Спецификация

Symantec Security Analytics Appliance

Быстрое реагирование и тщательное расследование инцидентов

Краткий обзор

Многофункциональные устройства Security Analytics Appliance:

- **Быстрая идентификация угроз** — предоставляет полную информацию о трафике: содержимое, классификацию, данные глубокого анализа пакетов, справочные сведения об угрозах и выявленные аномалии.
- **Оперативное реагирование на инциденты и упрощение расследований** — предоставляет данные о контексте, в котором произошел инцидент, помогая администраторам оперативно реагировать, устранять последствия и анализировать причины.
- **Экономическая эффективность** — устройства поставляются готовыми к работе, быстро устанавливаются и легко интегрируются в имеющуюся инфраструктуру, дополняя и упрощая процессы, связанные с безопасностью.

Для борьбы с комплексными угрозами, которым подвергается ваша организация, нужны интеллектуальные средства защиты, позволяющие быстро и эффективно отражать атаки. Чтобы вовремя выявлять и устранять уязвимости, вы должны полностью контролировать сетевой трафик и располагать обширным аналитическими возможностями. Устройства Symantec Security Analytics Appliance дают полную картину происходящего в сети организации и позволяют проводить необходимые расследования. Таким образом, у вас появляется возможность выполнять ретроспективный анализ и оперативно реагировать на инциденты безопасности, чтобы вовремя защищать сотрудников, укреплять периметр сети и улучшать процессы, связанные с безопасностью.

Интегрированное решение, готовое к использованию

Устройства Symantec Security Analytics Appliance входят в состав решений Incident Response and Forensics. Полностью готовые к эксплуатации и заранее настроенные устройства используют программное обеспечение Symantec Security Analytics для сбора, индексации, классификации и аннотации всего сетевого трафика (включая полные пакеты) в реальном времени. Данные хранятся в оптимизированной файловой системе, обеспечивающей быстрый анализ, извлечение и реконструкцию трафика.

Устройства могут располагаться в любой точке сети: на периметре, в центре, на опорной 10-гигабитной магистрали или в удаленном сегменте. В любом случае они будут предоставлять вам информативные и понятные аналитические данные, позволяющие быстро реагировать на инциденты и проводить расследования в режиме реального времени. Решение может быть установлено в двух конфигурациях:

- **Устройства на 2 Гбит/с:** высокопроизводительная аналитика; отличная масштабируемость; централизованное управление.
- **Устройства на 10 Гбит/с и хранилище SAN:** система корпоративного класса с большим числом интерфейсов, объемным хранилищем и памятью (до 1,5 ПБ на одном датчике).

Новое поколение надежной защиты

Устройства Security Analytics Appliance — единственные полностью интегрированные решения, которые были специально спроектированы для выполнения аналитических задач и обеспечения надежной защиты от угроз. Они позволяют существенно сократить время обработки инцидентов и гарантировать оперативное проведение расследований.

Symantec

Быстрая идентификация угроз

Благодаря сплошной записи и классификации сетевых пакетов компании получают в свое распоряжение всестороннюю информацию о корпоративном сетевом трафике — от ЦОД до удаленных офисов. Это позволяет быстро обнаруживать атаки на ресурсы компании и своевременно предпринимать меры по защите. Возможности устройств Symantec Security Analytics Appliance:

- **Классификация приложений.** Глубокая проверка пакетов (DPI) позволяет классифицировать для последующего анализа более 2800 приложений и несколько тысяч атрибутов метаданных, включая тип контента, имена файлов и многое другое.
- **Анализ угроз в реальном времени.** Тесная интеграция с Symantec Intelligence Services и глобальной сетью Symantec Global Intelligence Network снабжает устройство актуальной аналитической информацией, основанной на совокупном вкладе тысяч клиентов, миллионов пользователей и множества сторонних служб репутации. Symantec передает актуальные данные об угрозах, URL-адресах и репутации файлов непосредственно на устройства Security Analytics Appliance, поэтому вы можете быть уверены, что устройство располагает самой свежей информацией, помогающей отражать атаки на вашу организацию.
- **Выявление аномалий.** С помощью глубокого статистического анализа собранных данных устройство определяет стандартные модели поведения пользователей и использования сети. При обнаружении каких-либо аномалий генерируется предупреждение, после чего администраторы могут провести расследование и узнать, когда возникла аномалия, как часто она происходит и какие сегменты сети затрагивает.
- **Защита от угроз «нулевого дня».** Автоматическая отправка неизвестных файлов в Symantec Malware Analysis или сторонние службы для контролируемого заражения и оценки помогает подтвердить или опровергнуть подозрения о вредоносном характере того или иного действия.

Оперативное реагирование на инциденты и упрощение расследований

Устройства Security Analytics Appliance предоставляют всю информацию, необходимую для понимания контекста событий, связанных с безопасностью. Это позволяет быстро устранять возникающие инциденты и проводить расследование причин их возникновения. Возможность полного ретроспективного анализа и наличие актуальной информации в реальном времени помогает своевременно выявлять угрозы для приложений, файлов и веб-контента:

- **Аналитика на уровнях 2–7 (OSI).** Множество аналитических инструментов для составления полной картины угроз в среде компании: полная реконструкция сеансов, визуализация данных, анализ первопричин, хронологический анализ, реконструкция файлов и объектов, геолокация по IP-адресу, анализ тенденций и выявление аномалий. Например, в процессе анализа первопричин восстанавливается полная хронология подозрительных веб-сеансов, цепочек писем или сообщений в чате, что позволяет доказательно определить источник и масштаб инцидента.
- **Тесная интеграция с инфраструктурой безопасности.** Интеграция с лучшими технологиями безопасности, включая системы SIEM, брандмауэры следующего поколения NGFW, системы предотвращения вторжений IPS, службы контролируемого заражения и расследования, помогает получить максимальную отдачу от уже сделанных инвестиций и повысить эффективность имеющихся процедур и рабочих процессов.
- **Защита с учетом контекста.** Symantec предоставляет полную информацию о контексте, в котором происходят события, поэтому вы всегда сможете понять, что происходило до, во время и после атаки. Из любого предупреждения или журнала можно получить полную информацию о релевантном трафике и сразу же приступить к устранению инцидента или расследованию его причин.

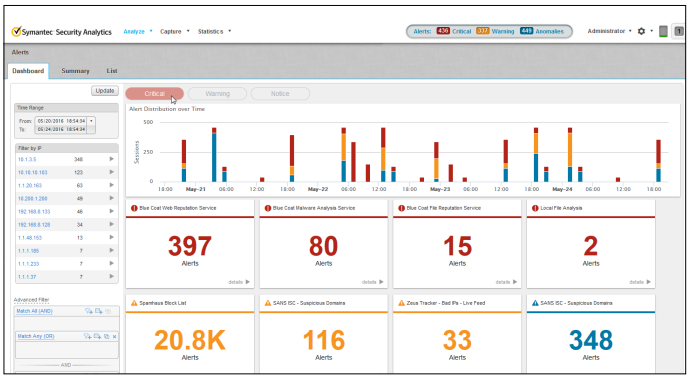
Быстрый ввод в эксплуатацию

Надежные, сертифицированные и тщательно протестированные устройства начинают приносить пользу сразу же после установки. Это интегрированные решения, полностью готовые к использованию:

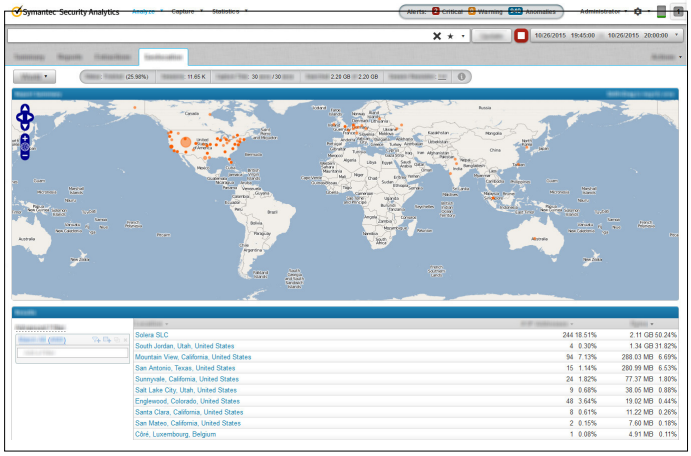
- **Эффективность.** Сбор, индексация и классификация пакетов выполняются без нарушения коммуникаций и не оказывают негативного влияния на производительность. Эти устройства магистрального класса построены на сертифицированной стандартной аппаратной платформе, обеспечивающей высокие показатели доступности и удобства обслуживания.
- **Масштабируемость.** Внушительный объем хранилища позволяет накапливать большой массив исторических данных. Оптимизированное хранилище SAN высокой плотности поддерживает добавление новых дисков и может иметь объем до нескольких петабайт, помогая вам соблюдать постоянно меняющиеся требования и обслуживать быстро растущий объем трафика.
- **Готовность к работе.** Устройства поставляются с заранее установленным и настроенным ПО Security Analytics. Они быстро устанавливаются и сразу же начинают приносить пользу. Компонент Security Analytics Central Manager позволяет централизованно управлять несколькими устройствами Security Analytics из одной панели.

Благодаря интуитивному пользовательскому интерфейсу вы можете быстро получать всю информацию, необходимую для устранения и расследования инцидентов.

Сводная панель помогает быстро проводить анализ



Наглядное представление источников трафика и угроз



Сохранение всех пакетов и дополнение их метаданными

Устройства Symantec Security Analytics Appliance: с напрямую подключенным хранилищем				
	2G Appliance	**10G Appliance**	**Модуль хранения**	**Central Manager**
ИНТЕРФЕЙСЫ	3 x 10/100/1000 BaseT	7 x 10/100/1000 BaseT 2 x 10 GbE	8 SAS (12 Гбит/с)	4 x 10/100/1000 BaseT
УСТАНОВЛЕННЫЕ ДИСКИ	12 ТБ полезный объем (данные + индекс): – 10 ТБ RAID-5 данные (6 x 2 ТБ) – 2 ТБ RAID-1 индекс (2 x 2 ТБ) – 2 ТБ RAID-1 система (2 x 2 ТБ)	42 ТБ полезный объем (данные + индекс): – 34 ТБ RAID-5 данные (17 x 2 ТБ) – 8 ТБ RAID-1 индекс (5 x 2 ТБ) – 3 ТБ RAID-1 система (2 x 2 ТБ)	12 самошифруемых дисков SAS 12 Гбит/с 4 ТБ 3,5”	6 ТБ полезных: – 6 ТБ RAID 5 (4 X 2 ТБ)
МАКС. ПОЛЕЗНЫЙ ОБЪЕМ	1 модуль на 40 ТБ: полезный объем 50 ТБ	До 6 модулей по 44 ТБ: полезный объем 264 ТБ	44 ТБ (44 ТБ полезных / 48 ТБ всего)	----
ПРОЦЕССОР	2 x Intel® Xeon® E5-2620 v3 (15 МБ кэш, 2,40 ГГц, 6 ядер)	2 x Intel® Xeon® E5-2680 v3 (30 МБ кэш, 2,50 ГГц, 12 ядер)	----	2 x Intel® Xeon® E5-2620 v3 (15 МБ кэш, 2,40 ГГц, 6 ядер)
ОЗУ	16 x 8 ГБ RDIMM	16 x 16 ГБ RDIMM	----	8 x 8 ГБ RDIMM
ВЫСОТА	1 модуль	2 модуля	2 модуля	1 модуль
ГЛУБИНА	755 мм	723 мм	507 мм	700 мм
КОНФИГУРАЦИЯ ШАССИ	До 10 жестких дисков	До 26 жестких дисков на 2,5”	Кейс JBOD на 12 дисков	До 4 жестких дисков
ИСТОЧНИКИ ПИТАНИЯ	Два, горячая замена, резервирование (1+1), 750 Вт	Два, горячая замена, резервирование (1+1), 1100 Вт	Два, горячая замена, резервирование, 595 Вт	Два, горячая замена, резервирование (1+1), 750 Вт
КАБЕЛИ ПИТАНИЯ	2 x NEMA 5-15P, вилка C13, 125 В, 15A	2 x NEMA 5-15P, вилка C13, 125 В, 15A	2x SP-305/IS-14, 10 A, 1,82 м, резервирование	2 x NEMA 5-15P, вилка C13, 125 В, 15 A
САЛАЗКИ	Телескопические салазки ReadyRails™ с кабельным органайзером	Телескопические салазки ReadyRails™ с кабельным органайзером	Неподвижные салазки на 2 модуля	Телескопические салазки ReadyRails™ с кабельным органайзером
ВНУТРЕННИЙ КОНТРОЛЛЕР RAID	12 Гбит/с SAS	12 Гбит/с SAS	----	12 Гбит/с SAS
ВНЕШНИЙ КОНТРОЛЛЕР RAID	12 Гбит/с SAS	2 x 12 Гбит/с SAS	----	----
ВСТРОЕННОЕ УПРАВЛЕНИЕ	Полный доступ из удаленной консоли с поддержкой съемных носителей	Полный доступ из удаленной консоли с поддержкой съемных носителей	----	Полный доступ из удаленной консоли с поддержкой съемных носителей
ПОТРЕБЛЯЕМАЯ МОЩНОСТЬ	386 Вт (1317,1 Б.Т.Е./ч)	646 Вт (2204,2 Б.Т.Е./ч)	810 Вт (2763,8 Б.Т.Е./ч)	316 Вт (1078,2 Б.Т.Е./ч)
РАСХОД ВОЗДУХА	13,9 л/с	15,4 л/с	23,3 л/с	11,3 л/с
МАССА	8,4 кг	29,5 кг	24,8 кг	16,9 кг

Устройства Symantec Security Analytics Appliance: с хранилищем SAN высокой плотности		
	10G HD Appliance	**300TB Storage Array**
СЕТЕВЫЕ ИНТЕРФЕЙСЫ	3 x 10/100/1000 BaseT 2 x 10 GbE	н/д
УСТАНОВЛЕННЫЕ ДИСКИ	Восемь (8) самошифруемых на 1 ТБ 7,2K FIPS 140-2 NLSAS 6 Гбит/с 2,5” с горячей заменой. Только для системного раздела.	360 ТБ (60 самошифруемых на 6 ТБ 7,2K FIPS 140-2 NLSAS 3,5” с горячей заменой)
МАКС. ПОЛЕЗНЫЙ ОБЪЕМ	н/д	312 ТБ 2 R5 (4+1) раздела для индексов = 48 ТБ 4 R5 (11+1) раздела для данных = 264 ТБ 2 для в горячем резерве
ПРОЦЕССОР	2 x Intel Xeon E5-2680 v3	н/д
ОЗУ	256 ГБ	н/д
ВЫСОТА	4,27 см	17,78 см
ГЛУБИНА	73,66 см	81,28 см
КОНФИГУРАЦИЯ ШАССИ	1 модуль	4 модуля
ИСТОЧНИКИ ПИТАНИЯ	Два с горячей заменой	Два с горячей заменой
КАБЕЛИ ПИТАНИЯ	2 x NEMA 5-15P, вилка C13, 125 В, 15 А	2 x C20/C19, тип PDU, 250 В, 16 А, 0,6 м
САЛАЗКИ	ReadyRails с кабельным органайзером	Неподвижные салазки
СЕРВЕРНЫЙ КОНТРОЛЛЕР RAID	PERC H730P Integrated RAID Controller	н/д
ВНЕШНИЙ КОНТРОЛЛЕР RAID	н/д	н/д
ИНТЕРФЕЙС СИСТЕМЫ ХРАНЕНИЯ	2 системных адаптера шины Emulex LPe16002B Dual Port 16 Гбит/с Fibre Channel	2 кэширующих контроллера 8 ГБ с поддержкой 16 Гбит/с Fibre Channel
ВСТРОЕННОЕ УПРАВЛЕНИЕ	Удаленное управление iDRAC Enterprise	SANtricity Storage Manager
ТЕПЛООТДАЧА	1563 Б.Т.Е./ч	5159 Б.Т.Е./ч
ВХОДНОЕ НАПРЯЖЕНИЕ	100–240 В~, автоподстройка, 50/60 Гц	200–240 В~, автоподстройка, 50/60 Гц
МАССА	16,92 кг	109,2 кг
РАСХОД ВОЗДУХА	16 л/с	109 л/с
ПОТРЕБЛЯЕМАЯ МОЩНОСТЬ	458 Вт	1512 Вт

О компании Symantec

Symantec Corporation (NASDAQ: SYMC) — лидирующая компания в сфере кибербезопасности. Мы обеспечиваем защиту важных данных как частных пользователей, так и крупных компаний, включая государственные учреждения. Интегрированные решения Symantec используются организациями в разных странах для защиты от комплексных атак на конечные точки, облачные среды и инфраструктуру. Более 50 миллионов индивидуальных пользователей и семей во всем мире доверяют продуктам Norton и LifeLock защиту своих домашних и личных устройств. Под управлением компании Symantec находится одна из крупнейших гражданских сетей анализа киберугроз, что позволят нам распознавать и блокировать самые изощренные угрозы. Дополнительные сведения см. на веб-сайте www.symantec.com или на наших страницах в Facebook, Twitter и LinkedIn.

Штаб-квартира Symantec Corporation

350 Ellis Street

Mountain View, CA 94043 США

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com