CASB 2.0

Symantec

Защита облачных приложений следующего поколения

CASB 2.0

Защита облачных приложений следующего поколения

Введение	3
CASB 1.0 – решение проблемы	3
Ограничения CASB 1.0	4
Возникновение потребности в CASB 2.0	4
CASB & SWG Не только обнаружение Shadow IT, нужен контроль	5
CASB & DLP Устранение многочисленных островов DLP	6
CASB & Encryption Сквозное управление правами доступа к данным	7
CASB & Malware Protection Использование сети Global Threat Intelligence для облаков	8
CASB & User Authentication Больше, чем Single-Sign-On (SSO)	9
CASB & Endpoint Protection Упрощение развертывания конечных точек	10
Заключение	11

Введение

В последние несколько лет появились решения класса Cloud Access Security Broker (CASB), направленные на удовлетворение новых требований безопасности, которые связаны с быстро растущим рынком облачных приложений и услуг. Как вы, несомненно, уже наблюдаете в своей компании, облачные приложения, такие как G Suite, Office 365 и Salesforce, предлагают огромные преимущества с точки зрения совместной работы и производительности сотрудников, но они также существенно увеличивают площадь атак в вашей компании.

В компаниях часто не знают, к каким облачным приложениям и сервисам обращаются их сотрудники. Такие облачные ресурсы называют Shadow IT. Еще более важно то, что компании не знают, что сотрудники делают в этих облачных приложениях, какую конфиденциальную информацию выгружают, к каким данным предоставляют общий доступ (создавая Shadow Data). И наконец, перспектива размещения ценных корпоративных данных в сервисах сторонних вендоров вызывает озабоченность из-за возможной эксфильтрации этих данных злоумышленниками. Большинство провайдеров облачных приложений поддерживают модель «разделенной ответственности», при которой они защищают серверную инфраструктуру, но не отвечают за действия пользователей при работе с приложением и за загружаемые им данные. Таким образом, скомпрометированные учетные данные могут привести к значительному ущербу, ответственность за который находится вне компетенции провайдера облачных услуг.

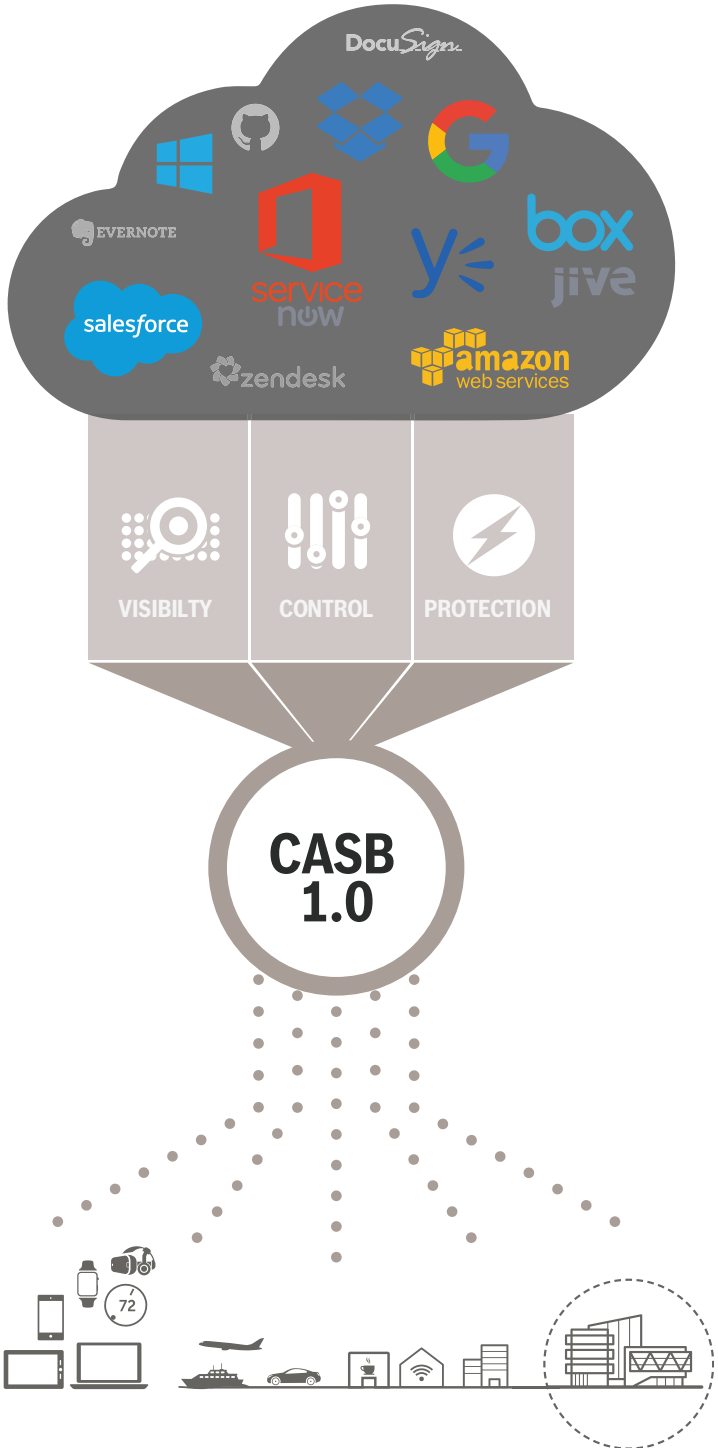
“К 2020 85% больших компаний будут использовать CASB- платформу при работе с облачными сервисами. Для сравнения – сегодня их число составляет менее 5%”.

—Gartner, ‘Market Guide for Cloud Access Security Brokers’, 24.10.2016

CASB 1.0 – решение проблемы

Первое поколение решений класса CASB помогало пользователям облачных приложений решать эти новые проблемы. Традиционное решение CASB 1.0 обеспечивает:

- Прозрачность использования облачных приложений, включая обнаружение использования несанкционированных облачных приложений, известных как Shadow IT.
- Прицельный контроль конфиденциальных данных, включая облачное DLP и реализацию политики токенизации и шифрования.
- Защита от вредоносных атак, посредством сбора аналитических данных о поведении пользователя или обнаружения аномалий для идентификации подозрительных действий пользователя.



Ограничения CASB 1.0

Хотя первые CASB продукты помогли решить новые проблемы, у них все же есть ограничения. Основное ограничение CASB 1.0 заключается в создании островка безопасности в облаке, не связанного с основными инвестициями компании в безопасность. Это затрудняет развертывание, требует высоких затрат и ограничивает эффективность безопасности.

Наличие отдельных зон безопасности, где решение CASB отделено от систем Data Loss Prevention (DLP), Secure Web Gateways (SWG), защиты конечных точек, шифрования и аутентификации, создает пробелы в функциональности, которые могут привести к утечке данных, компрометации учетных записей и заражению сети. Например, как можно гарантировать непрерывную реализацию политик основной системы DLP между локальными и облачными ресурсами? Или как можно не только идентифицировать рисковые приложения, но и ограничить их использование в реальном времени? Как можно гарантировать, что «лучшие в своем классе» современные инструменты защиты от вредоносного кода эффективно сканируют поток данных при взаимодействии с облаками?

Возникновение потребности в CASB 2.0

Для эффективной защиты облачных приложений и данных независимо от пользователя, местонахождения и устройства доступа CASB решение должно бесшовно интегрироваться с базовой инфраструктурой безопасности, включая DLP, веб-защиту, средства управления конечными точками, шифрования, аутентификации пользователей и передовой защиты от вредоносных программ. В конечном счете, вам захочется использовать все средства защиты, в которые вы уже инвестировали, для получения наилучшей защиты облачных ресурсов. Решения CASB 2.0 интеллектуально интегрируют функциональность CASB и все основные технологии защиты для наиболее широкого покрытия всей облачной активности.

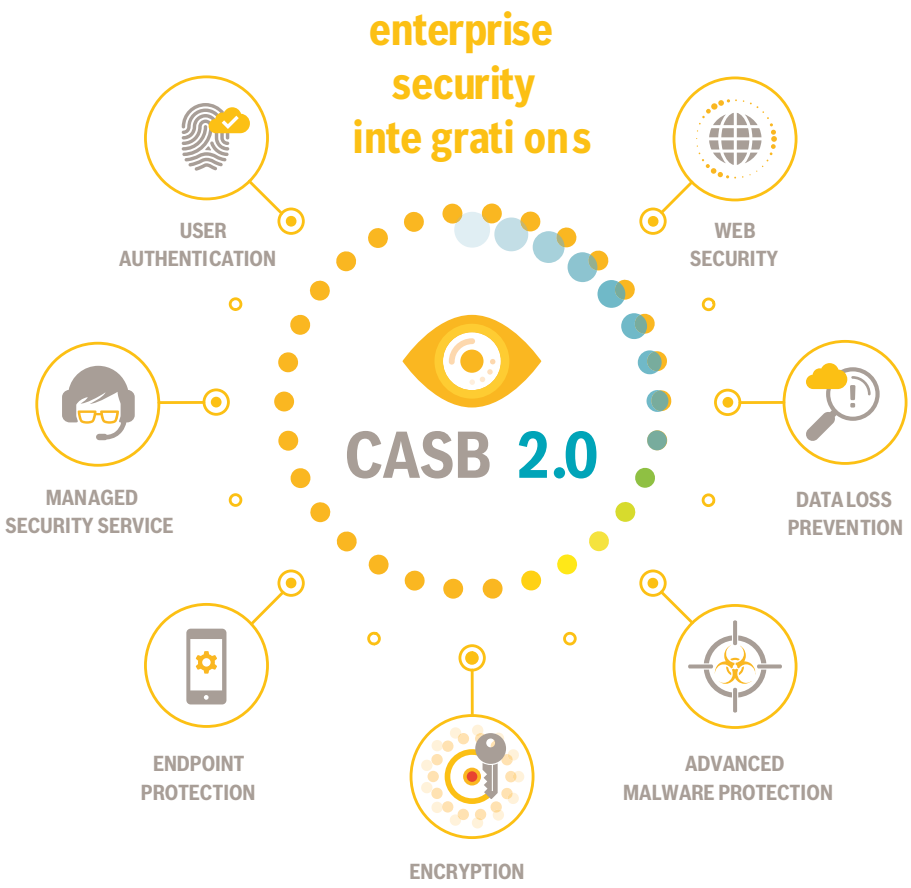
Решение CASB 2.0 обеспечивает следующие преимущества:

1. **Повышение эффективности безопасности.**
2. **Снижение операционых расходов.**
3. **Улучшение пользовательского опыта.**

Полноценное решение CASB 2.0 не может быть реализовано путем взаимодействия отдельных решений, требуется глубокая интеграция, чтобы решение было действительно ценным.

Такое решение должно:

- Обмениваться критической информацией между системами через нативные API
- Обеспечивать непрерывную реализацию политик через облачные и другие каналы
- Интегрировать пользовательские интерфейсы для обогащения управляющих консолей различных ролей
- Уменьшать сложность развертывания, связанную с многообразием решений для защиты
- Полнофункциональное решение CASB 2.0 дает значительные преимущества компаниям, которые желают использовать всю мощь облаков без ущерба для безопасности.



CASB & SWG

Не только обнаружение Shadow IT, нужен контроль

Многим компаниям требуется некоторая форма функционала SWG и CASB. Тем не менее, при развертывании сразу двух решений возникает много практических вопросов. Как направлять трафик между ними? Сколько раз пользователю придется аутентифицироваться? Как я могу организовать совместное использование данных этими системами? Какие я могу предпринять действия с рискованными приложениями при их обнаружении?

Используя подход CASB 2.0, решения SWG и CASB можно грамотно интегрировать для получения большего эффекта.

1. Расширьте возможности SWG при помощи обогащенных данных облачных приложений

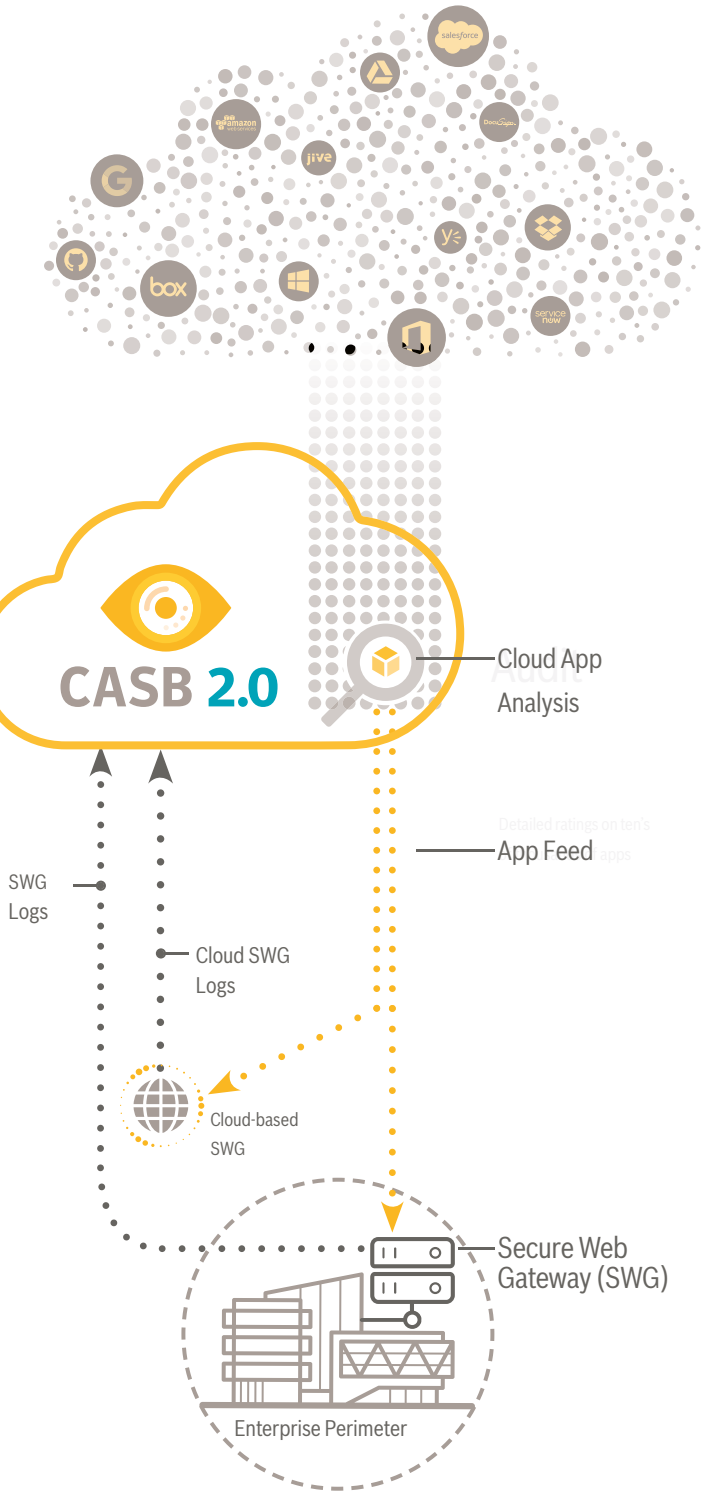
Полноценное CASB решение должно иметь мощную базу данных приложений, которая способна анализировать десятки тысяч облачных приложений на основе десятков характеристик защищенности (например, поддержка MFA). При использовании CASB 2.0 эту базу данных можно автоматически применять в локальных и облачных SWG решениях, повышая их возможности обеспечения прозрачности. Фактически, те компании, которые неохотно размещают решения в облаке, могут пользоваться существующими локальными SWG устройствами, чтобы получить функционал CASB.

2. Получите динамический контроль над Shadow IT

Полноценные CASB решения способны обнаруживать использование Shadow IT, включая рискованные приложения и сервисы, которые используют сотрудники без ведома и контроля работодателя. Но что компании могут делать с этой информацией? Разработка индивидуальных политик для блокирования каждого рискованного приложения на основе его названия или URL – утомительная работа, особенно если новые приложения обнаруживаются каждую неделю. Вместо этого, решение CASB 2.0 позволит определить динамические политики на основе критических рисковых атрибутов, таких как Business Readiness Rating (рейтинг, формируемый из 60+ атрибутов безопасности) или совместимость с SOC-2. Далее, эти политики могут реализовывать SWG решения без постоянного внесения ручных изменений. Решение CASB 2.0 непрерывно информирует SWG о появлении новых приложений и сервисов, которые соответствуют выбранным критериям, автоматизируя таким образом контроль за «теневым» ИТ.

3. Упрощайте развертывание

Внедрение и SWG, и CASB может быть нетривиальным. CASB 2.0 развертывается проще за счет возможностей управления трафиком между различными решениями (оптимизирует прокси цепочки), унификации аутентификации и интеграции пользовательского интерфейса. Эти и другие практические возможности обеспечивают простоту использования для администраторов и снижают непредвиденные расходы.



CASB & DLP

Устранение многочисленных островов DLP

Быстрый рост числа облачных приложений и сервисов, особенно обмен файлами, увеличил потребность в эффективных решениях Data Loss Prevention. Де-факто облако становится средством для обмена контентом, включая конфиденциальные и регулируемые данные. Много компаний уже инвестировали в DLP решения, которые нацелены на множество каналов, включая хранение информации, электронную почту, конечные точки и другие. Они ищут бесшовный способ расширить свои решения на облако.

Используя подход CASB 2.0, DLP решения могут бесшовно интегрироваться для управления всеми каналами, гарантируя эффективное покрытие и простое управление.

1. Используйте единые DLP политики локально и в облаке

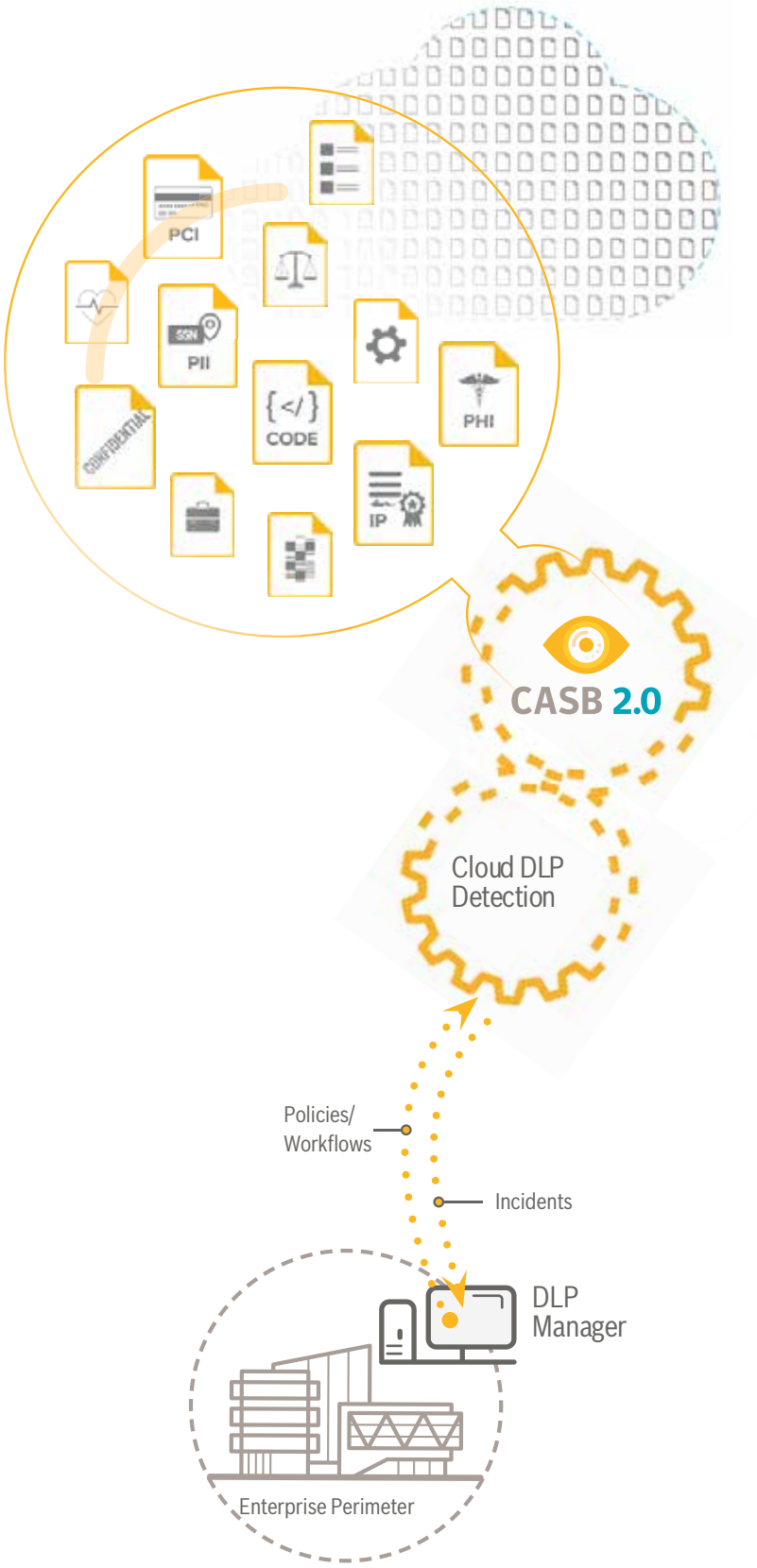
Решение CASB 2.0 должно уметь применять существующие, тщательно проработанные DLP политики, рабочие процессы и бизнес логику для облачных приложений и сервисов. Это помогает избежать неравномерных или противоречивых результатов при реализации DLP в различных каналах. Это также снижает непредвиденные расходы, позволяя избежать эффекта двух команд, управляющих DLP, наряду с попытками реплицировать политики и рабочие процессы.

2. Получите оптимальную производительность с помощью нативных облачных API

Хотя были предложения использовать ICAP с локальной DLP технологией обнаружения для сохранения политик, этот подход приводит к значительной потере полосы WAN и добавляет задержку. CASB 2.0, напротив, должно использовать облачное обнаружение наряду с нативными API для CASB, так что контент, хранимый в облаке, анализируется там же. Это помогает избежать передачи данных из облака в локальную сеть и обратно. Нативное API решение также обеспечивает совместное использование обогащенных атрибутов CASB и DLP системами, так что традиционные DLP решения могут использовать специфичные для облака атрибуты для анализа и создания политик.

3. Расширьте возможности DLP глубоким анализом CASB

Решение CASB 2.0 должно добавлять в традиционные DLP решения информацию, специфичную для облака. Например, оно должно позволять DLP использовать дополнительные, уникальные для облака атрибуты, при создании политик, например, «unshare a link» (отменить общий доступ к ссылке). Аналогичным способом, подробные данные о действиях пользователя в облаке или оценки угроз безопасности в результате действий пользователя могут совместно использоваться через панель управления DLP. Конечная цель состоит в том, чтобы дать возможность специалистам DLP иметь полную видимость и управление функциями, относящимся к ним, через единую консоль.



CASB & Encryption

Сквозное управление правами доступа к данным

Многие решения CASB 1.0 имеют возможность шифрования или токенизации. В этом случае обычно предполагается шифрование контента на пути к облачным приложениям и сервисам, а затем расшифровка этого контента при скачивании из облака. Однако, после скачивания конфиденциальной информации из облака, она может путешествовать в любом направлении. Конечные пользователи могут выгружать такой контент в личные облачные приложения, копировать на собственные устройства или USB-накопители. Фактически, компании могут потерять контроль над конфиденциальной информацией.

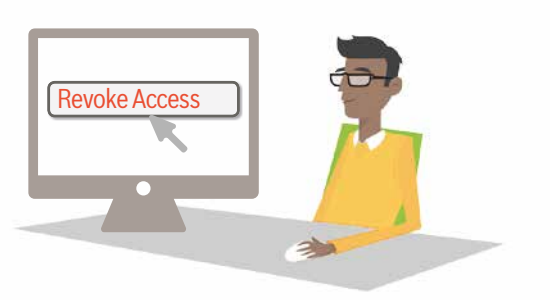
Использование CASB 2.0 может оказаться более надежным решением благодаря умной интеграции сквозного шифрования с технологией CASB. При таком подходе контент может быть зашифрован на пути к облачному приложению и сервису и оставаться зашифрованным при скачивании на различные конечные точки. Такой подход имеет много преимуществ:

1. Безопасность, которая следует за данными

РШифрование можно запустить на основе разнообразных критериев – при обнаружении финансовых данных или другого конфиденциального контента. После загрузки такого контента, он остается зашифрованным независимо от его перемещения, что гарантирует защиту данных безотносительно к способу распространения. Пользователям необходимо аутентифицироваться для просмотра контента, контроль над которым остается в руках предприятия.

2. Доступ к контенту, который может быть отозван в любое время

Полноценное CASB 2.0 решение должно уметь отслеживать контент во время его перемещения. В любой точке и в любое время компания должна быть в состоянии отозвать доступ к своим документам, например, когда данные стали недействительными. Идея отправки такого документа в «цифровой шредер» одним нажатием кнопки звучит заманчиво.



3. Поддержка разных платформ

Хотя некоторые облачные приложения имеют схожие возможности, корректно работающее решение со всеми облачными приложениями будет более ценным. Это дает возможность специалистам по безопасности более гибко применять правила в ландшафте облачных приложений и услуг, не думая об ограничениях и нюансах функций отдельных облачных приложений.

CASB & Malware Protection

Использование сети Global Threat Intelligence для облаков

Вредоносные программы, в том числе целенаправленног о характера, влияют на файлы и системы не только внутри периметра вашей сети, но и на облачные учетные записи. Данный контент может попасть в облачное приложение через прямое взаимодействие облако-облако. Такой контент можно создать в облачном приложении. В любом случае, традиционной защиты периметра уже недостаточно. Вредоносный код в облачном приложении является проблемой еще и потому, что многие пользователи синхронизируют вычислительные среды с облаком и организуют для них совместный доступ, что позволяет вредоносному ПО быстро распространяться.

Многие более ранние решения CASB просто использовали open source алгоритмы анализа вредоносных программ, но не содержали полноценную расширенную защиту от вредоносного ПО. Решение CASB 2.0 должно использовать лучшие в своем классе технологии защиты от вредоносных программ, чтобы обеспечить полноценную защиту своих ресурсов в облаке.

1. Используйте Global Threat Intelligence

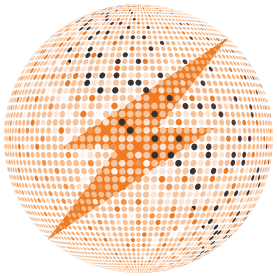
Решения CASB 2.0 должны использовать лучшую в своем классе сеть global threat intelligence для анализа облачного контента, включая анализ репутации файлов и отслеживание последних данных об угрозах, касающихся большого количества облачных приложений и сервисов. Это обеспечивает более полное покрытие всего ландшафта передачи корпоративной информации..

2. Блокирование и нейтрализация вредоносных файлов

Решения CASB 2.0 должны использовать ведущие в отрасли алгоритмы антивирусного сканирования, чтобы обеспечить тщательную полную проверку данных, передаваемых и хранимых в облачных приложениях. Этот анализ должен иметь практическую ценность, позволяющую пользователям блокировать и помещать в карантин вредоносный контент, чтобы не допустить заражения компании.

3. Обнаружение угроз нулевого дня

Решение CASB 2.0 должно интегрироватьс я с решениями Advanced Threat Protection (ATP), чтобы иметь возможность обнаруживать угрозы нулевого дня в облачных учетных данных и в транзакциях между пользователями и облачными приложениями. Необходимо использовать облачные песочницы для анализа неизвестных файлов на возможное вредоносное поведение.



Global Threat Intelligence Network

AV Scanning

Sandboxing

CASB & User Authentication

Больше, чем Single-Sign-On (SSO)

Аутентификация пользователей – это неотъемлемый компонент инфраструктуры облачной безопасности. Большинство продуктов CASB 1.0 поддерживают взаимодействие с рядом SSO решений для организации аутентификации, обычно через интеграцию SAML.

Подход CASB 2.0 может обеспечить более глубокий уровень интеграции. Вместо одностороннего обмена информацией (от SSO к CASB), решения CASB 2.0 могут использовать двусторонний обмен информацией. При этом аналитические данные CASB передаются решениям аутентификации пользователей. Такой подход может оказаться ценным, потому что дает возможность компаниям динамически изменять требования к доступу на основе реальной ситуации с рисками в сети. Эта концепция называется Adaptive Authentication или настраиваемая аутентификация.

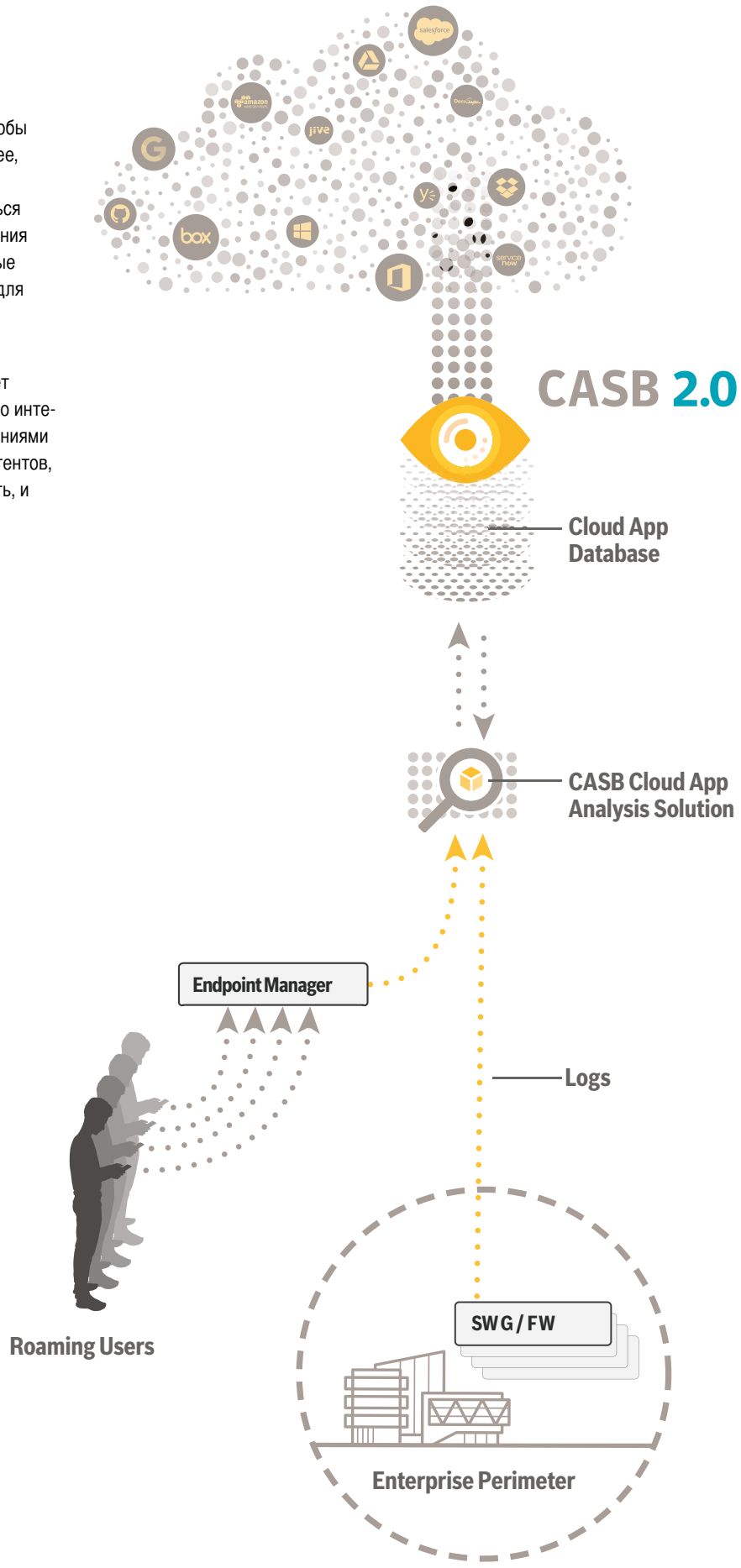
Например, если оценка угроз пользователя превышает определенный уровень (определяется на основе подозрительной активности), система может запустить требование многофакторной аутентификации (MFA) для авторизации этого пользователя. Полноценное решение должно позволять компаниям тонко определять политики на основе большого количества атрибутов транзакции. Это дает возможность повысить требования к аутентификации в тех случаях, когда пользователь собирается выполнить рисковые транзакции.

CASB & Endpoint Protection

Упрощение развертывания конечных точек

Многие решения CASB используют агентскую технологию, чтобы направлять трафик или реализовывать политики. Тем не менее, во многих организациях уже могут быть развернуты решения для защиты конечных точек, и такие компании могут отказаться развертывать еще один агент. При этом, существующие решения для защиты конечных точек генерируют аналитические данные о работе пользователя, которые могут оказаться полезными для CASB решений.

CASB 2.0 может принести больше пользы, если интеграция с существующими решениями для защиты конечных точек будет реализована на более глубоком уровне. Для упрощения можно интегрировать функциональность агента CASB с основными решениями для защиты конечных точек, снижая, таким образом, число агентов, которые необходимо развертывать и которыми надо управлять, и расширяя сеть устройств, поддерживающих CASB.



Заключение

В документе представлены только некоторые примеры, показывающие, как интегрирование технологии CASB с основными технологиями безопасности могут оказаться очень ценными для компаний, мигрирующих в облако. Использование CASB 2.0 позволяет повысить эффективность работы существующей инфраструктуры безопасности и избегать «просачивающихся» угроз. Также с CASB 2.0 снижаются непредвиденные расходы и повышается удобство использования решений как администраторами, так и пользователями. В отличие от развертывания «островков» безопасности, решающих отдельные проблемы, решения CASB 2.0 представляют собой более цельный подход, который предназначен связать комплексную инфраструктуру безопасности и дать наглядную картину взаимодействия локальной сети с облаками.

Дистрибьютор в России компания Web Control
+7(495)925-7794 / info@web-control.ru / www.web-control.ru