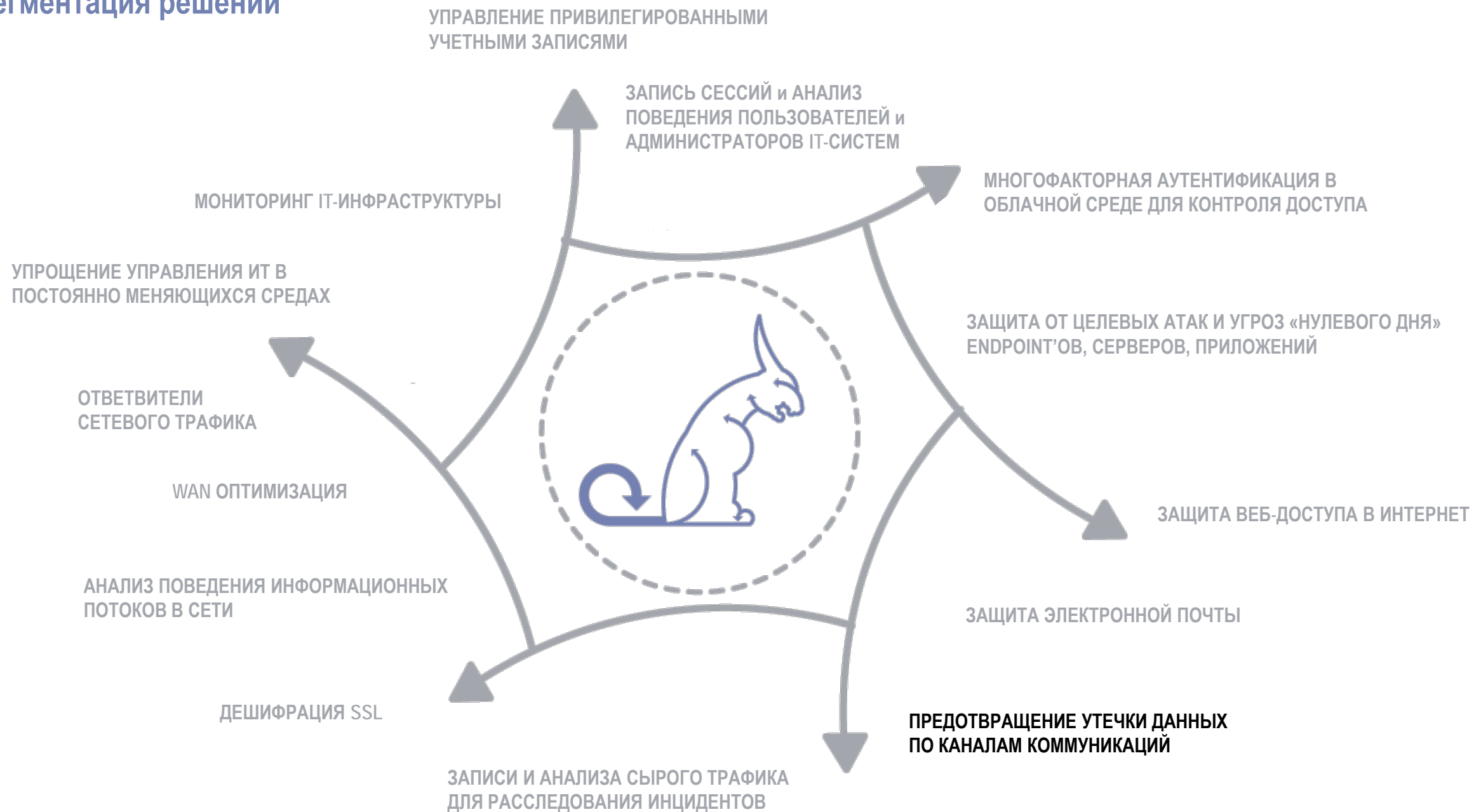


# Сегментация решений





## Решение от Symantec – Data Loss Prevention (DLP)

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ ПО КАНАЛАМ КОММУНИКАЦИЙ

<https://www.symantec.com/ru/ru/data-leak-prevention/>

### Поиск, мониторинг и защита конфиденциальной корпоративной информации.

DLP — это технология обеспечения безопасности с учетом содержимого, которая дает ответы на три главных вопроса о конфиденциальной корпоративной информации:

- Где хранится информация?
- Как она используется?
- Как обеспечить защиту от утечки и кражи информации?

### Data Loss Prevention

Чтобы ответить на эти вопросы, Symantec использует технологии **обнаружения** данных, хранящихся в облаке, на мобильных устройствах или в локальных средах; **мониторинга** использования данных в корпоративной сети и за ее пределами; а также **защиты** информации от утечки или кражи.

### Почему именно Symantec?

Ведущее решение Symantec расширяет область применения в том числе на **облачные среды** и **мобильные устройства**. Таким образом, Symantec DLP имеет расширенные по сравнению с конкурентами границы применения политик обеспечения безопасности. При низкой общей стоимости владения решение предоставляет интуитивно понятные инструменты управления инцидентами и политиками, а также обширную поддержку каналов передачи данных с высокой степенью риска.

### Data Loss Prevention — Управление и отчетность

С расширением набора поддерживаемых приложений и устройств становится все сложнее обеспечивать последовательное выполнение требований и политик в области безопасности. Унифицированная консоль управления Symantec DLP позволяет повсеместно применять единожды созданные политики и быстро устранять последствия инцидентов на основе автоматизированных рабочих процессов. Кроме того, в состав Symantec DLP включены средства подготовки отчетов, которые позволяют принимать более взвешенные решения по управлению рисками, демонстрируя преимущества DLP.

### Функционал системы набирается из модулей:

#### Data Loss Prevention for Cloud

Для многих предприятий перенос локальных приложений в облако позволяет повысить гибкость и снизить затраты. Но как реализовать преимущества облачных технологий без потери наглядности и контроля? Symantec DLP for Cloud решает эту проблему путем добавления надежных функций поиска, мониторинга и предотвращения утечки данных для облачных хранилищ и электронной почты, включая MS Office 365 и Box.

#### Data Loss Prevention for Endpoint

Несмотря на ускоренное внедрение мобильных и облачных технологий, традиционные конечные точки по-прежнему являются центральным репозиторием конфиденциальной корпоративной информации. Symantec DLP for Endpoint обеспечивает надежную защиту всей информации, предоставляя функции поиска, мониторинга и защиты данных на физических и виртуальных конечных точках для пользователей внутри корп. сети или за ее пределами.

#### Data Loss Prevention for Mobile

Идея BYOD стирает границы между работой и личной жизнью. Сегодня пользователи рассчитывают на круглосуточный доступ к конфиденциальным корпоративным данным независимо от используемого устройства или соединения. По статистике, двое из пяти сотрудников загружают рабочие файлы на свои смартфоны и планшеты. Symantec DLP for Mobile обеспечивает наглядное представление и контроль для мобильных пользователей, не подвергая риску вашу информацию.

#### Data Loss Prevention for Network

Согласно результатам исследований, примерно половина сотрудников постоянно пересылают рабочие файлы по электронной почте на личные учетные записи, поэтому электронная почта и Интернет являются самыми распространенными каналами утечки данных. Symantec DLP for Network помогает решить эту проблему с помощью функций мониторинга широкого спектра сетевых протоколов и предотвращения случаев неправильной обработки конфиденциальных данных.

#### Data Loss Prevention for Storage

Объем неструктурированных данных растет с пугающей быстротой, увеличиваясь на 70 процентов каждый год, в результате многие организации испытывают трудности при управлении информацией и ее защите. Symantec DLP for Storage помогает получить контроль над всеми неструктурированными данными, чтобы исключить риски, связанные с небрежными действиями сотрудников или атаками злоумышленников.

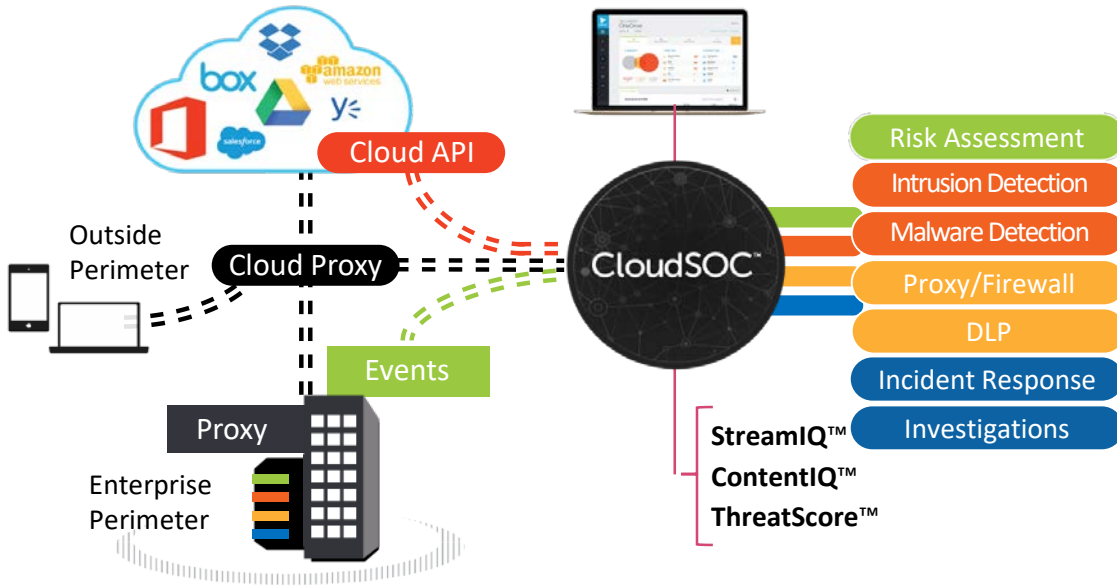




# Решение от Symantec – Cloud Access Security Broker

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 разворачивается 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>





Наименование	Краткое описание	Самая свежая информация о решении	Принцип лицензирования
<b>Решение от Symantec – Cloud Access Security Broker</b>	Контроль передаваемых данных в облачные приложения и сервисы	<a href="https://www.symantec.com/products/web-and-cloud-security/cloud-application-security-cloudsoc">https://www.symantec.com/products/web-and-cloud-security/cloud-application-security-cloudsoc</a>	<p>По модулям, модули наполняются по пользователям:</p> <ul style="list-style-type: none"> <li>• Elastica CASB Audit - App Visibility, Analytics and Control, Add Users</li> <li>• Elastica CASB Gateway - All Gatelets with Detect, Investigate and Protect, Add Users</li> <li>• Pack - Cloud App API, Detect, Investigate and Protect - Advanced Edition</li> <li>• Add Users, Blue Coat Cloud Data Protection Communication Server</li> <li>• Blue Coat Cloud Data Protection Communication Server, Subscription</li> <li>• Symantec Cloud Data Protection for AppService</li> <li>• Blue Coat Cloud Data Protection Server Subscription, Development Environment per App</li> </ul>
<b>Решение от Symantec – Data Loss Prevention (DLP)</b>	Предотвращение утечки данных по каналам коммуникаций	<a href="https://www.symantec.com/ru/ru/data-leak-prevention/">https://www.symantec.com/ru/ru/data-leak-prevention/</a> <a href="https://www.symantec.com/ru/ru/data-loss-prevention/">https://www.symantec.com/ru/ru/data-loss-prevention/</a>	<p>Лицензируется по модулям. Объем модулей набирается по количеству клиентов и устройств :</p> <p><b>По управляемым пользователям:</b></p> <p>DLP DISCOVER SUITE: •Network Discover •Network Protect  DETECTION PRODUCT: •Form Recognition  NETWORK PRODUCTS: •Network Monitor •Network Prevent for Email •Network Prevent for Web  STORAGE PRODUCTS: •Network Discover •Network Protec  CLOUD PRODUCTS: •Cloud Prevent for Microsoft Office 365 Exchange •Cloud Storage [for Box]  VERITAS PRODUCTS: •Veritas Data Insight •Veritas Data Insight Self Service Portal</p> <p><b>По управляемым устройствам:</b></p> <p>Endpoint Discover/Prevent, Mobile Prevent, Mobile Email Monitor.</p> <p><b>По БОЛЬШЕМУ значению пользователей или устройств:</b></p> <p>DLP ENTERPRISE SUITE: •Network Monitor •Network Prevent for Email •Network Prevent for Web  •Network Discover •Network Protect •Endpoint Discover •Endpoint Prevent •Mobile Email Monitor  •Mobile Prevent</p> <p><b>Oracle:</b></p> <p>можно использовать имеющийся или купить у Symantec (лицензируется по CPU)</p>

**STANDARD EDITION ONE VS. STANDARD EDITION (Oracle DB for DLP)**

Symantec resells Oracle Standard Edition One and Standard Edition licenses on a per CPU (Processor) basis:

-Oracle Standard Edition One is available for single server with up to 2 Processors.

-Oracle Standard Edition, which adds Oracle Real Application Clusters, is available for single or clustered servers with up to 4 Processors.



