Решения IBM для обеспечения информационной безопасности

Содержание

Эра нового вредоносного кода

Начиная с 2005 года, технологии интернет-атак значительно менялись. Эти изменения сохраняются и по сей день, и те организации, которые игнорируют новые методы атак, могут однажды понести значимые потери. Сегодняшние атаки нужны хакерам для получения финансовой выгоды, а не для доблести и почета. Они лучше организованы и используют совместный интеллектуальный потенциал для разработки новых стратегий нападения и нового функционала во вредоносных программах, что позволяет им проникать внутрь компаний. С целью получения выгоды или по политическим мотивам атакующие проникают в сети незамеченными, используя самые современные технологии. Традиционные технологии безопасности пасуют перед современными атаками. Ущерб от современной атаки обнаруживается не сразу, поскольку чем дольше атакующий остается незамеченным в сети, тем больше денег он зарабатывает. Современные технологии безопасности должны вскрывать и блокировать все имеющиеся скрытые угрозы и надежно блокировать появление новых их разновидностей.

Организациям необходимо оценить адекватность текущей защиты современным угрозам. Руководителям по информационной безопасности нужно сегодня ответить на вопрос: может ли моя сегодняшняя защита блокировать последние версии вредоносного кода?

ХАРАКТЕРИСТИКА АТАКИ	РАННИЕ АТАКИ	НОВАЯ ЭРА АТАК
Мотивация	Известность и почет	Выгода
Масштаб	Чем больше, тем лучше	Выбор цели, чтобы остаться незамеченным
Основной риск	Падение сети на время лечения	Прямые финансовые потери, кража корпоративных секретов, кража персональных данных и их раскрытие
Эффективная защита	Антивирусные сигнатуры, реактивный подход	Многоэшелонированная защита, превентивный и поведенческий подход
Восстановление	Поиск и удаление	Не всегда возможно, может требоваться восстановление системы
Типы атак	Вирусы, черви, spyware	Направленные вирусы, руткиты, фишинг, требование выкупа
Подход атакующего	Сказать всем, что я здесь	Стелс-технология работы и распространения вредоносного кода, множество разных технологий для атаки

Типы нового вредоносного кода

Designer Malware. Заказное вредоносное ПО – это вредоносный код для заражения одной или нескольких организаций с похожей защитой. Например, это может быть троян, написанный под конкретный банк.

Перед установкой такого вредоносного кода он, как правило, проходит тест на то, что он не будет обнаружен имеющимися в организации средствами защиты. Его код пишется так, чтобы как можно дольше оставаться незамеченным и не привлекать внимания. Его задача – не выходить за пределы организации с тем, чтобы антивирусные компании не получили его код. Известны случаи, когда подобный вредоносный код работал в организациях по году и более, собирая и отсылая своим разработчикам коммерческую и интеллектуальную информацию.

Ransomware. Вредоносный код для вымогательства. Он помещает ваши важные файлы в зашифрованный архив и удаляет оригинальные файлы, а пароль присылает после получения выкупа. Существуют более продвинутые сценарии манипуляций действиями пользователей и вымогательства.

В некоторых случаях традиционные антивирусные системы способны дешифровать ваши файлы, поскольку вирусы используют нестойкие алгоритмы шифрования. Но где гарантия, что вы заразитесь именно той версией вируса, для которой есть распаковщик?

Rootkit. Руткиты имеют способность быть полностью невидимыми средствами операционной системы и антивирусными программами. Функционал руткитов часто совмещают с другими видами вредоносного кода, чтобы они могли оставаться незамеченными долгое время. Поведенческие системы анализа помогают обнаружить такие виды угроз при их получении на системе, но после их установки в системе, как правило, искать их уже поздно. Есть утилиты для поиска руткитов, но лучшим решением является восстановление системы.

Spear Phishing. Направленный фишинг – это комбинация обыкновенного фишинга и социальной инженерии, он направлен против одного человека или целевой группы. Чтобы атака была успешной, она должна быть очень хорошо подготовлена и сфокусирована на конкретном человеке, чтобы не вызвать подозрений. Очень часто такие атаки направлены против финансовых организаций. Атакующий использует найденную персональную информацию о человеке и так подготавливает электронное, а может – и бумажное письмо, чтобы оно выглядело достоверно и заставляло человека среагировать на него и выдать свои приватные данные, такие как логины и пароли. Например, по найденной в журнале информации о назначении Мистера X на новую должность, ему присылается официальное с виду письмо от технической поддержки, которое приводит к тому, что Мистер X, позволяет «службе поддержки» установить у себя троянскую программу или просит завести себе логин и пароль, схожий с логином и паролем в другой системе.

Trojan. Троянские программы – достаточно старый вид угрозы, однако он вернул себе актуальность. Такой вредоносный код использует различные трюки, чтобы пользователь запустил его у себя. Пользователь даже не предполагает, что он запускает вредоносный код, который может выполнять перехват нажатий клавиш или похищает пароли.

Троянские программы, использующие технологии сокрытия, могут не распространяться, а находиться долгое время в системе, выполняя свою задачу по похищению данных.

Троянские программы могут быть обнаружены поведенческими системами анализа. Сигнатурные антивирусы редко знают о них и не обнаруживают их.

Одной из основных угроз при посещении клиентами банков стало наличие в системе троянов, которые похищают как логины и пароли, так и переводят деньги от их имени.

Появление новых угроз в будущем

Угрозы уже не будут простыми. Многие атаки – это комбинации различных методик. Использование только традиционных систем, таких как сигнатурные антивирусы, не дает возможности адекватно защищаться от современных типов атак. Организации, которые защищаются только от известных угроз, всегда рискуют, поскольку атакующие продолжают выдумывать и создавать новые техники атак.

Как защититься от растущих угроз

Из-за современных технологических возможностей и множества путей распространения корпоративные системы должны использовать несколько уровней защиты, чтобы снизить риски многокомпонентных атак. При растущем числе атак, использующих несколько компонентов, всегда существует угроза, что один из этих методов сработает, если вы не подготовились к нему.

У IBM есть чем ответить на новые угрозы. Для предотвращения zero-day-атак IBM использует технологию Virus Prevention System (VPS), которая по поведению обнаруживает вредоносный код. Любой код предварительно выполняется в виртуальном пространстве, где анализируются его действия. Если VPS обнаруживает вредоносное поведение, то такой код не запускается в реальной среде. Контроль вредоносного поведения является необходимым условием при обнаружении последних угроз в сегодняшней практике. Благодаря поведенческой технологии VPS обеспечивает защиту от широкого спектра современных угроз.

ОТЛИЧИЯ МЕЖДУ VPS И СИГНАТУРНЫМ АНТИВИРУСОМ

Защита от новых угроз	Designer Malware	Ransomware	Root Kit
Virus Prevention System (VPS)	Обнаруживает zero-day	Превентивно обнаруживает	Предотвращает установку
Сигнатурный антивирус	Нужен экземпляр кода	Может найти, но уже не может вернуть украденные данные	Не может удалить из ядра

Платформа безопасности на базе решений IBM Internet Security Systems

Защита от IBM обеспечивает полное покрытие защиты компании решениями по защите рабочих станций, серверов и сетей: все централизованно управляется из единой консоли.

Продукты IBM Internet Security Systems работают совместно. Каждый дополнительный компонент добавляет необходимую защиту от имеющихся угроз.

Специалисты

Группа безопасности X-Force компании IBM Internet Security Systems занимается исследованиями в области безопасности, разработкой новых технологий и продуктов, а также оказывает услуги в области безопасности. Специалисты ежегодно проводят мировое турне под названием X-Force Roadshow с целью оповестить специалистов по безопасности о новых угрозах и тенденциях. На территории СНГ в 2009 году X-Force Roadshow проходит в Москве и Санкт-Петербурге 27 и 28 мая соответственно.

Технологии

IBM разработала и продолжает создавать технологии для превентивной защиты от современных угроз. IBM предоставляет клиентам защиту, которая своевременно останавливает атаки, предотвращая возможный ущерб. Следуя развитию технологий виртуализации, IBM создает версии собственных продукты по защите сетей в виде виртуальных версий под VMware.

Защита рабочих станций

Решения по защите рабочих станций **IBM Proventia Desktop** и **IBM Proventia Endpoint Secure Control** используют совместно несколько компонентов защиты, что позволяет построить высокоэффективную систему защиты с единым управлением. Используемая уникальная технология **Virus Prevention System** позволяет своевременно заблокировать на рабочей станции неизвестные виды вредоносного кода.

Защита серверов

Продукты по защите серверов **IBM Proventia Server** и **IBM RealSecure Server Sensor** отличаются поддержкой большого числа операционных систем – Windows, Linux, Solaris, AIX, HP-UX и VMare – и содержат несколько уровней защиты.

Защита электронной почты

Подход IBM к защите электронной почты – комплексность. Продукт **IBM Proventia Network Mail Security** защищает от спама с точностью 98% и также блокирует вирусы, фишинг, атаки на почтовый сервер и контролирует утечки данных. Модули защиты от спама также содержатся в продуктах **IBM Proventia Mail Filter** и **IBM Proventia Multi-Function Security.**

Защита Web-трафика

IBM обладает самой большой в мире базой Web-фильтрации (100 миллионов URL с обновлением 150 тысяч URL в день), что позволяет контролировать посещение пользователями различных категорий сайтов, используя продукт **IBM Proventia WEB Filter** или **IBM Proventia Multi-Function Security** и предотвращая заражение вредоносным кодом и другие угрозы.

Защита сети

Продукты по защите сетей **IBM Proventia Intrusion Prevention System** и **IBM Proventia Multi-Function Security** включают как традиционные средства защиты, такие как firewall, IPSEC и SSL VPN, блокирование вредоносного кода и spyware, так и современную систему предотвращения атак. Также сетевая защита на лету обнаруживает спам и использует Web-фильтр, блокирующий посещение более 60 категорий сайтов. Имеющаяся у IBM система предотвращения атак на базе знаний об уязвимостях с высокой точностью блокирует атаки и вредоносный код. IPS понимает формат передаваемых по сети файлов и знает, куда злоумышленнику нужно поместить злонамеренный код, чтобы сформировать атаку. Не важно, какой именно конкретный злонамеренный код туда положили: он будет в любом случае заблокирован. Встроенный в IPS **Content Engine** контролирует передаваемую информацию, используя регулярные выражения, что предотвращает различные виды утечек информации из корпоративной сети (функционал систем DLP). Также IPS имеет функционал **Web Application Firewall**, защищая от атак на Web-приложения. Технология защиты **Virtual Patch** защищает ресурсы сети, на которых еще не установлены официальные обновления. Proventia IPS работает на скоростях до 40 Гбит в секунду.

Управление уязвимостями

Продукты **IBM Internet Scanner** и **IBM Enterprise Scanner** позволяют реализовать в сети компании полноценный цикл управления уязвимостями, согласно стандарту безопасности ISO 17799, включающий периодическую проверку уязвимостей, назначение ответственных за устранение уязвимости и последующий контроль сделанных исправлений.

Защита на базе услуг

IBM предлагает услуги для повышения защищенности корпоративных сетей: **Managed Security Services** и **Professional Security Services**, что подразумевает и удаленную помощь клиенту в управлении безопасностью (устройствами практически любого производителя), и выезд на место для проведения различных операций от аудита безопасности до разбора инцидентов. IBM – единственная компания на рынке, которая предлагает **гарантированную защиту**, то есть готова заплатить штраф до 50 000 долларов в случае пропуска инцидента безопасности.

Как провайдер услуг IBM постоянно отслеживает новые виды вредоносного кода и вредоносного поведения, что делает IBM готовой к постоянно меняющимся угрозам и обеспечивает гарантию предоставления своевременной защиты своим клиентам и постоянно предоставляет организациям необходимых им специалистов по консалтингу в области информационной безопасности.

Консультанты IBM занимаются только вопросами информационной безопасности, у них есть доступ к исследованиям и разработкам лабораторий IBM X-Force и C-Force и к информации о последних тенденциях в мире безопасности, о которых вы можете также узнать в ежеквартальном отчете аналитиков X-Force или подписаться на ежедневное оповещение о новых угрозах безопасности при помощи сервиса XFTAS (**X-Force Threat Analysis Service**).

IBM Proventia® Network Intrusion Prevention System (IPS)

Система предотвращения атак Proventia Network IPS предназначена для блокирования сетевых атак и аудита работы сети. Благодаря запатентованной технологии анализа протоколов решение IBM Internet Security Systems обеспечивает превентивную защиту – своевременную защиту корпоративной сети от широкого спектра угроз. Превентивность защиты основана на круглосуточном отслеживании угроз в центре обеспечения безопасности GTOC (gtoc.iss.net) и собственных исследованиях и поисках уязвимостей аналитиками и разработчиками группы X-Force (xforce.iss.net).

Выгоды от использования решений Proventia Network IPS

- ✓ Постоянная защита сети и предотвращение самых последних типов и способов атак, включая превентивное блокирование вирусных эпидемий, установку spyware.
- ✓ Автоматическое блокирование DoS-атак (около 200 фильтров).
- ✓ Аудит сетевых соединений. Отчеты и архивы событий дают полную информацию о событиях в сети (например, работа TOR, ICQ, MSN, Skype) и позволяют соответствовать требованиям стандартов безопасности.
- ✓ **Защита от утечек данных из внутренней сети.** Постоянный анализ контента, включая передачу офисных документов по P2P-сетям, службам мгновенных сообщений, Web-почте и другим протоколам.
- ✓ **Virtual Patch.** Автоматическая защита серверов и рабочих станций в случае отсутствия защиты и обновлений безопасности на них.
- ✓ Возможность за один день обучить своих сотрудников управлению устройством.
- ✓ Наличие услуги по установке и настройке устройства.
- ✓ Наличие услуги круглосуточного реагирования на инциденты, обнаруживаемые устройством, профессионально обученными и опытными специалистами.

Основные возможности Proventia Network IPS

- ✓ Блокирует атаки на более чем 7400 уязвимостей: собственная лаборатория X-Force и собранная ей информация об уязвимостях позволяет своевременно заблокировать zero-day-атаки.
- ✓ Блокирование атак на базе знаний об уязвимостях: алгоритмы ISS на лету разбирают форматы файлов и поля сетевых протоколов и понимают, куда злоумышленнику нужно поместить злонамеренный код, чтобы сформировать атаку. Не важно, какой именно конкретный злонамеренный код туда положили: он будет в любом случае заблокирован.
- ✓ Разбирает более 200 различных протоколов, включая протоколы уровня приложений и форматы данных (атаки через VoIP, RPC, HTTP и т.д. или внутри различных типов файлов DOC, XLS, PDF, ANI, JPG и т.д.).
- ✓ Более 2500 алгоритмов используется при анализе трафика для защиты от уязвимостей.
- ✓ Разные политики для разных сегментов сети компании, включая зоны VLAN.

- ✓ Работа в режиме пассивного мониторинга (режим IDS).
- ✓ FlowSmart – технология предварительного разбора пакетов на сетевом интерфейсе.
- ✓ Web Application Firewall, который защищает от SQL injection, LDAP injection, XSS, JSON hijacking, PHP file-includers, CSRF и других атак на Web-приложения.

Модельный ряд Proventia Network IPS

	Удаленные офисы		Периметр сети			Ядро сети	
МОДЕЛЬ	**GX3002**	**GX4002**	**GX4004**	**GX5008**	**GX5108**	**GX5208**	**GX6116**
Пропускная способность	10 Мбит/с	200 Мбит/с	200 Мбит/с	400 Мбит/с	1,2 Гбит/с	2 Гбит/с	15 Гбит/с
Скорость анализа	10 Мбит/с	200 Мбит/с	200 Мбит/с	400 Мбит/с	1,2 Гбит/с	2 Гбит/с	6 Гбит/с
Задержка	<1 мкс	<150 мкс	<150 мкс	<200 мкс	<200 мкс	<200 мкс	Любая*
Защищаемые сегменты	1	1	2	4	4	4	8
Порты (медь/SFP*)**	2/0	2/0	4/0	0/8, 8/0, 4/4	0/8, 8/0, 4/4	0/8, 8/0, 4/4	0/16
Размер корпуса	Desktop	1-RU	1-RU	2-RU	2-RU	2-RU	2-RU
Отказоустойчивость**	Нет	RAID RCF	RAID RCF	RAID RPS RCF	RAID RPS RCF	RAID RPS RCF	RAID RPS RCF
Модуль обхода***	Встроен.	Встроен.	Встроен.	Внешний	Внешний	Внешний	Програм. внешний

* В устройстве GX6116 величину задержки можно задать в параметрах конфигурации.
** RAID (Redundant Array of Inexpensive Disks), RPS (Redundant Power System), RCF (Redundant Cooling Fans).
*** SFP (small form factor pluggable transceiver) – сменные 1Гбит-интерфейсы, также именуемые mini-GBIC, могут быть как медными (TX), так и оптическими (SX/LX).
**** Модуль bypass нужен для непрерывной передачи данных через устройство в случае системной ошибки или отключения энергоснабжения.

Все модели имеют 1Гбит-порты, медные или оптические, кроме GX3002 (медные 100Мбит-порты).

Virtual Proventia Network IPS

Виртуальная версия IPS для защиты виртуальной среды: виртуальных серверов, контроль вредоносного трафика на виртуальных свитчах.

Дополнительные преимущества Proventia Network IPS

Детализированная настройка политик	• Раздельные политики для каждого порта • Раздельные политики по тегу VLAN (виртуальной сети) • Раздельные политики по IP-адресу и диапазону адресов
Реагирование на вторжения	• Блокирование, предупреждение, игнорирование, запись трафика атаки, отправка e-mail, карантин, SNMP • Настраиваемые пользователем действия
Запись трафика атаки	• Запись содержимого пакетов атаки
Собственные сигнатуры	Proventia OpenSignature (на основе правил Snort)
Опция Trust X-Force	Возможность блокирования новых угроз на основании рекомендаций экспертов X-Force
Правила пакетного фильтра	Правила основаны на следующих параметрах: • порт; • IP-адрес; • тип пакета
Карантин	Возможность блокирования подозрительного трафика от определенного компьютера с целью снижения риска заражения других компьютеров
Управление доступом	Играет роль точки управления доступом к сети, обеспечивая защиту взаимодействующих в корпоративной сети компьютерных систем с помощью агента IBM Proventia Desktop

IBM Proventia® Network Security Controller

Защита вашей сети на скорости 10 Гбит/с

- Защита сети на 10Гбит-интерфейсах с использованием Proventia Network IPS GX6116 и GX5208.
- 4 x 10Гбит-порта и 24 x 1Гбит-порта.
- Пропускная способность 20 Гбит/с.
- Поддержка High Availability.
- Модуль обхода гарантирует доступность сети даже при выключении питания.
- Поддерживает 10Гбит-интерфейсы типов SR и LR.
- Несколько техник обнаружения и предотвращения атак на базе глубокого анализа протоколов и знаний об уязвимостях.

IBM RealSecure® Network Sensor

Система обнаружения атак (Intrusion Detection System, IDS)

Этот программный продукт является реализацией сенсора системы обнаружения атак (IDS) и помогает обнаруживать вторжения в сеть и предоставляет средства реагирования, а также обладает непревзойденной производительностью и точностью обнаружения угроз – одной из лучших среди аналогичных программ. Используемый сенсором модуль обнаружения атак Protocol Analysis Module (PAM) аналогичен модулю, используемому в аппаратных устройства Proventia Network IPS. Основным отличием IDS от IPS является установка относительно сети: IDS прослушивает трафик через SPAN-порт, HUB или устройство TAP, а IPS пропускает трафик через себя, что позволяет использовать на IPS правила фильтрации для блокирования атак и изоляции атакующего. RealSecure Network Sensor может переконфигурировать правила межсетевого экрана Checkpoint Firewall-1 используя протокол OPSEC.

Более 2500 алгоритмов обнаружения атак и аудита

Сигнатуры систем обнаружения атак могут базироваться на знаниях об эксплойтах и на знаниях об уязвимостях. Последние используются в модуле PAM, что дает возможность превентивно обнаруживать атаки на уязвимости, не зная конкретного кода эксплойта, а имея лишь информацию об уязвимости. Сенсоры RealSecure Network обладают базой из более чем 2500 сигнатур на базе уязвимостей и на базе информации об иных контролируемых событиях. С помощью имеющегося языка описания атак, схожего с языком для системы Snort, можно создавать свои собственные сигнатуры.

Легкость в управлении

Система управления SiteProtector, бесплатно поставляемая вместе с RealSecure® Network, позволяет без лишних усилий и с минимумом сотрудников управлять сенсорами, установленными в различных сегментах корпоративной сети.

Продукт используется во всем мире

Достоинства сенсоров RealSecure Network были по праву оценены более чем 12 000 компаний в России и во всем мире. Системы RealSecure® Network 10/100 и Gigabit имеют множество наград от различных организаций и журналов, работающих в области информационной безопасности.

IBM Proventia® Server Intrusion Prevention System (IPS)

Агент защиты сервера

Proventia Server IPS обеспечивает информационную защиту для серверов, работающих под управлением операционных систем MS Windows и Linux. В число угроз, от которых защищает Proventia Server IPS, входят различные уже известные и еще не обнаруженные виды атак, а также внутренних злоупотреблений. Система не требует регулярных установок критических исправлений в серверных приложениях. Система осуществляет автоматическую загрузку обновлений систем безопасности для защиты уязвимых мест, пока не будут установлены исправления от разработчиков ПО. Proventia Server комбинирует следующие средства информационной защиты:

- ✓ межсетевой экран;
- ✓ система предотвращения атак;
- ✓ защита от переполнения буфера;
- ✓ система контроля за активностью приложений, обеспечивающая соответствие политик безопасности корпоративным политикам.

Решение предусматривает простую процедуру установки, конфигурирования и управления.

IBM RealSecure® Server Sensor

Агент защиты сервера

RealSecure Server Sensor, комбинируя проверенную временем систему IPS с механизмом аудита и анализа ОС, серверных приложений и сетевой активности, защищает серверные ресурсы от различного рода злоупотреблений и вторжений, практически не влияя на производительность системы. Пользователь данного продукта получает гибкое решение, которое предоставляет широкие возможности по конфигурированию и исследует деятельность сервера на предмет соответствия заданным политикам безопасности. Продукт использует встроенные сигнатуры, усовершенствованный анализ протоколов, наборы поведенческих моделей и автоматическую корреляцию событий для предотвращения известных и неизвестных методов атак.

RealSecure Server Sensor комбинирует следующие средства информационной защиты:

- ✓ межсетевой экран;
- ✓ система предотвращения атак;
- ✓ защита от переполнения буфера;
- ✓ система контроля за активностью приложений;
- ✓ система аудита системных событий и журналов.

RealSecure Server Sensor осуществляет защиту серверов, работающих под управлением операционных систем MS Windows, Solaris, AIX, HP-UX.

Общие достоинства продуктов Proventia Server IPS и RealSecure Server Sensor

- ✓ **Система предотвращения атак (Host IPS).** Используемый модуль IPS – Protocol Analysis Module (PAM) – сочетает в себе традиционный сигнатурный метод обнаружения атак, поведенческий метод анализа и множество других техник обнаружения вторжений. PAM распознает более 167 видов протоколов и форматов данных, в базе знаний X-Force содержится более 2500 сигнатур различных видов атак.
- ✓ **Технология Virtual Patch™.** С помощью технологии Virtual Patch автоматически обновляются и применяются политики безопасности, устраняющие возможность злоумышленного использования только что появившихся уязвимостей. Технология Virtual Patch позволяет обеспечить защиту от новых

уязвимостей с момента их обнаружения до установки официального исправления ПО.

- ✓ **Межсетевой экран.** Благодаря используемому межсетевому экрану фильтруется входящий и исходящий трафик и блокируется неавторизованный доступ к портам, IP-адресам или сервисам.
- ✓ **Система защиты от переполнения буфера (Buffer Overflow Exploit Prevention – BOEP).** BOEP предотвращает угрозы выполнения вредоносного кода, использующего атаки типа «переполнение буфера». Бессигнатурная технология BOEP позволяет защититься от подавляющего большинства известных атак и делает невозможными дальнейшие попытки использовать такого рода уязвимости (только для Windows).
- ✓ **Анализ SSL-трафика.** Защита Web-приложений, запущенных на Apache или IIS Web-серверах, обеспечивается посредством анализа SSL–трафика (Secure Sockets Layer) на предмет злоумышленной активности.
- ✓ **Аудит системных событий и журналов:**
  - мониторинг пользовательской активности (отказ в процедуре идентификации пользователя, вход в систему с административными привилегиями, использование недействительных учетных записей и т.д.);
  - мониторинг изменений свойств пользователей, групп пользователей;
  - контроль над файлами (целостность файлов, неудачные попытки открытия или изменения файлов и т.д.);
  - контроль над действиями с учетными записями;
  - контроль за наделением прав и очисткой системных журналов;
  - мониторинг сервисов.
- ✓ **Контроль соблюдения заданной политики безопасности.** Любые попытки внести изменения в политики безопасности блокируются.
- ✓ **Антивирусная осведомленность.** Контролируется наличие на сервере антивирусного средства (Symantec, McAfee) и своевременное обновление его антивирусной базы.
- ✓ **Контроль запуска сервисов и приложений.** Только авторизованные сервисы и приложения могут быть запущены на защищаемом сервере. Благодаря этому функционалу предотвращается установка неавторизованных программ.
- ✓ **Локальный интерфейс управления.** Управление может осуществляться как централизованно, так и локально. Кроме того, можно установить совместное управление.
- ✓ **Контроль над доступом к сети.** Только авторизованные сервисы и приложения могут обращаться к сети.
- ✓ **Собственная защита.** Агент защищен паролем и не может быть остановлен, отключен или реконфигурирован пользователями с административными правами. Доступ к сетевым ресурсам может быть запрещен, когда агент не запущен на сервере.
- ✓ **Унифицированная система централизованного управления.** Посредством централизованной системы управления SiteProtector, поддерживающей Active Directory, выполняется простой процесс управления, мониторинга, анализа событий от агентов RealSecure Server Sensor и Proventia Server IPS с одной консоли.

Поддерживаемые операционные системы

Proventia® Server: Windows Server 2003 SP1, Windows 2000 Server SP4, Windows 2000 Advanced Server SP4, Microsoft ISA Server 2000, SUSE Linux Enterprise Server (SLES) 10, Red Hat Enterprise Linux (RHEL) 5.0, VMware ESX 3.5.x.

RealSecure® Server Sensor: Microsoft Windows Server 2003 SP1, Microsoft Windows 2000 Server, Microsoft Windows NT 4.0, VMware GSX 3.1, ESX 2.5.1, Sun Solaris 8, 9, HP UX 11.0, 11i (11.11), IBM AIX 4.3.3, 5.1, 5.2, 5.3.

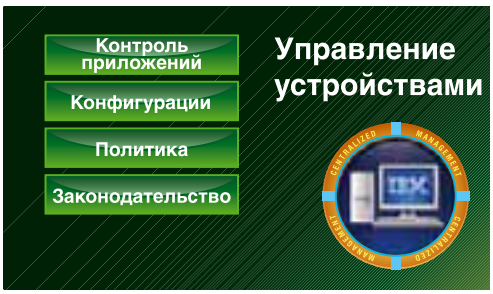
IBM Proventia Endpoint Secure Control (ESC)

Защита от всех типов угроз приводит к большой нагрузке на рабочие станции и к большому числу систем управления. IBM понимает, с какими трудностями сопряжено обеспечение соблюдения нормативных требований и противодействие интернет-угрозам, особенно – в условиях ограниченного бюджета и нехватки ИТ-персонала. Поэтому компания IBM представила решение Proventia ESC, чтобы помочь заказчикам получить максимальную отдачу от ИТ-инфраструктуры и в то же время оградить ее от новых угроз. IBM предлагает использовать новую философию управления рабочими станциями: единую систему управления агентами различных производителей. Используя продукт ESC на базе технологий BigFix, вы имеете единое ядро, легко добавляя или меняя различные компоненты, необходимые как администраторам безопасности, так и отделу ИТ. При использовании ESC в некоторых случаях нагрузка на администрирование снижается на 50%. Система способна управлять одновременно до 250 000 рабочих станций. IBM Proventia ESC является источником важнейших данных аудита безопасности для приложения IBM Tivoli Security Information and Event Manager (TSIEM), что еще больше расширяет возможности TSIEM в области формирования отчетов о соблюдении требований в масштабах предприятия.

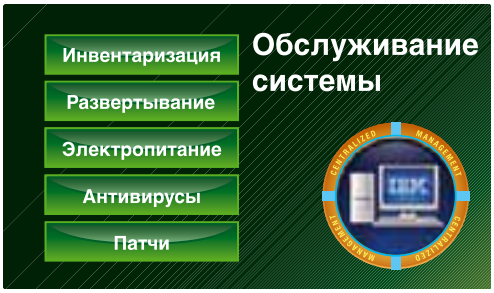
Используя Proventia Endpoint Secure Control, вы будете иметь возможность централизованно управлять такими компонентами,

- превентивная защита на базе исследований и разработок X-Force®;
- персональный firewall;
- система предотвращения атак на базе знаний об уязвимостях;
- сигнатурный антивирус;
- поведенческий антивирус;
- защита от атак с переполнением буфера.

- управление доступом к сети;
- защита от утечек информации;
- шифрование данных;
- анализ контента на наличие конфиденциальных данных.



- превентивная защита на базе исследований и разработок X-Force®;
- персональный firewall;
- система предотвращения атак на базе знаний об уязвимостях;
- сигнатурный антивирус;
- поведенческий антивирус;
- защита от атак с переполнением буфера.



- инвентаризация;
- установка и удаление ПО;
- управление питанием;
- управление антивирусным ПО;
- установка обновлений и патчей в реальном времени (с 90% уровнем с первого раза).

Сравнение функционала продуктов защиты рабочих станций Proventia Desktop и Proventia ESC

Функционал	Proventia	ESC
Firewall	✓	✓
IPS	✓	✓
Поведенческий антивирус	✓	✓
Сигнатурный антивирус	✓	✓
Anti-spyware	✓	✓
Расширенные возможности	-	✓
NAC	-	✓
DLP	-	✓
Контроль портов USB	-	✓
Управление патчами	-	✓
Инвентаризация ресурсов	-	✓
Управление уязвимостями	-	✓
Управление питанием	-	✓
Управление конфигурацией	-	✓
Управление системой	-	✓
Установка/удаление программ	-	✓
Контроль соответствия политике	-	✓

IBM Proventia® Desktop Endpoint Security

Агент защиты рабочей станции

Программный продукт обеспечивает превентивную защиту рабочих станций и мобильных компьютеров от угроз любых видов, не нанося ущерба производительности систем. Простота управления применяемыми технологиями встроенной защиты позволяет держать под контролем клиентские системы, минимизировать влияние на эффективность работы и повышать безопасность клиентов. Управление защитой рабочих станций осуществляется централизованно через SiteProtector.

Proventia Desktop предлагает высокоэффективную многоуровневую защиту, объединяя передовые технологии информационной безопасности.

- ✓ **Персональный межсетевой экран** блокирует доступ к различным сетевым сервисам и службам настольных компьютерных систем. Защитный механизм персонального межсетевого экрана также предотвращает атаки, нацеленные на протоколы и службы и применяемые злоумышленниками в корыстных целях.
- ✓ **Система предотвращения атак (Host Intrusion Prevention System – HIPS)** обеспечивает превентивную защиту путем глубокого анализа пакетов широкого спектра протоколов. Кроме выявления известных сигнатур атак применяется поведенческий и эвристический анализ. Помимо этого, IPS предотвращает проникновение как известных, так и неизвестных эксплойтов, злонамеренно использующих известные уязвимости.
- ✓ **Система контроля действий программных приложений** отслеживает и пресекает подозрительные операции системных приложений и пользовательских программ, в том числе связанные с обращением к внешним сетевым ресурсам.
- ✓ **Система предотвращения вирусных атак (Virus Prevention System – VPS).** Анализируя деятельность исполняемых файлов в изолированной виртуальной среде, система позволяет обнаруживать более 90% вирусов и множество других новых враждебных программ различных видов.
- ✓ **Система защиты от переполнения буфера (Buffer Overflow Exploit Prevention – BOEP).** Уязвимости переполнения буфера превалируют на сегодняшний день. Бессигнатурная технология BOEP позволяет защититься от подавляющего большинства известных атак и исключает возможность дальнейших попыток использовать уязвимости такого рода.
- ✓ **Сигнатурный антивирус** на базе антивирусного ядра компании BitDefender позволяет защищаться от известных модификаций вирусов и spyware. Proventia Desktop может поставляться с сигнатурным антивирусом и без него, если в компании уже используется какой-то сигнатурный антивирус.

IBM Proventia® Network Mail Security System

Комплексная защита корпоративной электронной почты

Модель MS3004

MS1002-VM – программная версия (virtual appliance)

Программно-аппаратный продукт IBM Proventia Network Mail Security осуществляет полную защиту электронной почты предприятия, как входящей, так и исходящей. В этом устройстве работают самые передовые антиспам-решения. Несколько компонентов антиспама разработаны командой IBM Internet Security Systems C-Force, которая специализируется только на защите от спама. Устройство легко интегрируется с различными почтовыми системами, с LDAP. Управляется через HTTPS или через систему управления SiteProtector. Интегрируется с любым e-mail-сервером с помощью протокола SMTP. Продукт имеет программную реализацию в виде виртуальной версии под VMware (так называемый virtual appliance).

Компоненты Proventia Network Mail Security

- ✓Модули многоуровневой защиты от спама (10 различных модулей анализа).
- ✓Модуль строгой фильтрации контента и карантина, который точно задает, кто, когда, что и кому может послать. Можно сказать, что он является почтовым брандмауэром (Mail Firewall).
- ✓Антивирус сигнатурный (Sophos) отлавливает все известные виды вирусов.
- ✓Антивирус на базе анализа поведения неизвестного кода в виртуальной среде Virus Prevention System (VPS) отлавливает неизвестные вирусы по поведению. По сути, этот механизм является единственным способом защиты от троянов, направленных на конкретную компанию, поскольку сигнатурные антивирусы такие атаки отлавливать не умеют. И наконец, это защита от новых вирусов, сигнатуры для которых еще не выпущены.
- ✓Система блокирования вредоносного кода внутри прикрепленных неисполняемых файлов (ShellCode Heuristics) обнаруживает вирусы в DOC, XLS, PPT, JPG, ANI и других файлах, в которых, казалось бы, вирусов не может быть.
- ✓Модуль предотвращения атак (IPS) выявляет сетевые атаки внутри протокола SMTP. В том числе работает модуль Virtual Patch™, который защищает системы от уязвимостей, которые еще не были пропатчены производителями ОС.
- ✓Модуль фильтрации контента по ключевым словам и по базе фишинговых и других злонамеренных сайтов (у IBM ISS база из 100 миллионов URL). На момент «по умолчанию» заложены английские и немецкие ключевые слова, можно добавлять свои, в том числе и русские.
- ✓Модуль отчетов для SiteProtector.
- ✓Модуль интеграции с SiteProtector.
- ✓Модуль протоколирования почтовых сообщений.

От каких угроз защищает Proventia Network Mail Security

- ✓ Спам;
- ✓ вирусы, spyware и другой злонамеренный код во вложениях;
- ✓ атаки на SMTP, в том числе атаки типа zero-day и DoS;
- ✓ утечка конфиденциальной информации;
- ✓ нарушения корпоративной политики безопасности;
- ✓ фишинг и фарминг;
- ✓ порча репутации.

Модули анализа спама Proventia Network Mail Security

- ✓ **Spam Fingerprint.** Каждое письмо получает уникальную 128-битную сигнатуру. Эта сигнатура сравнивается с существующими сигнатурами в базе данных фильтра, что позволяет точно контролировать существующий спам.
- ✓ **Spam Signature Database.** Уникальная 128-битная сигнатура высчитывается также для некоторых частей письма (например, одного абзаца). Эти сигнатуры сравниваются с уже существующими в базе, чтобы обнаруживать спам, несмотря на некоторые изменения всего сообщения.
- ✓ **Spam Structure Check.** Проверяет структуру HTML, давая возможность этому модулю классифицировать письма как спам на основе структуры письма.
- ✓ **Spam URL Check.** Более 80% всех рассылок спама содержат ссылки. Кроме сигнатур писем со спамом в базе данных хранятся и все URL, которые появляются в спамерских письмах. Одно вхождение URL из базы позволяет классифицировать письмо как спам.
- ✓ **Spam Heuristics.** Этот классификатор основывается на эвристическом анализе типичных признаков спам-письма, например некоторых полей в заголовке письма. Используется собственная система оценки для каждого признака, дающего либо положительное, либо отрицательное приращение, в зависимости от того, используется эвристика для поиска спама или хама. Если высчитанный коэффициент превышает заранее установленный уровень, то письмо классифицируется как спам.
- ✓ **Spam RBL check.** IP-адрес хоста, пославшего SMTP-сообщение, проверяется на одном или нескольких RBL-серверах.
- ✓ **Spam Bayesian Classifier.** Статистическая оценка, которая определяет, является ли письмо нужным или спамом по некоторым определенным частотным характеристикам. Этот модуль анализа очень точен при обнаружении нового типа спама.
- ✓ **Spam Flow Check.** Анализирует поток писем в течение заданного промежутка времени. Если одно и то же письмо (считается относительно числа одинаковых характеристик) получено более некоторого заданного заранее уровня раз в течение данного промежутка времени и имеет различные домены отправителя, то письмо классифицируется как спам.
- ✓ **Spam Keyword.** Этот классификатор использует стандартные ключевые слова и регулярные выражения, которые обычно находят в спаме. Группа C-Force собирает соответствующие ключевые слова и шаблоны из уже известных спам-писем и оценивает их индивидуально для дополнительной защиты от спама.
- ✓ **Phishing Check.** Представляет из себя целый набор методов, скомбинированных для обеспечения эффективной защиты против фишинговых писем, включая проверки URL и эвристику.
- ✓ **Dynamic Host Reputation.** Использование базы dnsbl.cobion.com и создание собственного динамического списка IP-адресов спамеров.
- ✓ **SMTP Banner Delay.** Пауза выдачи приветствия при превышении допустимого порога писем.

Автоматические обновления, имеющиеся в Proventia Network Mail Security, обеспечивают более эффективную защиту от спама, вирусов и другого вредоносного кода.

IBM Proventia® Network Enterprise Scanner (ES)

Программно-аппаратный сканер безопасности

Enterprise Scanner – программно-аппаратная реализация сканера безопасности. Enterprise Scanner позволяет осуществлять обнаружение и анализ уязвимостей, инвентаризацию ресурсов корпоративной сети с высокой скоростью и без снижения производительности сети. Вчерашние системы оценки уязвимостей уступают место современным системам управления уязвимостями. Следуя требованиям стандартов безопасности, необходимо находить уязвимости в компьютерных сетях до того, как их найдут хакеры. А они ищут уязвимости в сетях каждый день, поэтому в любой компании есть потребность для ежедневного автоматического контроля за безопасностью.

Модель ES1500

Модель ES750

Выгоды от использования Enterprise Scanner

- ✓ Своевременная информация о состоянии безопасности сети.
- ✓ Автоматическое назначение приоритетов и планирование работ по устранению уязвимостей.
- ✓ Повышение доступности важных для бизнеса служб.
- ✓ Снижение риска простоев в работе сети.
- ✓ Оптимизация защиты корпоративных ресурсов за счет обнаружения потенциальных угроз безопасности.
- ✓ Создание отчетов о результатах сканирования и проведенных работах по устранению уязвимостей.

Что представляет собой процесс управления уязвимостями и их защитой?

Управление уязвимостями и их защитой – это непрерывный процесс защиты важнейших данных компании, наиболее ценных сетевых ресурсов и интеллектуальной собственности. В рамках этого процесса происходит выявление уязвимостей, выполнение действий по их устранению и блокировке, а также осуществляется мониторинг уровня рисков.

Enterprise Scanner является уникальным продуктом на рынке средств обеспечения безопасности, позволяющим осуществлять обнаружение, мониторинг, блокировку, исправление, проверку и создание соответствующих отчетов. При этом исключаются многие выполняемые вручную операции, связанные с управлением уязвимостями.

Преимущества Enterprise Scanner

- ✓ Поставка в виде готового к работе устройства, работающего под управлением ОС семейства Linux.
- ✓ ***Распределение нагрузки*** по сканированию на множестве устройств Proventia® Network Enterprise Scanner.
- ✓ Понимает разные ***проекции уязвимостей:*** сканирование несколькими сканерами снаружи и изнутри сети и приоритезация уязвимостей, найденных из разных точек сети.
- ✓ Сканирование в фоновом режиме в заданных ***окнах сканирования.***

Подразделение IBM Internet Security Systems уже более десяти лет поставляет предприятиям и аудиторским организациям средства для обнаружения уязвимостей. С каждым годом появляются все новые возможности. Следующим шагом развития Enterprise Scanner является интеграция с функционалом сканера приложений компании Watchfire, который вошел в состав продуктов IBM и теперь продается отдельно под названием IBM Rational AppScan.

Основные возможности Enterprise Scanner

Инвентаризация ресурсов

- ✓ Идентифицируются более 1800 типов ресурсов, включая рабочие станции, серверы, маршрутизаторы, коммутаторы, приложения и операционные системы.
- ✓ Предусмотрено обнаружение новых подключенных устройств.
- ✓ Процесс обнаружения новых ресурсов проходит с использованием различных методов и источников: процесс активного сканирования, Active Directory, Proventia Network ADS, импортирование базы данных ресурсов, внесение в базу данных ресурсов вручную.
- ✓ Используются различные техники идентификации: Ping sweep, UDP probe, asset fingerprinting, rapid discovery, NetBIOS-based discovery, TCP discovery, UDP port discovery, OS fingerprinting, Integrated NMAP 4.0 database.
- ✓ Ресурсы группируются по иерархическому принципу на основе организационной структуры (AD).

Оценка защищенности

- ✓ Оценка защищенности обнаруженных ресурсов.
- ✓ Оценка защищенности с использованием различных проверок:
  - подключение новых проверок «на лету»;
  - обновление проверок на основе выхода обновлений технологии Virtual Patch;
  - небольшой объем обновлений (XPU) < 5 Мб.
- ✓ Эмуляция атак:
  - тесты без какого-либо воздействия на сетевую инфраструктуру;
  - анализ возможного эффекта воздействия реальной атаки;
  - непревзойденная по полноте база данных уязвимостей и программных ошибок, подготовленная X-Force®.
- ✓ Сканирование по приоритету критичности ресурсов.

Анализ результатов сканирования

- ✓ Группирование уязвимостей по приоритету.
- ✓ Собственная система реакции на инциденты.
- ✓ Интеграция с системой реакции на инциденты Remedy HelpDesk.
- ✓ Открытый программный интерфейс (API) для подключения других систем реакции на инциденты.
- ✓ Распределение уязвимостей по категориям и ресурсам.
- ✓ Традиционные рекомендации по устранению уязвимостей (рекомендация определенного патча).
- ✓ Интеграция с технологией Virtual Patch™ и системами Proventia IPS.

Генерация отчетов

- ✓ Генерация отчетов согласно организационной структуре организации.
- ✓ Группирование ресурсов в отчетах по уровню рисков, по географическому, территориальному, сетевому и другим признакам.
- ✓ Более 1800 видов отчетов.
- ✓ Представление в виде PDF, CSV, HTML.

IBM Internet Scanner® Software

Программный сканер безопасности Internet Scanner обеспечивает автоматизированное обнаружение и анализ уязвимостей в корпоративной сети. Internet Scanner реализует ряд проверок, идентифицирующих уязвимости сетевых сервисов, операционных систем, маршрутизаторов, почтовых и Web-серверов, межсетевых экранов и прикладного программного обеспечения, которые могут быть использованы злоумышленником для несанкционированного доступа к информационным ресурсам.

Internet Scanner обнаруживает и идентифицирует более 1450 уязвимостей различного программного обеспечения, предотвращающих срабатывание существующих защитных механизмов каким-либо способом. К таким уязвимостям могут быть отнесены: некорректная конфигурация сетевого оборудования, устаревшее программное обеспечение, неиспользуемые сетевые сервисы, слабые пароли и т.д. Internet Scanner осуществляет более 1000 различных проверок, в их числе:

- ✓ проверки FTP, LDAP и SNMP;
- ✓ проверки электронной почты;
- ✓ проверки RPC, NFS, NIS и DNS;
- ✓ проверки возможности осуществления атак типа «отказ в обслуживании»;
- ✓ проверки на наличие атак типа «подбор пароля» (Brute Force);
- ✓ проверки Web-серверов и CGI-скриптов, Web-браузеров и X-терминалов;
- ✓ проверки межсетевых экранов и proxy-серверов;
- ✓ проверки сервисов удаленного доступа;
- ✓ проверки файловой системы ОС Windows;
- ✓ проверки подсистемы безопасности и подсистемы аудита ОС Windows;
- ✓ проверки системного реестра ОС Windows;
- ✓ проверки установленных обновлений ОС Windows;
- ✓ проверки наличия модемов в сети;
- ✓ проверки присутствия «троянских коней»;
- ✓ проверки сервисов и демонов;
- ✓ проверки учетных записей.

Internet Scanner позволяет анализировать состояние защищенности выделенных участков сети в заданные интервалы времени и, следовательно, наблюдать за изменением уровня защищенности корпоративной сети после реализации соответствующих защитных мер.

Internet Scanner позволяет анализировать наличие какой-то одной уязвимости на заданном участке сети, например проверку установки конкретного обновления операционной системы.

Узнайте, может ли ваша компания получить 30-дневную пробную версию, обратившись в российский офис IBM. Для демонстрации системы на месте также обратитесь в IBM Internet Security Systems. Чтобы получить дополнительную информацию, посетите сайт: http://www.ibm.com/ru/services/iss/iss.html.

IBM Proventia® Network Multi-Function Security (MFS)

Многофункциональные устройства «все-в-одном» линейки Proventia Network Multi-Function Security объединяют в себе такие средства информационной защиты, как:

- ✓ полноценный межсетевой экран со statefull inspection;
- ✓ система предотвращения атак;
- ✓ поведенческий антивирус;
- ✓ сигнатурный антивирус;
- ✓ шлюз VPN;
- ✓ фильтрация доступа Web к Web-сайтам и их контенту;
- ✓ антиспам, проверка фишинговых ссылок в e-mail, проверка вложенных файлов.

Все эти системы работают в режиме реального времени и не требуют вмешательства администратора безопасности. Все технологии безопасности сосредоточены внутри устройства и управляются одним механизмом, что происходит одновременно с анализом данных мониторинга. Таким образом обеспечивается высокая производительность, в то время как ущерба работоспособности системы не наносится и снижается временная задержка, которую система безопасности привносит в работу сети.

Устройства Proventia Network MFS предназначены для обеспечения информационной безопасности удаленных филиалов, отдельных офисов, небольших компаний, которым требуется надежный автоматизированный инструмент защиты. Устройства могут работать либо как маршрутизаторы с поддержкой статической и динамической маршрутизации, либо в режиме фильтрующего моста (как коммутатор), что позволяет добавлять защитное устройство в сеть без переконфигурации существующей сети.

Основные достоинства

- ✓ Поставка в виде полностью настроенного и готового к работе устройства.
- ✓ Существенное снижение времени, затрачиваемого на установку, настройку и развертывание системы.
- ✓ Простота внедрения в корпоративную сеть.
- ✓ Балансировка двух каналов на двух разных провайдеров.
- ✓ Идеальное сочетание технологий информационной безопасности в одном устройстве (межсетевого экрана, антивируса, VPN, антиспама, контроля действий сотрудников в Интернете, предотвращения атак, в том числе с применением технологии Virtual Patch™).
- ✓ Protocol Analysis Module (PAM), комбинирующий интеллектуальную мощь исследовательской лаборатории ISS X-Force с различными алгоритмами распознавания враждебного кода на всех уровнях модели OSI. В частности, механизм сигнатурного анализа имеет в своей базе более 2500 сигнатур атак.
- ✓ Межсетевой экран сертифицирован Международной ассоциацией компьютерной безопасности (ICSA).

- ✓ Прозрачный режим работы. При работе в этом режиме нет необходимости вносить изменения в топологию сети, таблицы маршрутизации, конфигурации межсетевых экранов.
- ✓ Глубокий анализ более 200 видов сетевых протоколов и форматов данных.
- ✓ Возможность блокирования Skype, ICQ, P2P и других типов трафика.
- ✓ Возможность перенаправления трафика протокола ICMP.
- ✓ Поддержка протоколов OSPF, STP, PPPoE, DHCP.
- ✓ Антивирусный модуль на основе технологии компании Sophos, позволяющий обнаруживать более 90 000 различных вирусов в протоколах HTTP, FTP, SMTP, POP3.
- ✓ Блокирование установки spyware на рабочих станциях пользователей: на сетевом уровне блокируется вредоносный код, что не дает ему возможности установиться у пользователя.
- ✓ Блокирование соединений spyware. Если у пользователей устанавливается spyware, то оповещается администратор и блокируются соединения, им инициированные.
- ✓ Применение технологии анализа вирусов по поведению обнаруживает и блокирует новые и неизвестные вирусы, шпионское ПО и сетевые «черви» без использования периодически обновляемой антивирусной базы.
- ✓ Более 100 миллионов URL (болеле 9 миллиардов Web-страниц) в базе фильтрации Web-трафика, разбитых на 68 тематических категории, включая категорию сайтов, распространяющих вредоносный код. Обновление базы около 150 тысяч URL в день.
- ✓ База антиспамового механизма, актуального для протоколов SMTP и POP3, содержит более 200 тысяч спамовых шаблонов, трех миллионов сигнатур спам-писем, 80 типов файлов, а также тексты и изображения.
- ✓ Высокая надежность, обеспеченная резервированием устройств питания и хранения информации.
- ✓ Высокая отказоустойчивость, гарантированная благодаря формированию кластера высокой доступности в режиме Active/Passive из двух устройств.
- ✓ Управление через Web-интерфейс и посредством IBM SiteProtector.
- ✓ Дистанционные автоматические обновления баз через службу X-Press Update™ системы управления SiteProtector лаборатории X-Force.
- ✓ Уменьшенная совокупная стоимость владения системой обеспечения информационной безопасности.

МОДЕЛЬ	MX0804W	MX1004W	MX3006W	MX4006W	MX5008W	MX5110W
Интерфейсы Ethernet	4 x 100 Мбит/с	4 x 100 Мбит/с	6 x 100 Мбит/с	6 x 1 Гбит/с	8 x 1 Гбит/с	10 x 1 Гбит/с
Размер устройства	Desktop	Desktop	1-RU	1-RU	2-RU	2-RU
Максимально пользователей	50	100	500	1000	2000	3000
Скорость Firewall+ IPS + Web-filter, Мбит/с	100	100	200	450	730	800
Максимально соединений/с	2000	3000	4100	6800	9580	12 500

IBM Proventia® WEB Filter

Программный продукт Proventia Web Filter служит для фильтрации нежелательного Web-контента и реализует определенную политику использования Интернета в организации, направленную на обнаружение следующих вредоносных факторов:

- ✓ утечки конфиденциальной информации;
- ✓ поступление в сеть организации информации, не относящейся к роду ее деятельности;
- ✓ Web-страниц, доступ к которым запрещен корпоративной политикой.

Proventia Web Filter использует базу данных, в которой более 100 миллионов Web-сайтов систематизировано по 68 категориям. База данных обновляется со скоростью 150 тысяч URL в день. С помощью столь обширной информации эти устройства безошибочно блокируют нежелательный Web-контент. Благодаря этому создаются благоприятные условия для того, чтобы повысить продуктивность бизнеса и обеспечить соблюдение корпоративной политики использования ресурсов Интернета.

Принцип работы Web Filter

Web Filter функционирует на основе анализа текстов и изображений Web-сайтов, к которым обращаются пользователи. На основе проведенного анализа сайты ранжируются по категориям.

Основные возможности Web Filter

- ✓ Глубокий анализ контента интернет-сайтов (изображений и текстов).
- ✓ Создание «черных» и «белых» листов доступа.
- ✓ Блокирование доступа к запрещенным к просмотру страницам.
- ✓ Система обучения, основанная на обнаружении пользователями сайтов, не внесенных в систему категорий (технология WebLearn).
- ✓ Доступ с паролем к выделенным интернет-сайтам.
- ✓ Назначение различных правил доступа для различных пользователей и групп пользователей.
- ✓ Мощная система мониторинга и генерации отчетов Filter Reporter:
  - более 150 предустановленных отчетов;
  - простой механизм создания собственных видов отчетов;
  - генерация отчетов в режиме реального времени для немедленного анализа;
  - возможность сохранения отчетов более чем в десяти различных форматах данных, в том числе PDF, DOC, XLS.
- ✓ Мониторинг использования интернет-ресурсов.

Основные достоинства Web Filter

- ✓ Увеличение производительности деятельности сотрудников.
- ✓ Снижение затрат на оплату услуг интернет-провайдера.
- ✓ Повышение уровня безопасности информационной системы компании.
- ✓ Интеграция с proxy-серверами MS ISA, SQUID, BlueCoat SG, Netcache.

Поддерживаемые операционные системы

- Windows 2000, Windows XP, Windows 2003.
- Red Hat Linux 7.3, 8.0, 9.0* (kernel 2.4**).
- SUSE Linux 7.3, 8.1, 8.2, 9.0* (kernel 2.4**).

IBM Proventia® Management SiteProtector™

Система управления безопасностью

Модель SP1001

Система централизованного управления SiteProtector выпускается в виде программного комплекса и в виде программно-аппаратного устройства и предназначена для решения следующих задач.

- ✓ Управление средствами защиты. SiteProtector позволяет управлять всем спектром продуктов IBM ISS. Помимо этого, имеется возможность управления средствами защиты информации третьих фирм (Third Party), включая межсетевые экраны, средства построения VPN и т.д.
- ✓ Сбор и отображение событий в реальном режиме времени. Каждое устройство семейства Proventia или агент системы защиты сообщает системе SiteProtector обо всех детектируемых событиях. Кроме того, могут быть подключены системы защиты третьих фирм (Third Party).
- ✓ Фильтрация событий на консоли управления. В системе SiteProtector используются фильтры событий для сокращения массы данных, отображаемых на консоли. Также происходит группирование ресурсов, что в результате позволяет обратить внимание оператора системы лишь на действительно критичные и серьезные атаки и уязвимости. Существует как множество встроенных фильтров, так и возможность создания пользовательских фильтров.

Предопределенные фильтры позволяют быстро выяснить следующие данные:

- Кто атакует выбранные ресурсы?
- Какие ресурсы являются источниками атак?
- Какие узлы уязвимы?
- Какие узлы атакуют?
- Какие уязвимости на выбранных ресурсах?
- Какие критичные атаки зафиксированы?
- Какие критичные уязвимости зафиксированы?
- Какие атаки нанесли ущерб?

Собственные фильтры можно создавать на основе различных параметров, в их числеимя события, тип события (уязвимость, атака и т.д.), степень риска, время наступления события, число событий, адрес источника и цели события, порт источника и цели события, имя сенсора, зафиксировавшего событие.

- ✓ Анализ данных. По каждому из зафиксированных событий предоставляется подробная информация, а именно:
  - адрес источника события, включая IP-, NetBIOS-, DNS- и MAC-адреса;
  - тип события (уязвимости или атаки), степень риска и возможные последствия данного события;
  - адрес и имя сенсора, зафиксировавшего событие, и дата/время фиксации;
  - подробное описание события, включая пошаговые рекомендации по устранению возможности его реализации и использования;
  - подверженные событию операционные системы и приложения;
  - примеры ложных срабатываний;

- дополнительные ссылки на обновления, устраняющие возможности реализации и использования данного события.

✓ Корреляция данных, получаемых от всех управляемых средств защиты. Модуль корреляции данных Security Fusion используется на этапе анализа событий, что позволяет минимизировать избыточный сетевой трафик сообщений от инфраструктурных устройств безопасности и предоставить возможность администраторам сосредоточить внимание на более важных событиях безопасности.

✓ Автоматическое обновление компонентов средств защиты (X-Press Update). В системе SiteProtector реализован механизм X-Press Update, который позволит автоматически и своевременно получать обновления базы данных уязвимостей и атак или иных компонентов (например, новых отчетов) из специального хранилища по каналу, защищенному от несанкционированного доступа. В качестве такого хранилища может выступать как Web-сервер IBM ISS или внутренний корпоративный портал компании, так и сетевой или локальный диск, на которых хранятся все обновления X-Press Update.

✓ Система генерации отчетов. SiteProtector включает в себя множество предустановленных категорий отчетов. Отчеты могут отображаться как в графическом, так и в текстовом виде. Поддерживаются различные форматы представления данных: HTML, CSV, RTF.

Основные достоинства

✓ Система управления на аппаратной платформе. Возможность приобретения устройства с предустановленным программным обеспечением (SiteProtector Management Appliance SP1001).

✓ Категоризация ресурсов. Для упрощения и облегчения процессов анализа событий безопасности и создания отчетов в интерфейсе SiteProtector имеются поля категоризации ресурсов (risk index, criticality, owner, inventory ID).

✓ Работа с ролями и правами доступа. В SiteProtector реализованы механизмы объединения пользователей в группы и составления модели полномочий пользователей. Благодаря модели полномочий механизм создания и сопровождения групп пользователей приобретает большую гибкость и эластичность.

✓ Система реакции на инциденты (Ticketing system). С помощью данного механизма процесс отслеживания и реагирования на инциденты безопасности стал более простым и понятным. Помимо собственной системы реакции возможно использование отдельных внешних систем, таких как Remedy.

✓ Динамическая архивация событий. С помощью компонента Event Archive события информационной безопасности могут быть зафиксированы в текстовом файле и заархивированы. Другой компонент SiteProtector – Event Filtering – может собирать для архивирования не только все события с Event Collector, но и события по выбранному критерию (IP-адрес, название события).

✓ Поддержка кластеров для SQL-серверов. Для того чтобы укрепить защиту от потери информации в результате отказа базы данных, в SiteProtector реализована поддержка кластерных конфигураций для SQL Server.

✓ Поддержка отказоустойчивой конфигурации. Модуль SecureSync реализует механизм отказоустойчивой конфигурации для системы управления SiteProtector.

✓ Система лицензирования. Proventia OneTrust Licensing – это лицензионная система, благодаря которой пользователь получает одну лицензию на все продукты, управляемые SiteProtector, вместо набора лицензий на каждый продукт.

SiteProtector SecurityFusion

SecurityFusion позволяет коррелировать информацию об атаках и уязвимостях, обнаруженных системами анализа защищенности и предотвращения атак Proventia IPS. Данный модуль необходим для снижения числа ложных срабатываний и для того, чтобы сигналы тревоги отображались только тогда, когда это действительно нужно. Например, данный модуль позволяет не показывать на консоли SiteProtector сообщение об атаке, если она не способна нанести никакого ущерба корпоративным ресурсам.

К задачам, решаемым SecurityFusion, можно отнести:

- ✓ автоматический анализ журналов регистрации разнородных средств защиты, существенно сокращающий время, необходимое для такого анализа;
- ✓ экономию времени и денежных средств;
- ✓ создание эффективной системы защиты в условиях нехватки опыта и знаний;
- ✓ возможность для администратора оперативно выяснять, увенчалась ли удачей та или иная атака, что было известно хакеру о цели его атаки и т.д.

SecurityFusion позволяет:

- ✓ коррелировать события из журналов регистрации продуктов линейки IBM ISS;
- ✓ динамически изменять приоритеты атаки;
- ✓ добавлять или удалять варианты реагирования;
- ✓ учитывать время устаревания информации об уязвимостях.

В зависимости от событий, сопутствующих атаке или уязвимости, модуль SecurityFusion формирует выводы о том, уязвим ли атакуемый узел и нанесет ли хакерская атака реальный ущерб.

По результатам такого анализа модуль SecurityFusion может автоматически повысить или понизить степень риска данной атаки, администратор же, в свою очередь, не потратит времени на исследование безвредной атаки либо обратит внимание на опасную атаку и оперативно отреагирует.

SiteProtector SecureSync, Integrated Failover System

SiteProtector SecureSync – это программный модуль, реализующий механизм отказоустойчивости унифицированной системы управления SiteProtector.

Отказоустойчивость обеспечивается благодаря тому, что основная система управления SiteProtector дублирует дополнительную, резервную систему.

Использование SiteProtector SecureSync позволяет решить следующие задачи:

- ✓ сохранение функционала системы SiteProtector в случае критических сбоев в ее работе, при выходе из строя корпоративной сети или при других аварийных ситуациях.
- ✓ сохранение данных системы SiteProtector в случае выхода из строя основного узла управления.

Основные достоинства

- ✓ Постоянная доступность и бесперебойность работы системы.
- ✓ Полное исключение потери данных.
- ✓ Повышение качества обеспечения информационной безопасности за счет непрерывности процесса управления.
- ✓ Катастрофоустойчивость (в случае установки копий SiteProtector по территориально распределенному принципу).

SiteProtector Third Party Module

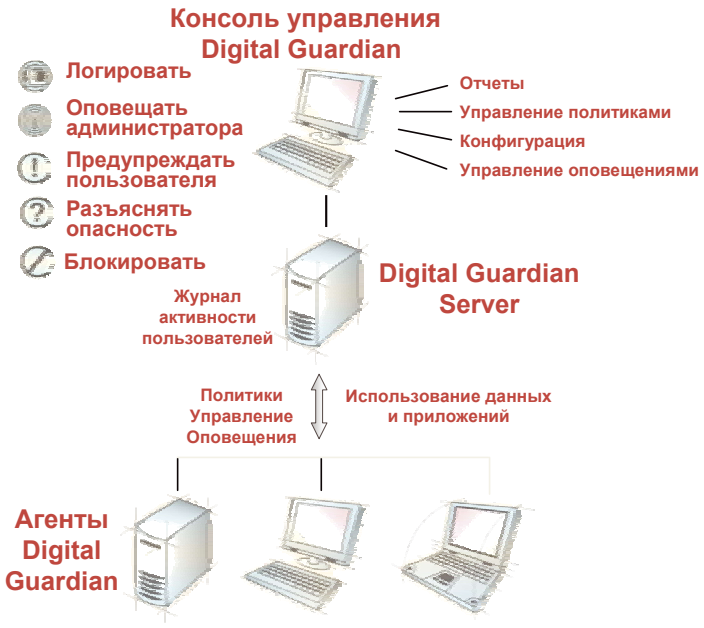
Подключаемый к системе централизованного управления SiteProtector модуль Third Party Module позволяет собирать и приводить к единому формату сигналы тревоги от решений третьих фирм. Например, от межсетевых экранов, компаний Cisco Systems и Check Point Software.

Основные возможности

- ✓ Автоматический сбор и анализ сообщений от межсетевых экранов.
- ✓ Контроль действий администратора на межсетевом экране.
- ✓ Поддержка стандарта OPSEC.
- ✓ Корреляция событий от межсетевых экранов.
- ✓ Поддержка Cisco PIX Firewall и Check Point Firewall-1.
- ✓ Повышение эффективности систем обнаружения и предотвращения атак.
- ✓ Снижение времени на принятие решения о реагировании на несанкционированные действия.

Verdasys Digital Guardian – защита от утечек данных

Программное решение Digital Guardian от Verdasys – это программное обеспечение, устанавливаемое на уровне ядра операционной системы, обеспечивающее полный контроль и безопасность потоков защищаемых данных внутри компании и за ее пределами. Digital Guardian реализует защиту данных в режиме реального времени вне зависимости от типа приложений и протоколов связи.



Полная функциональность решения Digital Guardian обеспечивает:

- ✓ Контроль защищаемой информации, гибкий функционал как в пределах, так и за пределами корпоративной сети.
- ✓ Контроль за перемещением и использованием информации с возможностью доказательства в случае возникновения инцидентов.
- ✓ Централизованное создание и применение политик, которые позволяют не только определять активность пользователей, но и классифицировать данные по контексту и контенту.
- ✓ Гибкое реагирование на действия пользователей при нарушении политик – предупреждение, блокирование, оповещение, ввод объяснения действия, а также – автоматическое шифрование файлов и электронной почты.

- ✓ Защищенное копирование, передачу, хранение и совместную работу с конфиденциальной информацией.
- ✓ Шифрование файлов, в том числе для устройств Blackberry и Microsoft Windows Mobile.
- ✓ Универсальный контроль над любыми типами данных на любых типах носителей – жесткие диски, съемные носители, электронная почта, смартфоны, FTP-серверы, сетевые устройства хранения данных, мейнфреймы и другие, включая защиту и контроль над съемными носителями (съемные диски, смартфоны, mp3-плееры и многое другое).
- ✓ Разработку политик безопасности и внедрение решение силами консультантов IBM.

Благодаря гибкой политике лицензирования решения Digital Guardian, заказчик может использовать всю или только часть необходимой функциональности.

Модули DLP решения Verdasys Digital Guardian

МОДУЛЬ	ОПИСАНИЕ	ПРЕИМУЩЕСТВА
Adaptive File Encryption	Модуль шифрования конфиденциальных файлов, расположенных или копируемых на локальные диски, сетевые хранилища, съемные носители, CD/DVD. Модуль работает прозрачно для пользователя за счет единого хранения и обмена ключами шифрования	Возможность использования единого решения для шифрования данных, принудительное использование политик шифрования для отчуждаемых данных, снижение риска потери информации
Adaptive Email Encryption	Модуль прозрачного шифрования почты, включая тело письма и вложения. Модуль работает прозрачно для пользователя за счет единого хранения и обмена ключами шифрования	Возможность использования единого решения для шифрования данных, принудительное использование политик шифрования для почтового трафика. Безопасный обмен конфиденциальными данными по e-mail
Adaptive Full Disk Encryption	Модуль прозрачного шифрования диска на уровне файловой системы	Защита данных при утере компьютера. Гибкое и простое в управлении решение. Возможность восстановления данных
Trust Verification Agents	Модуль предоставляет доступ к конфиденциальным документам только доверенным рабочим станциям, на которых установлен агент безопасности и применены политики безопасности	Модель запрещает доступ в корпоративную сеть, если агент безопасности не запущен и на нем не применены политики безопасности
Application Management	Модуль управления доступом к приложениям. Позволяет разрешить использование, запретить использование или разрешить только определенным пользователям использование любых типов приложений	Снижает риски использования несанкционированных приложений и запуск потенциально вредоносных программ
Application Logging and Masking	Модуль автоматического маскирования данных и протоколирования доступа для терминальных и Web-серверов на основе заданных политик, например, для номеров кредитных карт	Возможность обеспечения соответствия требованиям стандартов ИБ без необходимости внесения изменений в исходные приложения
Context Based Data Management	Поиск, классификация, мониторинг и применение политик на основе контекстных признаков – тип файла, название, время создания, автор, приложение, место хранения, размер, контрольная сумма и т.п.	Возможность применения гибких политик доступа для неклассифицированных данных

Content Based Data Management	Поиск, классификация, мониторинг и применение политик на основе контентных признаков – слова, словосочетания, «регулярные» выражения, типовые данные анализируются в более 300 форматов данных на более чем 90 иностранных языках	Возможность анализа данных на серверах, рабочих станциях, мобильных устройствах и терминальных серверах
eDiscovery and Forensic Reporting	Модуль обеспечивает сбор и предоставление информации о доступе и работе пользователей с конфиденциальной информацией. Может быть использован при проведении расследований	Возможность гибкого создания произвольных отчетов на основе запросов
Reporting for Audit and Decision Support	Модуль отчетности. Возможность применения на уровне приложений, типов конфиденциальных документов, пользователей и групп пользователей	Возможность гибкого создания произвольных отчетов на основе запросов

IBM Tivoli Provisioning Manager for Software

Этот продукт обеспечивает:

- ✓ инвентаризацию программного обеспечения;
- ✓ инвентаризацию аппаратного обеспечения;
- ✓ установку патчей, программного обеспечения, удаление запрещенных политикой безопасности программ.

Информация, полученная при инвентаризации, в дальнейшем может использоваться средствами идентификации угроз и уязвимостей.

IBM Tivoli Security Compliance Manager

IBM Tivoli Security Compliance Manager действует как система раннего предупреждения, помогая малым, средним и крупным предприятиям идентифицировать нарушения политики защиты и потенциальные системные уязвимости задолго до появления реальной угрозы. Он предлагает предприятиям быстрый, рентабельный и действенный способ сбора и обработки информации о состоянии защиты корпоративных систем.

Основые возможности.

- ✓ Сбор информации, относящейся к безопасности от информационных ресурсов и хранение в базе данных.
- ✓ Сравнительный анализ защищенности информационных систем с установленными шаблонами политик, предоставление отчетов о соответствии политике безопасности компании.

Пример проверки: контроль наличия на рабочей станции персонального firewall, антивирусной программы, своевременных обновлений антивирусных баз, **установленных патчей**, парольной политики, посторонних сервисов.

IBM Tivoli Security Compliance Manager интегрирован с IBM Tivoli Provisioning Manager для устранения выявленных несоответствий (удаление запрещенных программ, установка патчей), а также с решением Cisco Network Admission Control (Cisco NAC) для построения системы управления доступом к сети.

IBM Tivoli Identity Manager

IBM Tivoli Identity Manager обеспечивает централизацию и автоматизацию процедур создания, изменения и удаления учетных записей и управления идентификационными данными пользователей в масштабе всей ИТ-инфраструктуры.

Основные возможности

- ✓ Управление жизненным циклом идентификационных данных, от создания до блокирования и удаления.
- ✓ Возможность настройки электронного документооборота по заявкам на получение прав доступа (рабочий поток).
- ✓ Самообслуживание пользователями своих идентификационных данных.
- ✓ Консолидация идентификационных данных пользователей от различных систем, приложений, баз данных.
- ✓ Управление доступом, основанное на ролях (Role Based Access Control, RBAC), базируется на наборах разрешений, связанных с ролями, представляющими должностные функции пользователей.
- ✓ Средства единой централизованной аутентификации пользователей (single sign-on, SSO), позволяющие уполномоченным пользователям после однократной аутентификации обращаться к защищенным ресурсам, расположенным в различных системах, приложениях, базах данных.
- ✓ Аудит операций по управлению пользователями.

Общие принципы работы

1. Кадровое подразделение регистрирует нового сотрудника в программном приложении учета кадров.
2. В соответствии с установленной в компании процедурой утверждения заявок на предоставление доступа к информационным ресурсам осуществляется автоматизированное прохождение утверждения заявки уполномоченными должностными лицами с использованием встроенных средств электронного документооборота системы Identity Manager.
3. После утверждения заявки пользователю в автоматическом (полуавтоматическом, ручном) режиме присваиваются права доступа ко всем необходимым информационным ресурсам (приложениям, СУБД, электронной почте, каталогам, файловым ресурсам, принтерам и т.п.) в соответствии с его должностными обязанностями.
4. В случае изменения должностных обязанностей сотрудника производится оперативное изменение его роли в системе Identity Manager и предоставление иных прав доступа одновременно во всех информационных ресурсах в соответствии с его новой должностью.
5. При увольнении сотрудника кадровое подразделение регистрирует факт увольнения в программном приложении учета кадров, при этом система Identity Manager оперативно отслеживает изменение статуса сотрудника и блокирует доступ ко всем ранее предоставленным сотруднику ресурсам. В дальнейшем автоматически происходит удаление всех учетных записей сотрудника.

IBM Tivoli Identity Manager позволяет управлять идентификационными данными таких ресурсов, как Microsoft Windows /Active Directory, Novell NetWare, Sun Solaris, i5/OS, AIX, HP-UX, Red Hat Linux, Lotus Notes, LDAP V3 Compliant Directory Servers, DB2, Oracle, MS SQL, SAP-системы, Oracle ERP, Siebel, другие приложения (при помощи Application Management Toolkit).

Подробно смотрите на сайте http://publib.boulder.ibm.com/tividd/td/IdentityManager4.6.html.

IBM Tivoli Federated Identity Manager (FIM)

FIM реализует простую слабосвязанную модель управления идентификацией пользователей и доступом к ресурсам, размещенным в нескольких компаниях или защищенных зонах. Например, в случае двух взаимодействующих компаний решение IBM Tivoli Federated Identity Manager не реплицирует структуры управления идентификацией и администрирования безопасности обеих структур, а предоставляет простую модель для единого управления идентификацией и обеспечивает доступ к информации и сервисам на основе доверительных отношений между ними. Компаниям, применяющим сервис-ориентированные архитектуры (SOA) и Web-сервисы, решение FIM обеспечивает основанное на правилах единое управление безопасностью для так называемых федеративных Web-сервисов. Основа FIM – доверительные отношения, целостность и конфиденциальность данных. Это позволяет организациям совместно использовать идентификационные данные и правила доступа пользователей к сервисам, не применяя дублирование локальных идентификационных данных и правил безопасности. Совместное использование идентификаторов и правил безопасности в рамках «федерации» (объединения партнеров на условиях взаимного доверия) – ключевое условие для предоставления сотрудникам расширенных возможностей по перемещению между несколькими объединенными Web-сайтами этой федерации.

Доверительные отношения позволяют компаниям реализовать нежесткое объединение применяемых в каждой компании систем управления идентификацией пользователей.

Федеративная модель упрощает администрирование и позволяет компаниям распространить управление идентификацией и доступом на пользователей и сервисы других организаций.

Компании, собирающиеся реализовать межкорпоративные бизнес-процессы с идентификацией доступа, могут воспользоваться следующими возможностями решения IBM Tivoli Federated Identity Manager:

- ✓ Упрощение интеграции между Web-сайтами компании и ее партнеров, включая управление сессиями.
- ✓ Улучшение соответствия бизнес-требованиям благодаря ослаблению угроз безопасности.
- ✓ Расширение возможностей конечных пользователей благодаря технологии централизованного входа в систему (SSO).
- ✓ Расширение масштабов бизнеса поставщиков услуг благодаря созданию новых возможностей для получения дохода.
- ✓ Упрощение администрирования безопасности в межкорпоративных бизнес-процессах на основе сервисов безопасности.
- ✓ Обеспечение интегрированного управления безопасностью на основе правил для Web-сервисов в SOA-среде.
- ✓ Поддержка открытых стандартов и спецификаций, включая LAP, SAML, WS-Federation, WS-Security и WS-Trust.

Управление доступом и Single Sign-On

В организациях с большим количеством информационных ресурсов, требующих независимой аутентификации, существует проблема запоминания пользователями паролей и своих имен на разных ресурсах. Сложность запоминания приводит зачастую к тому, что пользователи начинают записывать пароли на бумаге, хранить их в незащищенных местах, сообщать коллегам, что существенно снижает уровень защищенности данных. Дополнительно возрастает нагрузка на службу поддержки по сбросу забытых паролей.

Сократить количество паролей для запоминания и снизить угрозы, связанные с неправильным обращением с паролями, позволяют решения по централизованной аутентификации пользователей (Single Sign-on). Благодаря их внедрению пользователю достаточно аутентифицироваться только один раз при входе в систему и далее аутентификация будет происходить прозрачно для пользователя для всех информационных ресурсов, доступ которым ему разрешен. Внедрение систем единой аутентификации дает следующие преимущества:

- Наличие единого средства аутентификации для доступа ко всем информационным ресурсам, доступным пользователю.
- Возможность повышения надежности аутентификации благодаря использованию спецсредств.
- Исключение необходимости запоминания большого количества паролей к разным ресурсам.

Для решения задачи централизации системы управления доступом IBM предлагает использовать решения на базе семейства продуктов Tivoli Access Manager: Tivoli Access Manager for e-business, Tivoli Access Manager for Enterprise Single Sign-On, Tivoli Access Manager for Operating Systems.

IBM Tivoli Access Manager for e-business

Tivoli Access Manager for e-business – это решение для создания централизованной системы управления доступом для приложений, построенных на Web-технологиях (порталы, Web-серверы), предназначенное для решения следующих основных задач:

1) Централизация процессов аутентификации и авторизации пользователей, в рамках которой принятие решения о возможности доступа пользователя к информационному ресурсу осуществляется центральным сервисом авторизации, а не в каждой системе отдельно.
2) Обеспечение единой точки доступа пользователей к информационным ресурсам, опубликованным на Web-серверах, порталах.
3) Обеспечение выполнения единой процедуры регистрации (механизм Global Sign-On) при доступе пользователей к информационным ресурсам, опубликованным на Web-серверах.
4) Использование политик безопасности в рамках процессов предоставления доступа пользователей к информационным ресурсам.
5) Централизация действий администраторов по управлению доступом пользователей к информационным ресурсам.
6) Эффективная организация аудита доступа пользователей к информационным ресурсам и формирование отчетов аудита.
7) Управление сессиями (сеансами) доступа пользователей к информационным ресурсам, опубликованным на Web-серверах.

IBM Tivoli Access Manager for Enterprise Single Sign-On (TAM E-SSO)

Решение TAM E-SSO позволяет пользователям использовать **один пароль для входа во все используемые приложения**, включая корпоративные приложения и приложения в Интернета. TAM E-SSO позволяет осуществлять регистрацию с помощью одного пароля практически для любого Windows-, Web- или разработанного внутри компании приложения.

TAM E-SSO использует приложение-агент, устанавливаемое на ПК пользователя, которое отвечает на запросы приложения (на ввод идентификационных данных пользователя) от имени пользователя. Агент автоматически предоставляет приложению все данные, необходимые для аутентификации пользователя, включая имя пользователя, пароль или другие данные, требуемые приложением.

Использование дополнительных адаптеров TAM E-SSO позволяет расширить функциональность решения:

- ✓ **Desktop Password Reset Adapter** позволяет пользователям самостоятельно и безопасно сбрасывать свои пароли Windows без обращения в службу поддержки посредством предопределенных ответов на секретные вопросы.
- ✓ **Authentication Adapter** позволяет использовать различные способы аутентификации пользователей – токены, смарт-карты, биометрию и пароли.
- ✓ **Provisioning Adapter** осуществляет интеграцию с системой управления пользовательскими записями Tivoli Identity Manager. При совместной работе с Tivoli Identity Manager позволяет заранее заполнить реестр учетных записей конечных пользователей TAM E-SSO, что избавляет пользователей от необходимости вводить свои идентификаторы и пароли или даже знать их.
- ✓ **Kiosk Adapter** устраняет потенциальные угрозы при совместном использовании сотрудниками одной рабочей станции или киоска, автоматически отключая неактивные сеансы и выключая приложения.

IBM Tivoli Access Manager for Operating Systems

IBM Tivoli Access Manager for Operating Systems обеспечивает дополнительный уровень авторизации для ОС UNIX/Linux вдобавок к уровню, предоставляемому операционной системой, что **помогает контролировать злоупотребления доступом.** Данное решение позволяет организовать доступ к ресурсам ОС на основе централизованно определяемых политик доступа. Данные политики позволяют принимать решение о возможности доступа к ресурсу на основании идентификационных данных пользователя, членства в группах, типа запрошенной операции с ресурсом, времени суток, типа ресурса и т.д. Такой подход позволяет закрыть большое количество уязвимостей, связанных с использованием учетных записей суперпользователей (‘root’) в ОС UNIX/Linux. Большинство сбоев в безопасности UNIX/Linux-систем связано со злоупотреблением данными учетными записями или их взломом, который приводит к возможности доступа к ОС (и соответственно – к приложениям, функционирующим в данной ОС) с правами суперпользователя.

Функции продукта IBM Tivoli Access Manager for Operating Systems:

- ✓ обеспечение централизованного сервиса авторизации для операционных систем UNIX/Linux;
- ✓ предоставление администраторам единого Web-интерфейса для управления доступом к ресурсам UNIX/Linux-систем;
- ✓ сбор информации аудита, включающей аудит операций с информационными ресурсами и аудит действий по управлению доступом, а также генерация отчетов.

Особенности продукта IBM Tivoli Access Manager for Operating Systems

- ✓ Использует единую инфраструктуру с продуктами IBM Tivoli Access Manager for e-business.
- ✓ Обеспечивает защиту критичных ресурсов ОС UNIX/Linux (файлов, процессов, приложений, TCP-соединений) для предотвращения несанкционированного доступа вне зависимости от административных прав пользователя.

- ✓ Позволяет обеспечить защиту класса mainframe, при этом обеспечивая простоту и удобство работы администратора и автоматическую генерацию отчетов аудита.
- ✓ Обеспечивает развитую систему предотвращения взломов – межсетевой экран, защиту приложений и платформы в целом, аудит и контроль действий пользователей, продвинутые механизмы аудита и проверки соответствия.
- ✓ Помогает построить систему защиты от основной угрозы, с которой сталкиваются организации, – злоупотреблений пользователей и сотрудников.

IBM Tivoli Compliance Insight Manager (TCIM)

IBM Tivoli Compliance Insight Manager – решение для внутреннего аудита действий всех пользователей, в том числе с высокими полномочиями доступа (администраторы сетей, баз данных, ОС, приложений). TCIM обеспечивает корреляцию событий безопасности от различных источников: операционных систем, СУБД, приложений, сетевых устройств, средств безопасности, мэйнфреймов, приведение полученных больших объемов информации о событиях безопасности к удобному для восприятию виду (кто, что, где, когда, откуда, куда), оперативное уведомление об нарушениях политики безопасности, возможности расследования инцидентов, контроль за действиями внутренних пользователей, привилегированных пользователей, сторонних консультантов, контроль непрерывности хранения журналов безопасности, контроль соответствия нормативным требованиям (включая ISO 27001, ISO 17799, SOX и другие).

Выгоды от использования продукта:

- ✓ обеспечивает полный контроль за действиями пользователей, включая суперпользователей, на уровне операционных систем, баз данных, приложений, сетевых устройств, средств безопасности, мэйнфрэймов;
- ✓ создание отчетов на соответствие нормативным требованиям, включая закон о персональных данных.

Функциональные особенности, преимущества, результаты

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ	ПРЕИМУЩЕСТВА	РЕЗУЛЬТАТЫ
Централизованный мониторинг действий пользователей	Оперативное выявление несанкционированных действий пользователей, в том числе суперпользователей, внешних консультантов, сторонних поставщиков услуг, в масштабах всей ИТ-инфраструктуры	Снижение рисков и угроз информационных ресурсов, связанных со злонамеренными или случайными нарушениями безопасности со стороны пользователей
Преобразование журналов безопасности от различных источников к единому наглядному формату	Отсутствие необходимости в рутинных операциях по анализу и обработке больших объемов событий безопасности, а также – для администраторов безопасности – в обладании экспертными знаниями в области различных технологий по анализу журналов событий безопасности	Оперативное выявление инцидентов безопасности. Сокращение длительности и трудозатрат на аудит. Сокращение расходов на службу технического сопровождения благодаря отсутствию необходимости в привлечении нескольких экспертов в различных технологиях
Масштабируемость	Возможность расширения архитектуры системы в зависимости от требований производительности	Масштабируемая гибкая архитектура, опирающаяся на распределенные хранилища данных о событиях безопасности
Интеграция	Возможность интеграции с продуктами IBM: – Tivoli Indentity Manager, – Tivoli Access Manager, – Tivoli Security Operations Manager, – IBM ISS, а также со средствами безопасности других производителей	Обеспечивает комплексное решение по обеспечению безопасности информации: – управление пользователями; – управление правами доступа; – контроль за действиями пользователей; – соответствие нормативным требованиям PCI, BASEL II и другим

IBM Tivoli Security Operations Manager (TSOM)

IBM Tivoli Security Operations Manager – **решение по мониторингу в реальном времени всех событий безопасности и предотвращению угроз.** TSOM предназначено, в основном, для снижения рисков и угроз, исходящих от внешних нарушителей и технологий при помощи автоматизации часто повторяющихся и трудоемких операций, применяемых специалистами для своевременного обнаружения угроз. К примеру, сопоставление сообщений от сетевых устройств безопасности по всему пути прохождения атаки, оценка интенсивности (частоты) этих попыток, анализ журналов систем и сообщений узловых приложений обнаружения вторжений (HIDS), соотнесение этих данных с учетными данными по уязвимости конкретных систем и сообщениями антивирусного ПО и т.п.

TSOM поддерживает более 250 устройств и программ информационной безопасности от различных производителей: межсетевые экраны, хостовые и сетевые системы обнаружения и предотвращения атак, сканеры безопасности, антивирусное программное обеспечение, журналы операционных систем и прикладного ПО, сетевые устройства, ПО служб каталогов и систем аутентификации и авторизации.

TSOM выдерживает поток 500 и более сообщений в секунду на один агрегационный модуль. Анализ и приоритезация данных производятся при помощи четырех дополняющих друг друга корреляционных техник.

- ✓ **Корреляция на основе правил (Rule-based Correlation)** позволяет выявить известные атаки и нарушения политики безопасности.
- ✓ **Корреляция с учетом уязвимости цели (Vulnerability Correlation)** сопоставляет известные атаки с известными слабыми местами на атакуемой системе. Данные по уязвимости могут экспортироваться из сканеров безопасности.
- ✓ **Статистическая корреляция (Statistical Correlation).** Запатентованный алгоритм этой корреляции позволяет выявлять неизвестные ранее атаки и ненормальные, потенциально опасные действия. В среднем одна только статистическая корреляция может выявлять до 70% всех инцидентов.
- ✓ **Корреляция с учетом восприимчивости (Susceptibility Correlation)** определяет вероятность нанесения повреждения атакуемому объекту.

IBM Rational AppScan – безопасность Web-приложений

Согласно последним данным аналитиков 75% атак приходятся на Web-приложения, в то время как на обеспечение их безопасности тратится только 10% от общих затрат. Будучи протестированы, 90% сайтов оказываются уязвимыми для атак на уровне приложений. По данным Gartner, 80% компаний столкнутся с проблемами от таких атак к 2010 году, что может привести к краже или потере важных данных, имеющих значение для бизнеса организации.

Для повышения безопасности Web-приложений IBM предлагает семейство продуктов AppScan (ранее Watchfire), которое занимает лидирующее положение на рынке Application Security. Запатентованный механизм сканирования AppScan постоянно проверяет Web-приложения, тестирует их на предмет проблем безопасности и соответствия нормативным требованиям и составляет отчеты с рекомендациями по исправлению ситуации.

AppScan может эмулировать атаки хакеров, например межсайтовый скриптинг, разделение HTTP-ответов, фальсификацию параметров, манипуляции со скрытыми полями, скрытые возможности/ошибки отладки, замаскированное управление, принудительный просмотр, переполнение буфера приложений, отправление в Web-приложение модифицированных маркеров, неправильное изменение конфигурации третьим лицом, известные слабые места в системе защиты, HTTP-атаки, SQL-инъекции, подозрительный контент, тесты XML/SOAP, спуфинг контента, инъекции по облегченному протоколу доступа к каталогам (LDAP), XPath-инъекции и фиксацию сеанса.

AppScan Enterprise позволяет тестировать Web-сайты с тысячами приложений и анализировать несколько приложений одновременно.

AppScan позволяет не только обнаружить проблемы, но выявить конкретные причины уязвимостей, а также получить рекомендации по их устранению. Надежная система составления отчетов на основе базы данных может автоматически направлять результаты сканирования в центральное хранилище с возможностью настройки представления данных и сквозного анализа.

IBM Managed Security Services (MSS)

Круглосуточное управление безопасностью в режиме реального времени

Не многие организации имеют возможность обеспечивать оперативное реагирование на постоянно меняющиеся угрозы сетевых атак, опасных для деятельности и прибыли компании. Корпоративная безопасность – система, которая круглосуточно и без выходных обеспечивает выполнение требований по обновлению ПО, управляет устройствами в разнородной ИТ-инфраструктуре и следит за выполнением политик безопасности в отношении сотрудников, поставщиков и заказчиков компании. В пакет услуг IBM Managed Security Services входят внедряемые сотрудниками IBM комплексные решения для обеспечения безопасности в режиме реального времени, предназначенные в том числе для мониторинга системы, оперативного реагирования и круглосуточной защиты. Цена предложения во много раз меньше стоимости реализации подобной системы безопасности, проведенной собственными силами компании.

Мониторинг операций по обеспечению безопасности из командного центра

Центр IBM ISS Virtual-Security Operations Center (Virtual-SOC) дает организациям возможность просматривать и управлять всеми устройствами и услугами, связанными с обеспечением безопасности – как IBM ISS, так и других поставщиков, посредством одной Web-консоли – портала Virtual-SOC. Таким образом, Virtual-SOC предоставляет в распоряжение каждого заказчика все возможности шести оперативных центров по обеспечению безопасности IBM ISS, в том числе:

- ✓ опыт признанных специалистов в области безопасности из знаменитого подразделения X-Force;
- ✓ круглосуточный мониторинг и управление – 7 дней в неделю, 365 дней в году;
- ✓ комплексные услуги консультантов IBM ISS;
- ✓ средства регистрации, отслеживания неполадок и оповещения о них, средства обращения в службу поддержки и средства реагирования;
- ✓ средства составления отчетов, архивации и поиска информации;
- ✓ взаимодействие с экспертами подразделения IBM ISS в реальном времени.

IBM Managed Protection Services (MPS)

Это пакет услуг, предлагающий ведущее в отрасли соглашение об уровне обслуживания (SLA) на основе результатов, которое позволяет без труда переложить задачу обеспечения безопасности сети на доверенного партнера. Решения по обеспечению безопасности, входящие в этот пакет, не просто обеспечивают мониторинг сети и управление устройствами, но также предлагают соглашения SLA, в соответствии с которыми в случае нарушения безопасности сети заказчик получит возмещение в размере 50 000 долларов США*. Кроме того, эти решения в режиме реального времени осуществляют мониторинг и выявление неполадок в работе сетей, серверов, настольных компьютеров и беспроводных приложений, которые входят в состав инфраструктуры, объединяющей различные платформы и операционные системы.

IBM Managed and Monitored Firewall Services

Входящие в этот пакет услуги обеспечивают комплексный и круглосуточный мониторинг, анализ журналов брандмауэров и управление ими с целью обнаружения и предотвращения возникающих угроз. Для предоставления услуг разработаны различные планы, чтобы заказчики могли получить максимальную отдачу от инвестиций в существующую систему безопасности за малую часть той суммы, в которую обошлась бы разработка системы своими силами.

IBM Managed IDS & IPS Services (MIDS/IPS)

Этот пакет услуг помогает защищать сети и серверы от внешних и внутренних вторжений. Стоимость этого пакета услуг значительно меньше суммы, которую компании пришлось бы потратить при разработке систем защиты от вторжений (IPS) и обнаружения вторжений (IDS) своими силами. Входящие в этот пакет услуги обеспечивают комплексный и круглосуточный мониторинг и анализ событий IDS, а также управление ими, помогая в реальном времени реагировать на возникающие угрозы и обращаться в службы поддержки, а также предоставляя все необходимое для расследования действий злоумышленников и восстановления сети после атак.

IBM Security Event and Log Management Services

Этот пакет услуг помогает организациям объединить различные технологии обеспечения безопасности в единую платформу, предназначенную для сбора, анализа, корреляции данных и выявления тенденций в сетевых событиях и событиях, имеющих отношение к безопасности, а также управления процессами реагирования и ликвидации последствий. Заказчики имеют возможность запрашивать данные из журналов приложений и операционных систем с помощью разнообразных устройств, пользуясь единым общим интерфейсом. Это существенно ускоряет расследование нарушений безопасности в инфраструктуре, содержащей большое количество устройств. Кроме того, подразделение IBM ISS предоставляет средства для архивации содержащихся в журналах данных, что крайне упрощает выполнение требуемых законодательством действий по обеспечению безопасности.

IBM Vulnerability Management Service (VMS)

Эта услуга позволяет автоматизировать весь жизненный цикл управления уязвимостями, наглядно показывая каждую область, представляющую потенциальный риск. Услуга полностью готова к использованию и предназначена для обеспечения непрерывной деятельности компании, делая возможным анализ работы серверов, брандмауэров, коммутаторов и прочих устройств, а также управление ими в реальном времени. Она также объединяет управляемые службы сканирования и возможности для профессионального управления потоком работ и возникающими проблемами для защиты сетевой инфраструктуры от вторжений, потенциально опасных для бизнеса.

* Возврат денег (только для уровня IBM Managed Protection Services – Premium Level): если специалисты подразделения IBM ISS не смогут выполнить гарантийные обязательства по предотвращению нарушений безопасности (Security Incidents Prevention Guarantee), заказчику будет выплачена сумма в размере 50 000 долларов США за каждый случай невыполнения условий гарантии. Дополнительные сведения смотри в соглашениях об уровне услуг IBM Internet Security Systems.

IBM X-Force® Threat Analysis Service (XFTAS)

Эта услуга предоставляет актуальную именно для вас информацию о широком спектре угроз, которые могут повлиять на безопасность вашей сети, и обеспечивает подробный анализ глобальных угроз на основе достоверной информации, поступающей в режиме реального времени из международной сети центров безопасности IBM ISS, и данных, которые предоставляют специалисты по исследованиям и разработке подразделения X-Force.

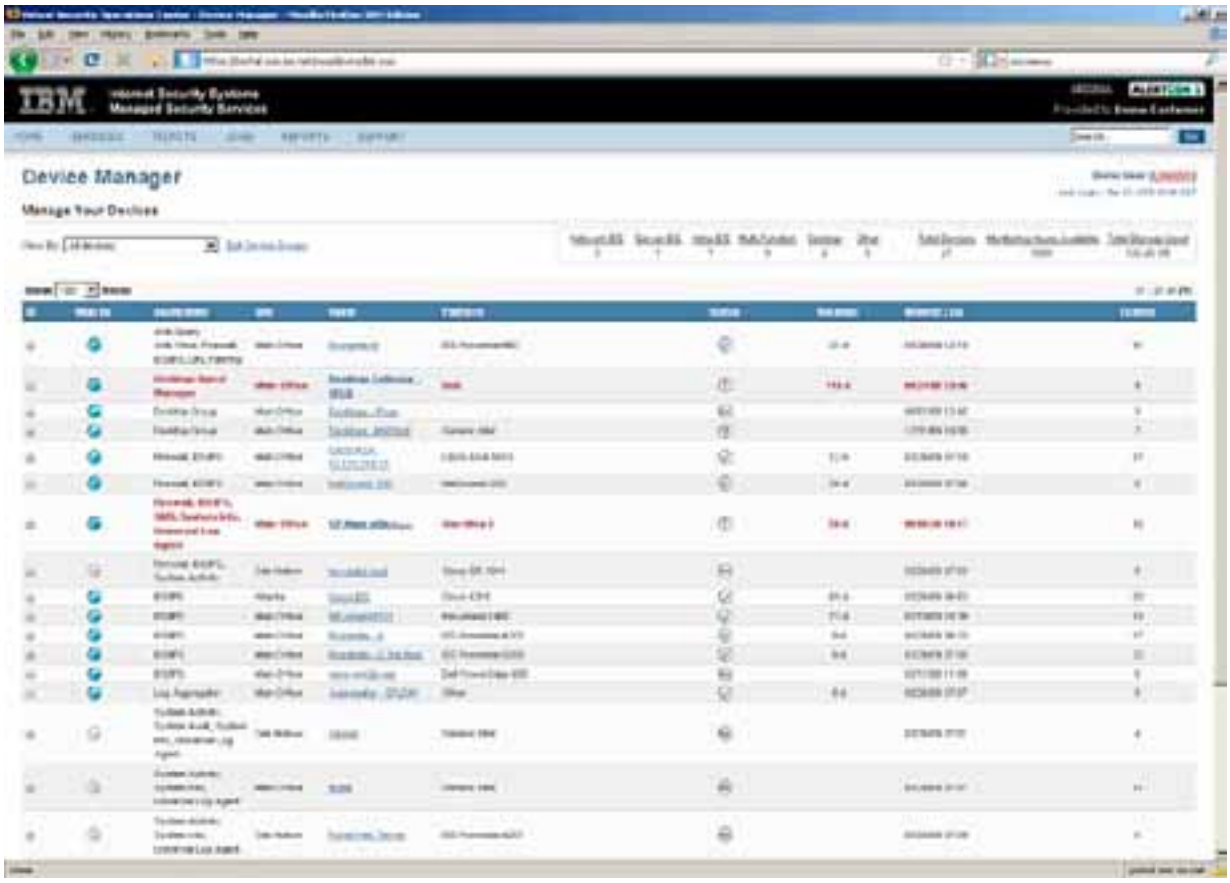
Портал Virtual SOC

Главная страница портала VSOC

Ключевую роль в обеспечении управляемых сервисов играет портал для пользователей услуг MSS (на рисунке выше). Все события, регистрационные журналы, данные о безопасности, а также другие данные, включая заявки на обслуживание, данные об инцидентах безопасности и прочую информацию из системы безопасности, сохраняются в базе данных центра SOC. Каждый авторизованный пользователь получает онлайновый доступ через MSS-портал ко всей информации инфраструктуры безопасности. Гибкая настройка правил доступа к порталу позволяет предоставить сотрудникам отдельных распределенных подразделений заказчика доступ только к информации их площадок, тогда как ИТ-персонал центрального офиса заказчика будет иметь доступ к информации по безопасности всех своих филиалов. Большой выбор стандартных отчетов и удобный инструмент создания индивидуальных отчетов предоставляют ИТ-персоналу все необходимые данные для полноценного управления сервисом.

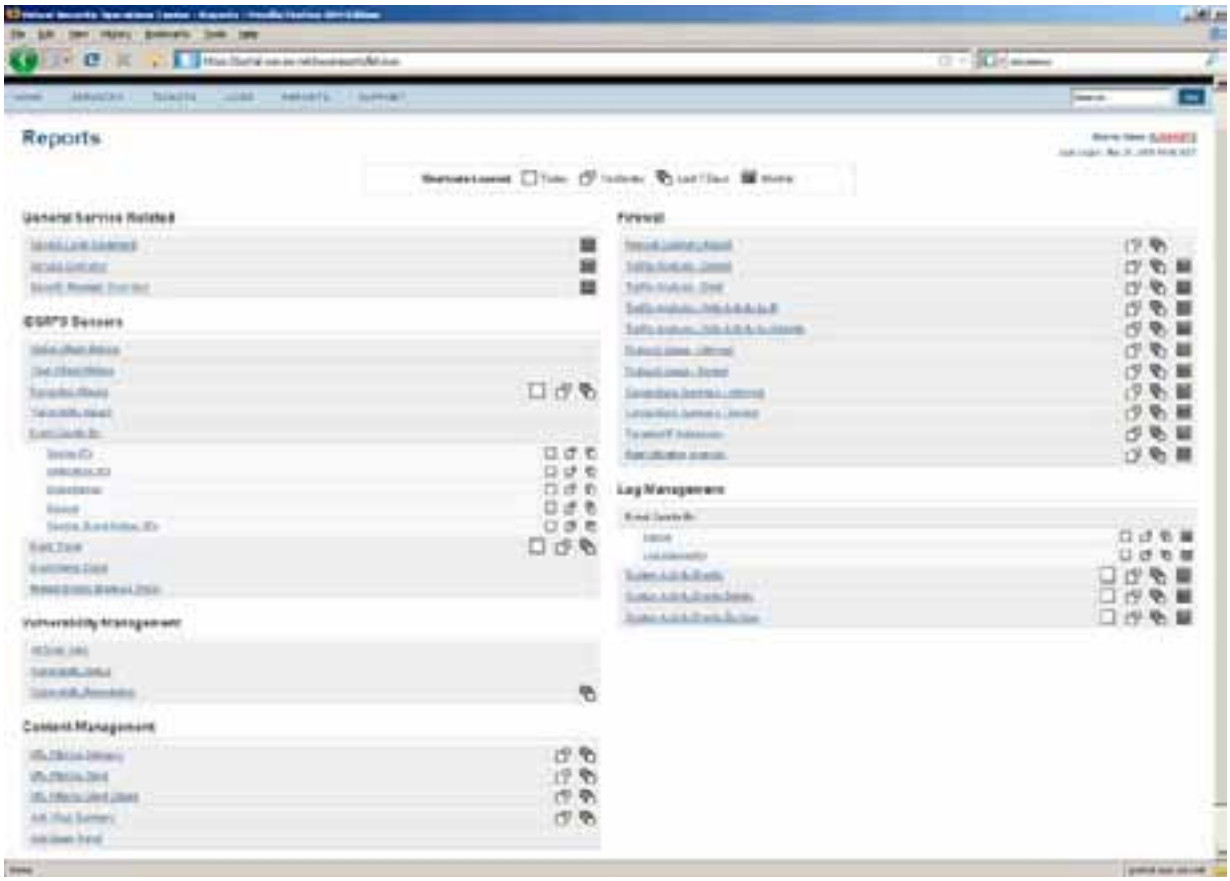
Всем пользователям услуг MSS предоставляется доступ к так называемой системе раннего оповещения (Early Warning System) – аналитической информации, постоянно обновляемой группой X-Force. В нее входит полная база данных всех известных уязвимостей, последние обнаруженные вирусы, троянские программы, описание известных атак, принципов защиты от них и многое другое. Для каждой уязвимости указывается перечень ПО, в котором она обнаружена, и рекомендации по ее устранению. С помощью фильтров (например, Mail Server/Microsoft Corporation/Exchange/5.0 SP2) можно выбрать только те уязвимости, которые отвечают заданному критерию, и автоматически получать уведомления по электронной почте в случае их выявления. Эта система раннего оповещения дает пользователям большие преимущества, поскольку позволяет принимать превентивные меры для защиты систем, непосредственно не охваченных сервисом.

Портал также используется для визуализации, управления инфраструктурой безопасности и сетью заказчика и их обновления.



Панель управления устройствами

Наряду с использованием средств портала для описания организационной структуры и сетевой среды еще одна его задача состоит, несомненно, в управлении событиями безопасности (на рисунке выше) и устройствами и подготовке отчетов (на рисунке ниже). К важнейшей функции портала можно отнести возможность доступа к одной и той же информации, представленной в различной форме. Таким образом, можно отслеживать заявки на расследование, связанные с определенным инцидентом безопасности. Выбрав щелчком мыши инцидент, можно увидеть во всплывающей строке соответствующее событие. Выбор события покажет все данные, зафиксированные соответствующим сенсором системы безопасности. Доступен ряд отчетов, содержащих суммарные сведения о событиях, например обо всех атаках, зарегистрированных за последние семь суток, в виде диаграммы или списка.



Создание отчетов из портала VSOC

С помощью средств портала можно создавать множество предварительно определенных, но гибко настраиваемых отчетов. Все отчеты просматриваются непосредственно на экране либо сохраняются в виде документов формата PDF, HTML, XML. Данные из каждого отчета можно экспортировать в CSV-формате (табличный текст, разделенный запятыми) в различные внешние системы.

Все действия и задачи, выполненные специалистами центра SOC, регистрируются во внутренней базе данных системы документооборота SOC с обязательным указанием даты и времени. Таким образом, автоматически генерируемые ежемесячные отчеты наглядно показывают, выполняются ли со стороны IBM ISS требования соглашений об уровне обслуживания соответствующих сервисных контрактов.

Услуги безопасности на базе Virtual SOC

Услуги безопасности на базе платформы удаленного мониторинга сетей и сетевой безопасности Virtual Security Operations Center (Virtual SOC) можно разделить на две категории.

Первая – это управление безопасностью и мониторинг, включая управление межсетевыми экранами (Checkpoint, Juniper, Cisco, ISS и т.д.), системами IDS/IPS (ISS, Cisco, 3Com/Tipping Point и т.д.), VPN, защитой серверов и рабочих станций. Вторая категория – вспомогательные услуги: управление сканированием и выявлением уязвимостей, анализ событий и логов безопасности, управление почтовым и Web-контентом.

Пользуясь услугами IBM ISS, заказчики получают доступ к информационной защите мирового класса, осуществляемой в рамках установленных правил и условий сервисного контракта и

соглашения об уровне обслуживания (Service Level Agreement, SLA), четко прописанных правил и процедур, на основе фиксированной ежемесячной оплаты. Каждый вид услуги определен в документе Service Description («Описание сервиса»), в котором в точности оговариваются задачи и функции сервиса. Соглашение об уровне обслуживания SLA дополняет описание сервиса и определяет договорные обязательства IBM ISS, а также штрафные санкции к компании в тех случаях, когда эти обязательства не выполняются. Для большей гибкости предлагаются три разных уровня обслуживания – Standard, Select и Premium.

При формировании своего портфеля услуг обеспечения безопасности IBM ISS использует два разных подхода.

Услуги управления безопасностью (Managed Security Services, MSS) относятся к проблемно-ориентированному виду услуг, в соответствии с чем в описании сервиса указываются все задачи, которые нужно выполнить, а в соглашении SLA перечисляются штрафные санкции, которые будут накладываться на поставщика услуг в случае невыполнения этих задач в рамках установленных ограничений. Так, IBM ISS проводит настройку и конфигурирование оборудования, мониторинг событий ИБ и оперативное уведомление клиента в случае возникновения опасности. Сервисы MSS не привязаны к конкретному производителю оборудования и доступны на различных платформах (IBM ISS Proventia, Cisco, Tipping Point, CheckPoint и т.д.).

Услуги гарантированной защиты от угроз (Managed Protection Services, MPS) превосходят традиционные услуги MSS с точки зрения предоставляемых гарантий. Услуги защиты предусматривают те же самые задачи, однако в MPS-режиме IBM ISS гарантирует абсолютную защиту обслуживаемого сегмента. Сервисный контракт MPS подразумевает более жесткие ограничения для IBM ISS, а также возможность применения штрафных санкций, оговоренных в соглашении об уровне обслуживания, в случае пропуска инцидента информационной безопасности. Вследствие более строгих условий соглашения об уровне обслуживания MPS гарантируется только при использовании для защиты продуктов IBM ISS и требует постоянного применения режима активной блокировки (active blocking).

IBM Professional Security Services (PSS)

В дополнение к программным продуктам подразделение IBM ISS предоставляет услуги по обеспечению безопасности на уровне мировых стандартов, помогая спроектировать, построить и поддерживать надежную концепцию обеспечения безопасности.

Подразделение IBM Professional Security Services предоставляет услуги специалистов по безопасности, помогая как небольшим, так и крупным компаниям снизить риск, обеспечить соответствие системы безопасности действующему законодательству, поддерживать бесперебойную работу компании и добиться поставленных целей в области безопасности. Деятельность консультантов IBM Professional Security Services полностью сосредоточена на безопасности. Они используют апробированные методы работы, соответствующие рекомендациям мирового стандарта ISO 17799. Группа экспертов в области безопасности, используя уникальные инструменты, актуальные данные, относящиеся к безопасности, и передовые превентивные подходы, поможет вам разработать эффективные программы обеспечения безопасности для защиты и развития вашего бизнеса.

Предлагаем вам воспользоваться следующими услугами:

IBM Penetration Testing

Эта услуга предназначена для обнаружения уязвимостей в сети и предоставления количественной оценки внешней угрозы при помощи имитации скрытой злонамеренной деятельности, типичной для сетевых вторжений, в рамках безопасных и управляемых испытаний. Она обеспечивает не просто оценку безопасности или сканирование сети, но не имеет себе равных в отрасли по глубине и охвату. Наши опытные эксперты-консультанты проанализируют вашу сеть с точки зрения хакера и представят вам результаты своей работы в виде списка действенных мер, направленных на повышение безопасности, с указанием приоритетов.

IBM Application Security Assessment

Эта услуга предназначена для проведения детального и целенаправленного анализа исходного кода приложений для обнаружения слабых с точки зрения безопасности мест. Она помогает повысить безопасность приложений, работающих с ценными данными. Результатом работы является список подробных рекомендаций по повышению безопасности таких приложений.

IBM Information Security Assessment

Эта услуга предназначена для комплексной оценки системы защиты компании, в том числе политик безопасности, процедур, систем управления и механизмов, а также физической безопасности, сетей, серверов, настольных компьютеров и баз данных. Такая комплексная проверка поможет найти слабые места в ИТ-инфраструктуре, механизмах управления, стратегиях и процедурах. Услуга оценки защищенности основывается на лучших методах в области компьютерной безопасности, и вы получаете готовый план по улучшению всей системы безопасности в целом.

IBM Payment Card Industry Assessment

Эта услуга поможет организациям внедрить стандарты безопасности данных, принятые в индустрии платежных карт (Payment Card Industry, PCI). Подразделение IBM ISS признано Советом по стандартам безопасности PCI в качестве квалифицированного эксперта-консультанта по безопасности (QSA) и авторизованного поставщика услуг сканирования (ASV). Консультанты подразделения имеют сертификаты PCI, позволяющие им проводить оценку безопасности в соответствии с процедурами PCI. Кроме того, мы также можем предложить вам приложение для оплаты посредством карт, которое было разработано консультантами, имеющими звание квалифицированных специалистов по безопасности платежных приложений (QPASP).

IBM Emergency Response Services

Эти услуги включают реагирование на инциденты безопасности, предварительную настройку оборудования для сбора и последующего анализа собранных данных об атаке, проводимых нашими экспертами по безопасности. На эти услуги можно подписаться заранее или пользоваться ими по требованию. Специалисты IBM Emergency Response Services помогут отразить уже начавшуюся атаку и разработать соответствующий потребностям организации план оперативного реагирования для уменьшения ущерба от будущих атак. Кроме того, специалисты по безопасности помогут вам провести криминологический компьютерный анализ, оценить ущерб и подать судебный иск, чтобы найти и наказать нарушителей, использовавших брешь в системе безопасности.

IBM Policy Development

Эта услуга предназначена для разработки стратегии и политики, лежащих в основе критически важных процессов, технологий, управленческих и административных решений. Она помогает защитить ИТ-ресурсы и обеспечить соответствие требованиям законодательства.

IBM Network Architecture DesignServices

Наши специалисты оценят архитектуру вашей сети и совместно с вашими сотрудниками разработают подробный план сети, обеспечивающий максимальную безопасность ИТ-инфраструктуры.

IBM Technology Implementation Planning

Эта услуга поможет вам получить максимальную отдачу от применяемых вами технологий безопасности, потому что с ее помощью можно разработать план внедрения решений по обеспечению безопасности, по возможности не прерывающий нормальной работы сети. Она также поможет вам спланировать техническую поддержку вашей системы безопасности и повседневное управление ею.

IBM Deployment Consulting

Эта услуга поможет вам получить максимальную отдачу от инвестиций в решения IBM ISS. Специалисты по безопасности IBM ISS помогут вам с установкой, конфигурированием и настройкой, а также с переходом на новые решения, разработанные подразделением ISS.

IBM Staff Augmentation

Это возможность укрепить внутренние ресурсы вашей компании прикомандированными экспертами по безопасности подразделения IBM ISS. Консультанты IBM ISS, работая в штате вашей компании, смогут внедрить экономически эффективные инновационные технологии обеспечения безопасности, позволяя штатным сотрудникам сосредоточиться на поддержке повседневной работы компании.

IBM Vertical & Regulatory QuickStart Program

Эта услуга поможет оценить, насколько существующая система безопасности вашей компании соответствует отраслевым стандартам и действующему законодательству, в том числе стандарту систем диспетчерского контроля и получения данных (SCADA), закону Sarbanes-Oxley, закону по обеспечению доступности и подотчетности в медицинском страховании (HIPAA). После этого мы предоставим подробные инструкции, как обеспечить соответствие законодательству и повысить безопасность в целом.

IBM Security Awareness Training

Эта услуга помогает организациям повысить осведомленность своих сотрудников в вопросах безопасности, знание передовых методов защиты информации и правил посредством электронного обучающего курса. Помимо электронного курса подразделение IBM ISS также поможет вам получить максимальную отдачу от инвестиций в решения IBM ISS. Соответствующие учебные курсы будут проводиться на вашей территории или в других местах.

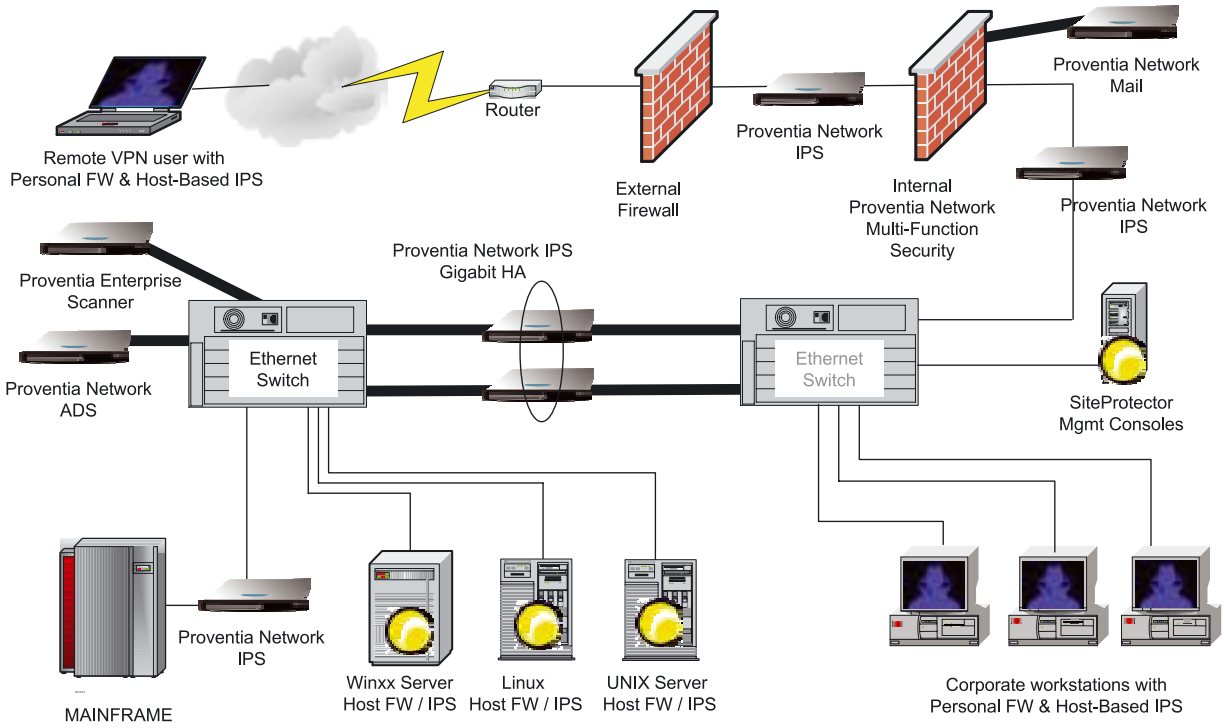
IBM Tivoli Indentity&Access Manager Deployment

Установка продукта семейства Tivoli силами IBM ISS позволит получить максимальный эффект от приобретения продукта и реализовать все функции продукта с максимальной отдачей для бизнеса, что позволит начать эффективно централизованно управлять идентификаторами сотрудников и контролировать доступ своих сотрудников к различным ресурсам сети.

Почему услуги IBM Internet Security Systems?

Для реализации превентивного подхода к обеспечению безопасности нужно провести тщательную исследовательскую работу, знать о последних тенденциях в области угроз безопасности и технологиях защиты от них, а также иметь простую и доступную по цене платформу для предоставления современных решений в области безопасности, основанных на знаниях. Подразделение IBM ISS Security Systems имеет в своем распоряжении обширные знания, инновационные методы исследований и сложные технологии – все, что необходимо для реализации превентивного подхода. Опытные и сертифицированные консультанты, архитекторы, руководители проектов и эксперты в конкретных областях готовы предложить вашей организации комплексную платформу продуктов и услуг в области безопасности, предназначенную для защиты всей ИТ-инфраструктуры – от сетевого шлюза до компьютеров пользователей.

Пример решения по защите сети продуктами IBM Internet Security Systems®



Программно-аппаратные и программные продукты IBM Internet Security Systems

Все продукты имеют единую систему управления и корреляции событий SiteProtector

***Proventia* Multi-Function Security – MX5110, MX5008, MX3006, MX1004, MX0804** Устройство все в одном:
-IDS/IPS, FW, антиспам, Web Filter, антивирус, Anti-spyware, VPS, VPN

***Proventia* Network Mail Security**
MS3004, MS1002-VM Превентивная защита и антиспам для вашей корпоративной почты
- сигнатурный и поведенческий антивирус
- антиспам+URL-фильтр
- IPS
- mail firewall

***Proventia* Intrusion Prevention System (IPS)**
Блокирование атак, аудит протоколов, защита от утечек данных
GX3002, GX4002, GX4004, GX5108, GX5208, GX6116

***Proventia* Server**
Агент защиты сервера
- Windows
- Linux Red Hat, SUSE

***RealSecure* Server Sensor**
- Windows
- Solaris
- AIX
- HP-UX

***Proventia* Desktop**
Многоуровневая защита рабочей станции:
- Firewall
- Virus Prevention System
- HIPS
- Buffer Overflow Protection
- Сигнатурный антивирус
- Application Control

Для получения более подробной информации посетите сайт: http://www.**ibm.com**/ru/services/iss/iss.html или отправьте запрос по адресу issru@ru.ibm.com

Контакты технических специалистов ISS в московском офисе IBM:

Денис Батранков,
batrankov@ru.ibm.com

Алексей Ивлев,
alexey.ivlev@ru.ibm.com

Алексей Строкин,
a-strokin@ru.ibm.com

IBM Восточная Европа/Азия

123317, Москва
Краснопресненская наб., 18
Тел.: +7 (495) 775-8800
Факс: +7 (495) 258-6468, 258-6404
ibm.com/ru/services/iss/iss.html