webcontrol

ДИСТРИБЬЮТОР
ПЕРЕДОВЫХ РЕШЕНИЙ
ДЛЯ ЗАЩИТЫ
ИТ-СИСТЕМЫ

СПРАВОЧНИК РЕШЕНИЙ
WEB CONTROL

Средства Web-защиты и управление SSL/TLS

- **Symantec (ex Blue Coat) ProxySG апплайнс, virtual Secure Web Gateway виртуальный апплайнс** – прокси-платформа для обеспечения безопасности при взаимодействии с веб-ресурсами в Интернете и применения корпоративных политик доступа (функционал Web Security), для защиты собственных веб-приложений (функционал Web Application Firewall) и оптимизации работы бизнес-приложений (функционал WAN optimization).
- **Symantec (ex Blue Coat) Web Security Service** – облачный веб-шлюз с возможностью интеграции с экосистемой ИТ/ИБ.
- **Symantec (ex Blue Coat) Content Analysis** – многоуровневая фильтрация веб-контента для выявления вредоносного поведения и угроз нулевого дня, используется совместно с Symantec прокси. CAS позволяет подключить несколько антивирусных движков и выполнять безопасную детонацию подозрительных файлов и URL-адресов в on-box или внешних песочницах.
- **Symantec (ex Blue Coat) Advanced Secure Gateway** – апплайнс сочетает возможности ProxySG и Content Analysis, но без возможности активации песочницы on-box и интеграции с SEP'ом.
- **Symantec (ex Blue Coat) Web Application Firewall** – защита ваших веб- сервисов от атак из Интернета по OWASP TOP 10, фильтрация загружаемых файлов и ускорение доставки контента клиентам на базе Symantec ProxySG, virtual SWG или ASG. Symantec WAF позволяет выполнять 14 способами аутентификацию пользователей, выполнять SSL/TLS off-loading, извлекать объекты из SSL/TLS, применять политики и фильтрацию, журналировать доступ, абстрагировать серверы (URL rewrite). Акселерация веб-контента включает в себя ряд технологий, в том числе сжатие, кэширование, оптимизация протоколов и управление полосой.
- **Symantec (ex Blue Coat) SSL Visibility** – специализированное высокопроизводительное устройство для управления SSL/TLS трафиком и с лидирующей в отрасли поддержкой наборов шифров (RSA, DHE, ECDHE, ChaCha, Camilla и т.д.) Извлеченный трафик передается на проверку в существующие системы безопасности (DLP, IPS, NGFW, anti-malware, песочницы и др.)
- **Symantec (ex Fireglass) Web Isolation** – передача визуальной информации вместо исполнения кода для безопасного доступа к опасным веб-сайтам, когда их все-таки требуется просматривать, а не блокировать. Веб-изоляция создается путем передачи визуальной информации на компьютер пользователя, а веб-контент при этом загружается в безопасную среду исполнения устройства Web Isolation.

Защита почты

- **Symantec Email Security.cloud** – облачная защита почтовых сообщений от направленных атак, целевого фишинга и нежелательных рекламных рассылок. Включает в себя технологии предотвращения утечки данных и шифрования электронной почты. Поддерживаются приложения Microsoft Office 365, Google Apps, локально или с хостингом Microsoft Exchange, а также другие почтовые службы.
- **Symantec Messaging Gateway** – виртуальное или аппаратное устройство для защиты электронной почты, сочетает высокоточную защиту от СПАМа и вредоносного кода, расширенные возможности фильтрации содержимого, функции предотвращения утечки данных и шифрования электронной почты.
- **Symantec Mail Security for Microsoft Exchange** – интегрированная защита почты от вредоносных программ, спама и угроз безопасности, а также соблюдение корпоративных политик на серверах Microsoft Exchange.

- **Symantec Gateway Email Encryption** – защита исходящих почтовых сообщений без установки дополнительного ПО на почтовых клиентах. Полная интеграция с существующими стандартными решениями шифрования электронной почты, такими как OpenPGP и S/MIME.

Управление IT-инфраструктурой

- **Symantec IT Management Suite** – пакет включает в себя Client Management Suite и Server Management Suite, а также Asset Management Suite и ServiceDesk. Реализация единой среды управления для распределенных и разнородных сред. Управление изменениями и выполнение рутинных повседневных операций. Автоматизация основных IT-процессов и при этом не нужно добавлять новые инструменты, нанимать новых сотрудников или разрабатывать новые методики.
- **Symantec Client Management Suite** – развертывание, управление, защита и устранение неисправностей в системах, включая настольные компьютеры, ноутбуки и Mac, на всем протяжении их жизненного цикла. Организации могут управлять большим числом технологий с большей эффективностью, на большем количестве платформ, включая Windows, Mac, Linux и виртуальные среды.
- **Symantec Server Management Suite** – управление физическими и виртуальными серверами на различных платформах. Содержит решения для создания ресурсов на серверах, контроля, автоматизации и отслеживания работы серверов с центральной консоли.
- **Symantec Asset Management Suite** – управление лицензиями на ПО, контрактами, ресурсами, предоставляет отчеты и аналитику; позволяет оптимизировать расходы на лицензии. ИТ-подразделения получают четкую картину ресурсов на всех этапах их жизненного цикла.
- **ServiceDesk** – инструмент на основе ITIL и лучших практик для управления инцидентами, проблемами, изменениями и знаниями, включая портал самообслуживания. Помогает соответствовать SLA. Встроенный планировщик бизнес- процессов. ServiceDesk интегрируется с продуктом IT Management Suite, что помогает сократить прерывания работы для обслуживания, ускорить восстановление системы в работоспособное состояние, обеспечить устранение системных проблем и сократить время простоя.
- **Deployment Solution for Clients и Deployment Solution for Servers** – массовое развертывание образа настроенной системы с помощью технологии Symantec Ghost, позволяет настроить каждую систему по стандартным правилам с учетом должности, расположения и типа пользователя. Предоставляет средства для создания заданий и задач, автоматизации развертывания и миграции, в том числе создание образов, установка операционной системы по сценарию, настройка и развертывание программного обеспечения.
- **Symantec Ghost Solution Suite** – позволяет выполнять массовое развертывание образа настроенной системы. Также к ключевым возможностям относятся: интеллектуальные технологии сопоставления драйверов и устройств, удаленное выполнение задач в определенной последовательности, миграция пользователей системы и параметров приложений.

Многофакторная аутентификация

- **Symantec VIP** – единый вход в систему (SSO), надежная многофакторная аутентификация, контроль доступа пользователей к критичным бизнес-системам. Пользователь получает одноразовый пароль с помощью push-уведомлений на своем мобильном устройстве или иными способами (e-mail, sms, voice).

СПРАВОЧНИК РЕШЕНИЙ Web Control

Организация рабочего процесса администраторов, смена паролей и ключей, запись действий и анализ поведения пользователей

- **sPACE** – служит для комплексной организации бизнес-процесса администрирования IT-систем: согласование и предоставление допуска на необходимый период времени с требуемым уровнем привилегий для удаленного подключения к IT-системам, подключение происходит через единую контрольную точку с регистрацией всех действий, защищенная среда администрирования изолирует учетные данные от недоверенной внешней среды и позволяет безопасно проводить работы с любыми IT системами; возможность автоматической смены паролей и ключей, в том числе технологических.

- **Teramind** – предназначен для записи и анализа действий сотрудников. Создает предупреждения о возможных утечках данных и инсайдерских атаках. Встраивается в ИТ ландшафт компании за счет интеграции, в том числе с JIRA, Trello, BaseCamp, Redmine. Развертывается on-premise, на виртуальных машинах, в частных и гибридных облаках и поставляется в трех вариантах:

► Teramind Starter – базовый функционал для стартапов и небольших компаний, которым требуется мониторинг действий сотрудников, запись сеансов пользователей и оптимизация бизнес-процессов.

► Teramind UAM – эффективное обнаружение и предупреждение инсайдерских атак с помощью анализа поведения пользователей и автоматизированного реагирования на основе правил и политик (есть встроенные шаблоны и редактор). Мониторинг действий пользователей. Контроль использования рабочего времени и производительности сотрудников.

► Teramind DLP – все вышеуказанное плюс элементы DLP. Защита всех типов данных и IP, правила на основе контента, контроль операций с файлами, предотвращение вредоносной или небрежной утечки данных, отслеживание документов по их цифровым отпечаткам, соответствие нормативным требованиям PII, PHI / HIPAA, GDPR.

- **BeyondTrust** – единая платформа по контролю и управлению доступом с повышенными привилегиями во всех проявлениях. Состоит из трех основных модулей:

► Endpoint Privilege Management - управление привилегиями на конечных точках в парадигме «гранулированное предоставление минимальных но достаточных привилегий без ущерба для производительности персонала.» Для Windows, Mac, Unix, Linux, сетевых устройств. Возможно бесшовное включение Unix, Linux машин под управление Active Directory без изменения схемы AD.

► Secure Remote Access управляет и контролирует привилегированным удаленным доступом сотрудников и внешних подрядчиков. Служит для организации поддержки корпоративных серверов и рабочих станций безопасно, удаленно, без VPN, в том числе без присутствия человека на обслуживаемом устройстве. Состоит из:

- Privilege Remote Support, для оказания поддержки рабочих станций, вне зависимости от того где находится инженер поддержки и рабочая станция - внутри или вне периметра.
- Privilege Remote Access, для организации контролируемого доступа внешних исполнителей к серверам и прочим основным ИТ ресурсам компании.

► Privileged Password Management (включает Password Safe, Cloud Vault и DevOps Secrets Safe). Позволяет организовать, контролировать и управлять доступом к критическим активам в компании.

Управляет сессиями доступа, журналирует и записывает их, создает алерты по событиям внутри сессий, по которым создает оповещения и блокирует подозрительную активность. Находит, подключает, управляет и проверяет каждую привилегированную учетную запись - как пользовательскую, так и служебную. Противостоит компрометации паролей за счет их ротации по расписанию или факту использования

Запись и анализ сырого трафика

- **Symantec Security Analytics** – для сбора, индексирования, классификации и обогащения всего сетевого трафика (включая полные пакеты) в режиме реального времени. Записанный сырой трафик хранится в оптимизированной файловой системе для быстрого анализа, поиска и полной реконструкции сессий для поддержки действий по реагированию на инциденты.

Symantec. BeyondTrust Flowmon Driving Network Visibility sPace XebiaLabs Now Digital.ai

PROFITAP TERAMIND NETSCOUT WhiteSource

Контроль комплаенса

- **Symantec Control Compliance Siute** – выявление уязвимостей и недочетов в безопасности, автоматизация оценки соответствия различным нормативным требованиям, включая GDPR, HIPAA, NIST, PCI и SWIFT.

Защита серверов, рабочих станций и мобильных устройств от вредоносного кода и направленных атак

- **Symantec Control Compliance Siute** – Symantec Endpoint Protection – многоуровневая защита endpoint'ов от вредоносного кода и атак с применением сигнатурных проверок.
- **Symantec Endpoint Protection Mobile (ex Skycure)** – многоуровневая защита мобильных устройств от целенаправленных атак.
- **Symantec Advanced Threat Protection** – автоматически устанавливает взаимосвязи между событиями, зарегистрированными модулями SEP, ATP:Endpoint, ATP:Network и ATP:Email для выявления и ранжирования угроз, идентификации подозрительных сценариев и эксплойтов; автоматическое создание инцидентов. Используется один агент (SEP) и единая консоль. Функции Endpoint Detection and Response (EDR) реализуются интеграцией решений SEP + ATP:Endpoint + ATP:Network + песочница + SWG + Email Security. cloud + ATP:Email для обнаружения и реагирования на изощренные атаки, которые невозможно выявить даже продвинутым антивирусным решением.
- **Symantec Data Center Security** – специализированная защита для серверов, облачных сред и устаревших платформ от атак, контроль доступа к процессам (PAC), брандмауэр и HIPS/HIDS на уровне хоста, защита системы и файлов от изменений, а также контроль приложений и устройств на основе политик.
- **Symantec Critical System Protection** – специализированная надежная защита для Интернета Вещей (IoT), ограниченных в ресурсах embedded систем и высоконагруженных бизнес- критичных систем.

Защита информации, передаваемая по каналам коммуникаций

- **Symantec CASB** – поиск и аудит использования облачных сервисов, оценка их защищенности, интеграция с выбранными облачными сервисами для детального контроля взаимодействия с ними, обезличивание данных в выбранных облачных сервисах.
- **Symantec DLP** – используются 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.
  - ► DLP for Cloud - для облачных хранилищ и электронной почты, включая MS Office 365 и Box.
  - ► DLP for Endpoint - для физических и виртуальных конечных точек.
  - ► DLP for Mobile - для мобильных пользователей.
  - ► DLP for Network - для корпоративной электронной почты и контроля взаимодействия с Интернет-ресурсами.
  - ► DLP for Storage - помогает получить контроль над всеми неструктурированными данными.

WAN-оптимизация для ускорения работы бизнес-критичных приложений

- **Symantec (ex Blue Coat) PacketShaper** – позволяет автоматически классифицировать и замерять работу сетевых приложений, обеспечивать для них QoS, а также увеличивать пропускные способности WAN при помощи сжатия трафика. Бизнес-критичные приложения должны работать с той же скоростью, с которой происходит деловая активность. PacketShaper предоставляет возможности оптимизации WAN при помощи модулей: мониторинга, распределения трафика по скорости и модуля сжатия.

Мониторинг и диагностика IT инфраструктуры

- **Netscout – семейство сетевых решений:**

► NETSCOUT nGeniusONE – предоставляет в режиме реального времени визуализацию и мониторинг ключевых бизнес-приложений, таких как веб-приложения, базы данных, голосовая и видеосвязь, финансовые и другие приложения, сервисов и сетевой ИТ-инфраструктуры. Платформа nGeniusONE сводит воедино управление производительностью для обеспечения целостного восприятия работоспособности на всех уровнях: приложений, сетей и различных пользовательских устройств.

NETSCOUT nGeniusONE®, используя запатентованную технологию Adaptive Service Intelligence™ (ASI) и глубокий анализ пакетов (DPI), анализирует данные реального сетевого трафика, получаемые из проводных и беспроводных сред, виртуальной инфраструктуры или из облаков, генерирует масштабируемые с высокой степенью точности метаданные, которые позволяют получить полное представление о производительности сервиса, сети и приложения в сложной многоуровневой ИТ-среде.

► NETSCOUT nGeniusPULSE предоставляет визуализацию, необходимую для современной развивающейся ИТ-экосистемы, для обеспечения доступности, надежности и производительности критически важных бизнес-сервисов в мульти-облачной среде, через Ethernet или Wi-Fi, откуда бы ни обращался пользователь. Таким образом nGeniusPULSE обеспечивает мониторинг работоспособности вашей инфраструктуры.

► NETSCOUT TAP — пассивные ответвители для надежной передачи копии трафика. Медные ответвители имеют релейную функцию Fail-Safe, а оптические работают по принципу разделения светового потока с помощью зеркал - что позволяет им работать без питания и без влияния на источник трафика.

► NETSCOUT nGenius Packet Flow Switches – свитчи для управления сетевым трафиком. Фильтрация на уровнях L2-L7, балансировка нагрузки, агрегация трафика, VLAN тегирование, маркировка пакетов.

- **Profitap** – волоконно-оптические и медные сетевые ответвители трафика, регенерирующие, агрегирующие и bypass -тапы (TAP), сетевые пакетные брокеры (NPB), сетевые средства захвата и анализа трафика серий ProfiShark, ProfiSight и IOTA.

► Устройства серии ProfiShark представляют собой специальные портативные сетевые TAP-устройства для диагностики Ethernet и волоконно-оптических линий связи, мониторинга сети, захвата и анализа трафика.

ProfiShark позволяет получить легкий доступ к сети и захватывать каждый пакет с точной отметкой времени. Это обеспечит получение высококачественных данных, которые можно использовать в программном анализаторе пакетов, например, в Wireshark, или сохранять непосредственно на диск для последующего анализа.

► IOTA — это универсальное комплексное решение, объединяющее возможности захвата, хранения и аналитики в одном устройстве. Его можно легко развернуть в любом месте, как в портативном, так и в стоечном исполнении. Линейная схема IOTA изолирована от других интерфейсов, внутреннего хранилища и обработки анализа, обеспечивая целостность контролируемой сети.

► Network Packet Broker (NPB) — это устройство, которое оптимизирует поток трафика между соединениями TAP и SPAN и инструментами мониторинга, безопасности и оптимизации сети. Поддерживая сопоставление портов «многие ко многим» (M: M) сетевых портов с портами мониторинга, NPB могут максимально эффективно направлять сетевой трафик и применять фильтры для оптимизации использования полосы пропускания в сети. Это также означает, что производительность внешних инструментов увеличится, поскольку они получат только самые необходимые данные.

► Оптоволоконные ответвители (TAP), разработанные для обеспечения бесперебойного оперативного мониторинга оптоволоконных сетей 1G, 10G, 40G и 100G, отслеживают все 7 уровней OSI, пакеты всех размеров и типов и ошибки нижнего уровня. Не оказывают негативных воздействий, не имеют IP-адресов и изолируют устройства мониторинга от сети для полной безопасности.

- Медные Ethernet ответвители легко дублируют полнодуплексный трафик 10M / 100M / 1G / 10G на скорости соединения, что позволяет им просматривать все 7 уровней, включая пакеты всех размеров и типов, а также ошибки нижнего уровня.
- TAP регенераторы позволяют использовать для ответвления волоконно-оптическую линию без потери мощности оптического сигнала. TAP регенерации компенсируют потери оптического сигнала, возникающее в результате его расщепления. Регенерируется сигнал как на сетевых, так и на портах мониторинга.
- TAP-репликаторы. В ситуациях, когда вы хотите отслеживать один критический сегмент сети с помощью нескольких инструментов, вам нужен TAP-репликации. TAP репликации отправляет копию сетевого трафика нескольким инструментам мониторинга одновременно.
- Агрегирующие TAP соединяют МНОГО сетевых портов с ОДНИМ портом мониторинга (M: 1), объединяя несколько потоков входящего в один поток исходящего трафика.
- Bypass TAP могут поддерживать активные встроенные средства сетевой безопасности и производительности. Они были разработаны, чтобы избежать проблемы «единой точки отказа» с другими устройствами безопасности.
- Profitap vTAP обеспечит полную видимость трафика виртуальных машин (включая трафик между ВМ) для мониторинга безопасности, доступности и производительности.
- ProfiSight позволяет быстро просматривать данные потока, извлекая метаданные из захваченного потока пакетов с помощью ProfiShark или других источников файлов захвата. Вы можете получить обзор общего состояния в несколько кликов и определить проблемы безопасности или производительности в сети.

Анализ сетевой активности и выявление аномалий

- **Flowmon** – сетевой мониторинг, выявление аномалий и атак, в том числе DDoS, запись трафика и мониторинг производительности приложений. Решение класса Network Behavior Analysis функционирует на основе анализа Netflow/IPFIX с возможностью обогащения данных с помощью зондов данными уровня L7. Визуализация сетевой активности с функциональной (по группам пользователей, типам серверов) и географической разбивкой хостов, с демонстрацией ключевых характеристик приложений и возможностью анализа вплоть до отдельных пользовательских сессий.
- Центр мониторинга (FMC) - это ядро решения Flowmon; профессиональный инструмент для эффективного устранения неполадок в сети, мониторинга производительности и планирования емкости. Вместо просто красного / зеленого состояния инфраструктуры, он помогает администратору понять взаимодействия пользователей, сводя при этом к минимуму количество шума данных и аналитической работы.
- Flowmon Collector - это устройство для мониторинга сети, которое собирает, хранит и обрабатывает flow-данные – сетевую статистику в формате Netflow/IPFIX, включая нормализацию, визуализацию и анализ. Телеметрия сети и приложений отображается на настраиваемой информационной панели, превращая сеть в прозрачную среду, предоставляя параметры статистики, визуализации и детализации для эффективного устранения неполадок и планирования мощностей.
- Flowmon Probe - самый мощный экспортер flow-данных на рынке. Если данные, экспортируемые из активных сетевых устройств, не являются достаточными для мониторинга работы пользователей, поиска неисправностей и обнаружения угроз в сети, зонд (Probe) генерирует данные вплоть до уровня приложений и измеряет их производительность.
- Система обнаружения аномалий Flowmon (ADS) - это решение для информационной безопасности, использующее машинное обучение для обнаружения аномалий, скрытых в сетевом трафике. ADS дополняет обычные средства безопасности и создает многоуровневую систему защиты, способную обнаруживать угрозы на любом этапе компрометации.
- Flowmon Packet Investigator (FPI) - это инструмент автоматизированного аудита сетевого трафика, который записывает и интерпретирует полные пакетные данные. Сочетая в себе автоматическое исследование PCAP и встроенные экспертные знания, он дает администраторам не только понимание возникающих проблем, но и предлагает рекомендации по их устранению, экономя часы или даже дни ручной работы.

- Flowmon Application Performance Monitoring (APM) - это система для измерения пользовательского опыта и производительности критически важных для бизнеса приложений. APM ускоряет процесс устранения неполадок и предоставляет надежные данные об использовании, производительности, частоте возникновения ошибок и SLA, помогая тем самым избежать оттока клиентов и создать условия для продуктивной работы сотрудников.
- Flowmon DDoS Defender Обеспечивает самое современное выявление DDoS, глубокое понимание характеристик атаки и смягчение последствий путем использования полного диапазона методов (RTBH, BGP, PBR и Flowspec). Интеграция через сторонние решения или облачные сервисы (совместимые со стандартом NetFlow) обеспечивает полное смягчение последствий атак.

Решения для DevOps / SecDevOps

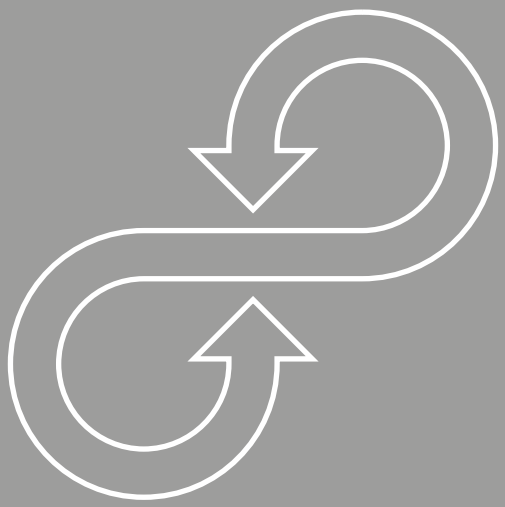
- **Xebia** – XebiaLabs DevOps Platform состоит из 2 основных инструментов – XL Deploy, который автоматизирует развертывание приложений с использованием различных цепочек инструментов и различных сред, и XL Release, который соединяет и осуществляет оркестрацию DevOps инструментов, что дает возможность контролировать и видеть полную картину процесса DevOps компании. Платформа поддерживает интеграцию свыше 250 инструментов. Третий инструмент, XL Impact, предназначен для сбора аналитических данных, рекомендация и генерирования отчетов.

Управление компонентами с открытым кодом при разработке ПО

- **WhiteSource** – современные программные разработки на 60-80% состоят из компонентов с открытым кодом. WhiteSource осуществляет входной контроль качества open source компонентов и разработчики на самой ранней стадии получают информацию для правильного подбора компонентов и повышения качества своего продукта. WhiteSource на протяжении всего жизненного цикла разработки проводит учет, оценку качества и лицензионные соглашения применяемого открытого исходного кода, включая зависимости.

ДИСТРИБЬЮТОР В РОССИИ – КОМПАНИЯ

WEB CONTROL



INFO@WEB-CONTROL.RU
+7 (495) 925-77-94