

Программное обеспечение EnCase[®] Enterprise Security

Руководство по дополнению инфраструктуры системы безопасности предприятия



Комплексная модель безопасности (The Comprehensive Security Model) системы безопасности включает пять основных компонентов, призванных обеспечить надежную защиту организации. Каждый из компонентов или процессов модели незамедлительно предоставляет данные другому компоненту/процессу, что позволяет непрерывно получать сведения о положении безопасности организации, а также осуществлять стратегию эффективной защиты.

Цель данного руководства – помочь разобраться в продуктах и решениях которые способствуют работе комплексной модели безопасности (The Comprehensive Security Model), а также понять, каким образом программное обеспечение EnCase Enterprise делает работу уже существующих наработок в области обеспечения безопасности более эффективной.

Данное руководство отвечает на следующие вопросы:

- В каких областях EnCase Enterprise может дополнять уже существующие наработки в сфере обеспечения защиты организации?
- Какие продукты (поименно) дополняет EnCase Enterprise?

Современный рынок предлагает огромное количество продуктов так или иначе предоставляющих возможность осуществлять один или несколько способов защиты. По этой причине в данном руководстве упоминаются решения, типично объединяемые в соответствии со стандартами отрасли или спецификацией поставщика, для каждого соответствующего раздела.

Оценка	Название марки продукта*	Каким образом EnCase® Enterprise дополняет Вашу существующую систему безопасности
Сканеры уязвимостей приложений (Application Vulnerability Scanners)	<ul style="list-style-type: none"> N-Stealth Web Server Analyzer AppSentry Oracle Application Server DominoScan Domino Server Scanner AppDetective for Web Applications and MySQL Kavado Web App 	<ul style="list-style-type: none"> Сканеры, выявляющие уязвимости в приложениях, ищут либо известные уязвимости, либо возможные известные сценарии которые послужили причиной уязвимостей в исходном коде приложения в прошлом. EnCase Enterprise подтверждает статический код, определенный сканером приложений, и проверяет сохранность кода, осуществляющего функционирование критически важных ресурсов организации.
Сканеры уязвимостей сети (Network Vulnerability Scanners)	<ul style="list-style-type: none"> Symantec NetRecon Nessus ISS Internet Scanner BindView HackerShield Axent NetRecon SARA SAINT 	<ul style="list-style-type: none"> Сканеры, выявляющие уязвимости в сети, предупреждают об известных уязвимостях и конфигурациях представляющих опасность для сети. Опираясь на реакцию операционной системы, сканеры уязвимостей в сети распознают функционирующие процессы, приложения и конфигурации. Полученная в результате анализа операционных систем, уровней пакетов обновлений, функционирующих приложений или текущих процессов передачи данных информация может быть обманчивой или неточной. EnCase Enterprise осуществляет анализ с точки зрения пользователя с целью выявить какие-либо запрещенные или приносящие вред программы, или несанкционированные процессы передачи данных. Программа также позволяет распознавать неизвестные или скрытые программы которые могут использовать уязвимости операционной системы. Данная операция осуществляется благодаря возможности анализировать профили машины пользователя (включая названия процессов и соответствующие им значения хэш-функции MD5), а также возможности распознавать руткиты (rootkits) на компьютерах с системой Windows.
Управляемые службы безопасности (Managed Security Services)	<ul style="list-style-type: none"> TruSecure Penetration Testing and Security Assessments 	<ul style="list-style-type: none"> Управляемые службы безопасности позволяют оценивать общий уровень безопасности в организации, используя известные и проверенные инструменты и методы. EnCase Enterprise позволяет определять протекающие неизвестные или вредоносные процессы, а также вредоносный или неизвестный код, находящийся в состоянии бездействия на сканируемом устройстве.

Защита	Название марки продукта*	Каким образом EnCase® Enterprise дополняет Вашу существующую систему безопасности
Корпоративные брандмауэры (Enterprise Firewalls)	<ul style="list-style-type: none"> Cisco PIX CheckPoint / Nokia FW-1 Juniper <NetScreen> Symantec Enterprise Firewall 	<ul style="list-style-type: none"> Стандартная функция брандмауэров заключается в осуществлении контроля над сетевым трафиком и регистрации нарушений политики сети, как имеющих место внутри организации, так и поступающих извне. EnCase Enterprise позволяет производить быстрый анализ, как в автоматическом порядке, так и с ручными настройками, компьютеров вовлеченных в процесс нарушения политики сети, параметры которой определяются настройками системы брандмауэров организации.
Корпоративные антивирусы (Enterprise Antivirus)	<ul style="list-style-type: none"> McAfee Antivirus Symantec Norton Antivirus Trend Micro OfficeScan Sophos PestPatrol 	<ul style="list-style-type: none"> Системы антивирусов занимаются поиском известных вирусов, червей и других вредоносных кодов, заражающих операционную систему посредством сопоставления известных сигнатур файлов и значений хеш-функций с подозрительным кодом. После обнаружения вредоносного кода антивирус, как правило, либо уведомляет об обнаруженной опасности, либо устраняет ее. EnCase Enterprise является единственным коммерческим решением, позволяющим находить и исправлять последствия работы руткитов действующих на базе Windows. EnCase осуществляет глубокий анализ операционной системы с целью обнаружения и уничтожения скрытых процессов и средств, используемых руткитами. Таким образом, выявляя эти скрытые процессы, EnCase служит дополнением к установленным антивирусам и системам защиты от вредоносных программ. Дескриптор приложений, наборы хэш-функций, профили и технология Snapshot EnCase Enterprise позволяют быстро выявить и устранить неизвестные вредоносные коды, которые невозможно обнаружить при помощи существующих антивирусных решений. Подобного рода программы использующие уязвимости системы и черви в большинстве случаев ускользают от антивирусных систем, так как они не совпадают с известными сигнатурами. EnCase служит дополнением к установленной системе антивирусного программного обеспечения предоставляя средства для быстрого выявления проблем, определения масштаба их распространения, источника возникновения, а также для устранения последствий на компьютерах подвергавшихся риску. Сразу после обнаружения неизвестного процесса EnCase Enterprise может в автоматическом порядке произвести анализ других компьютеров в организации с целью найти другие машины которые могли подвергаться атаке ранее обнаруженного червя или вредоносной программы.

Защита	Название марки продукта*	Каким образом EnCase® Enterprise дополняет Вашу существующую систему безопасности
Сканеры содержимого интернета, почты и сети (Web, Mail and Network Content Scanners)	<ul style="list-style-type: none"> • Websense • SmartFilter • Finijan SurfinGate • McAfee WebShield • VERICEPT 	<ul style="list-style-type: none"> • Сканеры содержимого сканируют послания электронной почты, страницы Интернета, другое содержимое сетевого трафика, а также приложения с целью обнаружить вредоносный код или содержимое запрещенного характера и предотвратить их попадание в организацию или выход за ее пределы. • Как только запрещенный процесс был обнаружен одной из перечисленных систем, EnCase Enterprise может произвести анализ компьютера и предоставить ключевую информацию (Интернет историю, данные кэш-памяти Интернет, поиск по ключевым словам) для подтверждения нарушений установленной политики и его источник.
Шифрование файлов, дисков и электронной почты (Encryption File, Disk & Email)	<ul style="list-style-type: none"> • PGP Disk • Pc Guardian Encryption+ • PGP mail • EFS • BestCrypt 	<ul style="list-style-type: none"> • Технологии шифрования позволяют пользователю обеспечивать защиту важной информации как внутри, так и за пределами организации. • Технологии шифрования также используются сотрудниками с целью скрыть информацию и инструменты которые могут использоваться для несанкционированной деятельности. • EnCase Enterprise позволяет сотрудникам отдела безопасности выявлять существование на компьютерах организации зашифрованных данных, которые могут противоречить политике корпорации. • EnCase Enterprise позволяет анализировать данные зашифрованные EFS как в автономных, так и в подтвержденных доменом системах. • EnCase Enterprise позволяет сотрудникам отдела безопасности просматривать и анализировать зашифрованные тома и логические накопители с целью определить открывались ли они подозреваемым во время проведения расследования.

Обнаружение	Название марки продукта*	Каким образом EnCase® Enterprise дополняет Вашу существующую систему безопасности
Системы выявления атак (Intrusion Detection Systems)	<p>Сетевые системы выявления атак (Network Intrusion Detection Systems)</p> <ul style="list-style-type: none"> • ISS RealSecure • Snort • Network Flight Recorder (NFR) • Axent NetProwler <p>Централизованные системы обнаружения вторжения (Host-based Intrusion Detection Systems)</p> <ul style="list-style-type: none"> • Zone Alarm • Cisco CSA • Symantec Host IDS 	<ul style="list-style-type: none"> • Система выявления атак предпринимает попытки обнаружить вредоносные процессы или нарушения политики организации в сегментах сети или хостах в пределах организации. Перечисленные системы могут базироваться как в сетевой инфраструктуре (как в случае с сетевыми системами выявления атак), так и в системах с конечным узлом, таким как клиентские рабочие станции и серверы (в случае с централизованной системой выявления атак). • EnCase Enterprise предоставляет возможность автоматического реагирования на происшествия, и также позволяет осуществлять эту функцию вручную. Совместно с установленной системой выявления атаки EnCase позволяет выявлять происшествия в режиме реального времени при помощи функции, известной как Snapshot, запуск которого происходит сразу после поступления сигнала тревоги. Незамедлительный анализ компьютера-источника и компьютера-цели предоставляет информацию об известных, неизвестных и скрытых процессах, открытых файлах, драйверах устройств, сервисах, данные протоколов TCP и другие данные позволяющие определить, осуществляется ли вторжение на компьютер, и виртуально устранить возможность ложных или ошибочных результатов. Автоматически срабатывающая сразу же после обнаружения происшествия функция Snapshot показывает последствия атаки во времени, таким образом, вы узнаете, имело ли происшествие место на самом деле и, если да, то каковы его источник и последствия. <p>Вы также можете использовать аналогичные возможности функции Snapshot для быстрого блокирования небезопасных процессов и осуществлять ответные действия вручную.</p> <ul style="list-style-type: none"> • После подтверждения того, что вредоносный процесс имел место, EnCase Enterprise может осуществлять автоматический анализ компьютеров во всей организации с целью обнаружить компьютеры, которые подвергались атаке того же червя или программы.
Верификаторы целостности системы (System Integrity Verifiers)	<ul style="list-style-type: none"> • TripWire • Data Sentinel 	<ul style="list-style-type: none"> • Верификаторы целостности системы генерируют значение для каждого файла и системы текущего контроля чтобы определить имели ли место, и когда, изменения файла или системы служащие признаком возможных несанкционированных доступов или вредоносных процессов. • EnCase Enterprise может осуществлять автоматическую проверку не только целостности статических файлов системы, но также протекающих в системе процессов. Программа может собирать дополнительную информацию из системного реестра, файловой системы, сети, чтобы определить имел ли место несанкционированный доступ к машине.

Обнаружение	Название марки продукта*	Каким образом EnCase® Enterprise дополняет Вашу существующую систему безопасности
Инструменты управления информацией систем безопасности (Security Information Management Tools)	<ul style="list-style-type: none"> • Arcsight • Symantec Incident Manager • NetIQ Security Manager • NetForensics • Intellitactics • neuSecure • Protego 	<ul style="list-style-type: none"> • Системы управления корреляцией и регистрацией событий собирают регистрационные записи и сигналы тревоги из различных систем и группируют их, устанавливая между ними корреляции чтобы определять потенциальные угрозы выявленные ранее и сократить общее число ошибочных результатов поиска. • EnCase Enterprise автоматически реагирует на различные типы сигналов тревоги и подтверждает возникновение опасности. Несмотря на то, что инструмент управления информацией систем безопасности осуществляет расширенную корреляцию среди множества систем чтобы сгенерировать сигнал тревоги, он не позволяет подтвердить с позиции целевого компьютера наличие угрожающего процесса и определить степень нанесенного ущерба. EnCase Enterprise предоставляет возможность осуществлять реакцию после того, как происшествие было идентифицировано.
Управляемые службы безопасности «обнаружение» (Managed Security Services "Detection")	<ul style="list-style-type: none"> • TruSecure IntelliShield Alert Manager • Symantec MSS • Guardent • Verisign 	<ul style="list-style-type: none"> • Управляемые службы обнаружения предоставляются сторонними поставщиками и служат для управления сигналами тревоги и регистрационными записями систем обнаружения угроз безопасности. Как и работу внутренних отделов безопасности, работу этих систем усложняют многочисленные ошибочные срабатывания. • EnCase Enterprise предоставляет возможность моментально проверить и отреагировать на происшествия выявленные управляемыми службами обнаружения в режиме «живой системы», что позволяет ценным корпоративным ресурсам оставаться в оперативном режиме в то время как производится оценка риска, которому подвергается организация.

Реагирование	Название марки продукта*	Каким образом EnCase® Enterprise дополняет Вашу существующую систему безопасности
Системы предотвращения вторжений (Intrusion Prevention Systems)	<ul style="list-style-type: none"> • NAI IntruShield • ISS RealSecure Guard • TippingPoint UnityOne • NetScreen IDP 	<ul style="list-style-type: none"> • Система предотвращения вторжений обнаруживает вредоносные действия или нарушения политики организации в сегментах сети или на хостах и предпринимает корректирующие действия, либо блокируя ячейки системы, либо обрывая сеанс, либо задавая новые параметры сеанса через сброс и повторные настройки протокола (режим реагирования). • EnCase Enterprise может определить удалось ли неизвестным угрозам избежать предпринятых системой предотвращения вторжений мер по защите, а также проверить явились ли ответные меры по защите целевого хоста, предпринятые системой предотвращения вторжений, успешными.
Управляемые ответные действия (Managed Response)	<ul style="list-style-type: none"> • Verisign • TruSecure Investigative Response 	<ul style="list-style-type: none"> • EnCase часто выполняет роль инструмента выбора службы управления ответных действий. Установка EnCase Enterprise позволит организации снизить затраты на управление ответными действиями, а также позволит осуществлять постоянный контроль за деятельностью сторонних поставщиков служб управления ответными действиями.
Управление инцидентами и автоматическое исправление (Incident Management and Automated Correlation)	<ul style="list-style-type: none"> • Symantec Incident Manager • NetIQ Security Manager 	<ul style="list-style-type: none"> • Системы управления инцидентами и автоматического исправления позволяют организации отслеживать все угрозы, которые имели место в прошлом, а также фиксировать последовательности действий, предпринятых с целью их устранения. • EnCase Enterprise является важным решением которое предоставляет вам необходимые сведения о том как происходила верификация угрозы, а также «профиль» вторжения в «живую систему» (то есть сведения о точке и последующем ходе вторжения) не прерывая работу критически важных ресурсов. Данная функция носит особую важность, так как предоставляет возможность сотруднику отдела безопасности более оперативно отреагировать в случае повторного вторжения. Без сведений, собранных EnCase Enterprise, большинство компаний следуют принципу - «вижу и исправляю», не раскрывая истинной природы вторжений. Это, в свою очередь, может послужить причиной неверных ответных действий и привести к очередному вторжению.