Trend Micro™

DEEP SECURITY™

Всесторонняя защита физических, виртуальных, облачных и гибридных сред

Виртуализация уже преобразила центры обработки данных, и сейчас организации все чаще перемещают свои рабочие нагрузки в частные и публичные облака. Если вы хотите воспользоваться преимуществами гибридных облачных вычислений, в первую очередь вам необходимо позаботиться о безопасности всех ваших серверов, будь то физическое, виртуальное или облачное устройство.

Кроме того, ваша система безопасности не должна влиять на производительность узла и плотность размещения виртуальных машин (ВМ), а также снижать рентабельность инвестиций в виртуализацию и облачные вычисления. Платформа Deep Security™ от компании Trend Micro™ обеспечивает комплексную безопасность в одном решении, специально предназначенном для виртуализованных и облачных сред, что позволяет устранить пробелы в безопасности или возможное негативное воздействие на производительность.

Защита от компрометации данных и перебоев в работе
Платформа Deep Security, доступная как в виде программного модуля, пакета для Amazon Web Services (AWS) или Microsoft® Azure™, так и в виде виртуализованной службы, предназначена для защиты вашего центра обработки данных и облачных рабочих нагрузок от компрометации данных и перебоев в работе. Deep Security помогает достичь соответствия нормативным требованиям, эффективно и экономически выгодно закрывая бреши в защите гибридных облачных сред.

Единая информационная панель для контроля нескольких средств безопасности
Deep Security содержит множество интегрированных модулей, включая защиту от вредоносных программ, проверку репутации веб-служб, межсетевой экран, модуль предотвращения вторжений, мониторинг целостности, управление приложениями и проверку журналов для обеспечения защиты серверов, приложений и данных в физических, виртуальных и облачных средах. Deep Security может быть развернут в виде единого многофункционального агента во всех средах, что упростит управление безопасностью благодаря единой панели управления всеми функциональными возможностями. В качестве информационной панели вы можете использовать решение Trend Micro Control Manager или стороннюю систему, например, VMware vRealize Operations, Splunk, HP ArcSight или IBM QRadar.

Полная интеграция обеспечивает единые политики для всех облачных сред.
Deep Security полностью интегрируется со всеми облачными платформами, включая рабочие нагрузки AWS, Azure и VMware®, что позволяет распространить политики безопасности центров обработки данных и на облачные рабочие нагрузки. Благодаря широкому спектру функциональных возможностей, оптимизированных для различных сред, Deep Security позволяет предприятиям и поставщикам услуг предоставлять своим пользователям дифференцированную и безопасную мультиарендную облачную среду.

Основные сложности у современных предприятий

Безопасность виртуальных рабочих столов
Сохранение показателей производительности и уровня консолидации благодаря комплексной системе защиты, оптимизированной для максимальной защиты сред VDI.

Виртуальные исправления ошибок
Своевременная защита от уязвимостей сокращает эксплуатационные расходы, связанные с экстренным устранением уязвимостей, частым выпуском исправлений и простоями в работе.

Соблюдение нормативных требований
Выполнение основных требований стандартов PCI DSS, HIPAA, NIST, SSAE16 и многих других.

> “Использование Deep Security позволило нам отказаться от другого антивирусного решения на наших серверах... Оно потребляло большой объем памяти и генерировало множество процессорных сбоев во время сканирования. А с Deep Security таких проблем у нас не возникает.”
>
> **Блейн Избель (Blaine Isbelle)**
> Системный администратор
> Технологии информационных услуг
> Калифорнийский университет в Беркли

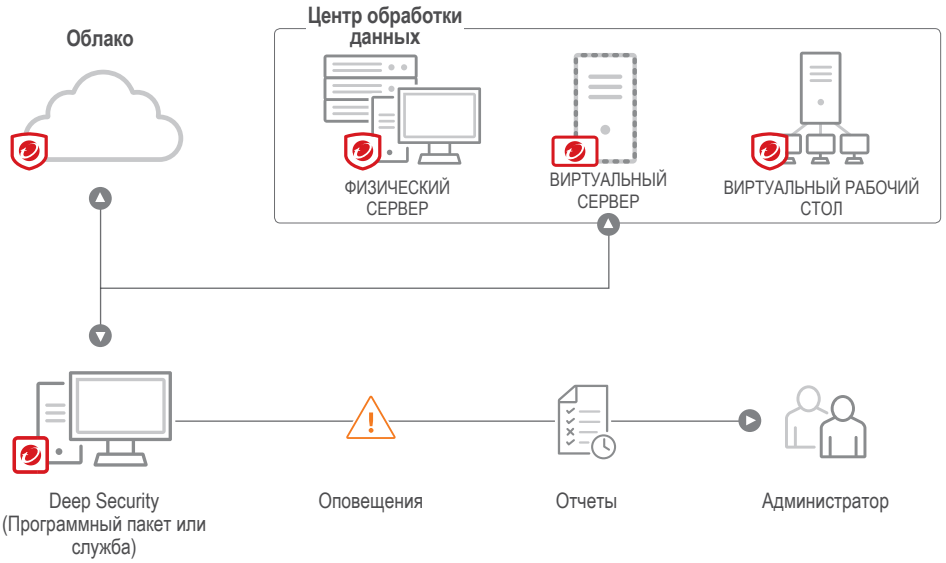
НАДЕЖНАЯ БЕЗОПАСНОСТЬ ГИБРИДНЫХ ОБЛАЧНЫХ СРЕД

Защита виртуальных сред
Deep Security защищает виртуальные рабочие столы и серверы от вредоносных программ нулевого дня, включая программы-вымогатели и сетевые атаки, одновременно минимизируя операционные расходы, связанные с неэффективным использованием ресурсов и экстренным устранением уязвимостей.

Защита облачных сред
Благодаря Deep Security поставщики услуг и руководители современных центров обработки данных могут предоставлять безопасную мультиарендную облачную среду с политиками безопасности, которые могут быть распространены на все облачные рабочие нагрузки и управляться централизованно в соответствии с контекстными политиками.

Интегрированная защита серверов
Deep Security объединяет все функции безопасности серверов в единую комплексную, интегрированную и гибкую платформу, которая оптимизирует защиту физических, виртуальных и облачных серверов.

СИСТЕМА БЕЗОПАСНОСТИ ГИБРИДНОЙ ОБЛАЧНОЙ СРЕД



ОСНОВНЫЕ ПРЕИМУЩЕСТВА

Действенность и эффективность

- Более эффективное использование ресурсов и управление при повышенной плотности развертывания ВМ по сравнению с традиционными антивирусными решениями.
- Дополнительная гибкость и возможности защиты благодаря единому, простому в управлении многофункциональному агенту.
- Исключительная производительность благодаря дедупликации сканирования на уровне гипервизора.
- Интеграция с облачными платформами, включая AWS, Microsoft Azure и VMware vCloud Air, что позволяет организациям управлять своими физическими, виртуальными и облачными серверами с помощью согласованных контекстных политик безопасности.
- Поддержка поставщиков услуг в плане предоставления клиентам безопасного общедоступного облака, изолированного от других арендаторов благодаря применению мультиарендной архитектуры.
- Предоставление услуг автоматического масштабирования, вычислительных ресурсов и самообслуживания для поддержки динамичных организаций, обслуживающих программно-определяемый центр обработки данных.
- Использование глубокой интеграции Deep Security с VMware для автоматического обнаружения новых виртуальных машин и применения контекстных политик для обеспечения целостной безопасности центра обработки данных и облачной среды.
- Интеграция с VMware vSphere 6 и NSX™. Расширение преимуществ микросегментации в программно-определяемых центрах обработки данных с помощью функций и политик безопасности, которые автоматически применяются к виртуальным машинам, где бы они ни находились.

Защита от компрометации данных и перебоев в работе

- Предотвращение запуска неизвестных приложений на наиболее важных серверах.
- Обнаружение вредоносных программ на виртуальных серверах и их устранение в режиме реального времени с минимальным снижением производительности.
- Обнаружение и блокирование несанкционированного программного обеспечения с контролем приложений.
- Защита от известных и неизвестных уязвимостей в корпоративных и веб-приложениях и операционных системах.
- Улучшенное обнаружение угроз и устранение подозрительных объектов с помощью анализа с использованием «песочницы».
- Отправка оповещений и инициация профилактических мер при обнаружении подозрительной или вредоносной активности.
- Отслеживание уровня доверия веб-сайтов и защита пользователей от зараженных сайтов с помощью анализа репутации веб-служб по глобальной базе данных репутации доменов компании Trend Micro.
- Выявление и блокировка взаимодействия с командными центрами (C&C) в бот-сетях и при направленных атаках с использованием аналитической информации об угрозах из глобальной базы данных репутации доменов компании Trend Micro.

Значительное снижение эксплуатационных затрат

- Отсутствие необходимости развертывать несколько программных клиентов и дополнительная экономия благодаря многоцелевому программному агенту или виртуальному устройству с централизованным управлением.
- Снижение сложности управления за счет тесной интеграции с панелями управления от Trend Micro, VMware, а также с корпоративными службами каталогов, включая VMware vRealize Operations, Splunk, HP ArcSight и IBM QRadar.
- Защита контейнеров Docker на узлах во всех средах с помощью предопределенных политик для безопасности узлов.
- Защита от уязвимостей, позволяющая осуществлять безопасное кодирование и экономичное внедрение незапланированных пакетов исправлений.
- Снижение затрат на управление безопасностью благодаря автоматизации требовательных к ресурсам рутинных задач, снижению количества ложных оповещений о безопасности и настройке четких процедур реагирования на инциденты.
- Значительное упрощение мониторинга целостности файлов с помощью облачных списков разрешенных и верифицированных событий.
- Обнаружение уязвимостей и программного обеспечения с помощью функции Recommendation Scanning («Рекомендуемое сканирование») для обнаружения изменений и защиты от уязвимостей.
- Повышение эффективности работы благодаря более динамичному и менее требовательному к ресурсам интеллектуальному агенту, который упрощает развертывание и оптимизирует распределение ресурсов между центром обработки данных и облачной средой.
- Соответствие уровня безопасности требованиям политик, что позволяет реализовывать определенные меры защиты с использованием меньшего количества ресурсов.
- Упрощенное администрирование благодаря централизованному управлению различными продуктами Trend Micro для обеспечения безопасности. Централизованное формирование отчетов по различным средствам безопасности, устраняющее необходимость создавать отчеты для отдельных продуктов.

Экономически эффективное соблюдение нормативных требований

- Соответствие основным требованиям стандартов PCI DSS, HIPAA, NIST, SSAE16 и многих других при помощи единого интегрированного и экономически эффективного решения.
- Доступные для аудита подробные отчеты, содержащие информацию о предотвращенных атаках и соблюдении политик.
- Сокращение времени и усилий, требующихся на подготовку к аудиту.
- Поддержка внутренних инициатив по обеспечению соответствия требованиям для усиления контроля.
- Проверенная технология, сертифицированная для Common Criteria EAL.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ DEEP SECURITY

Защита от вредоносных программ с проверкой репутации

- Интеграция с API-службами VMware vShield Endpoint для защиты виртуальных машин VMware от вирусов, шпионских, троянских и других вредоносных программ, скрывающих признаки присутствия.
- Защита от вредоносных программ физических, виртуальных и облачных серверов, включая среды AWS, Microsoft и VMware.
- Улучшенная производительность благодаря кэшированию и дедупликации VMware уровня ESX.
- Оптимизация работы системы безопасности, позволяющая избежать «антивирусных штормов», обычно наблюдаемых при полном сканировании системы и обновлениях шаблонов традиционными средствами безопасности.
- Защита от сложных атак в виртуальных средах путем изоляции вредоносных программ от целевой операционной системы и компонентов безопасности.
- Выявление и анализ подозрительных объектов с использованием «песочницы».
- Интеграция со средствами оценки репутации веб-служб Trend Micro™ Smart Protection Network™ для усиления мер защиты серверов и виртуальных рабочих столов.

Проверка журналов

- Сбор и анализ журналов операционной системы и приложений в более чем 100 форматах, выявление подозрительного поведения, событий безопасности и административных событий в масштабе всего центра обработки данных.
- Поддержка соответствия нормативным требованиям (PCI DSS, раздел 10.6) благодаря оптимизации выявления важных событий безопасности в многочисленных записях журналов.
- Передача сведений о событиях в систему SIEM или на централизованный сервер регистрации для сопоставления, формирования отчетов и архивации.

Предотвращение вторжений

- Проверка всего входящего и исходящего трафика на отклонения от протокола, нарушения политик или наличие содержимого, свидетельствующего об атаке.
- Автоматическая защита от известных, но неисправленных уязвимостей путем установки виртуального пакета исправлений (виртуальной защиты) от неограниченного количества эксплойтов на несколько тысяч серверов за считанные минуты без перезагрузки системы.
- Поддержка соответствия нормативным требованиям (PCI DSS, раздел 6.6) для защиты веб-приложений и данных, которые они обрабатывают.
- Защита от SQL-инъекций, межсайтового скриптинга и других уязвимостей веб-приложений.
- Встроенная защита от уязвимостей для всех основных операционных систем и более чем 100 приложений, в том числе баз данных, веб-серверов, почты и FTP-серверов.
- Модуль предоставляет более подробную информацию о приложениях, получающих доступ к сети, и обеспечивает более полный контроль над ними.

Двунаправленный межсетевой экран на базе узла

- Уменьшение поверхности атаки физических, облачных и виртуальных серверов путем тщательной фильтрации, применения индивидуальных политик для каждой сети и данных о местоположении для всех IP-протоколов и типов фреймов.
- Централизованное управление политикой серверного межсетевого экрана, включая создание шаблонов для общих типов серверов.
- Предотвращение атак типа «отказ в обслуживании» и обнаружение признаков зондирования.
- Протоколирование событий межсетевого экрана на узле для формирования отчетов о соответствии нормативным требованиям и в целях аудита, что особенно важно при развертывании публичных облачных сред.

Мониторинг целостности

- Обнаружение вредоносных или неожиданных изменений системных файлов и файлов приложений, включая каталоги, разделы и значения реестра, и отправка уведомлений о них в режиме реального времени.
- Дополнительная защита и контроль соответствия нормативным требованиям на уровне гипервизора за счет применения технологии Intel TPM/TXT для мониторинга целостности гипервизора от любых несанкционированных изменений.
- Снижение административных расходов благодаря функции назначения тегов для разрешенных событий, которая автоматически реплицирует действия для схожих событий в рамках всего центра обработки данных.
- Упрощенное администрирование за счет значительного сокращения количества известных разрешенных событий с помощью автоматической проверки по облачному белому списку службы Trend Micro™ Certified Safe Software Service.

Контроль приложений

- Автоматическое обнаружение и блокирование несанкционированных программ.
- Сканирование компьютеров и определение имеющихся приложений.
- Блокирование системы после создания списка ресурсов, предотвращая тем самым запуск новых приложений без внесения их в белый список.
- Интеграция со средой DevOps для поддержки непрерывных изменений стеков приложений, одновременно защищая функции контроля приложений с помощью API.
- Обнаружение угроз, которые еще не имеют сигнатур, включая некоторые угрозы нулевого дня.

АРХИТЕКТУРА

Виртуальное устройство Deep Security Virtual Appliance. Прозрачное применение политик безопасности на виртуальных машинах VMware vSphere. Виртуальное устройство обеспечивает защиту от вредоносных программ, выполняет проверку репутации веб-служб, предотвращает вторжения, отслеживает целостность файлов, а также защищает с помощью межсетевого экрана без использования агентов в средах VMware NSX. В средах, не относящихся к NSX, можно использовать комбинированный режим, когда виртуальное устройство используется для защиты от вредоносных программ и мониторинга целостности файлов без установленного агента, а функции предотвращения вторжений, контроля приложений, межсетевого экрана, проверки репутации веб-служб и проверки журналов выполняет агент.

Агент Deep Security Agent. Небольшой программный компонент развертывается на защищаемом сервере или на виртуальной машине (может быть автоматически развернут с использованием ведущих инструментов управления, таких как Chef, Puppet и AWS OpsWorks) и обеспечивает применение политик безопасности центра обработки данных, включая функции контроля приложений, защиты от вредоносных программ, предотвращения вторжений, межсетевого экрана, мониторинга целостности и проверки журналов.

Диспетчер Deep Security Manager. Мощная централизованная панель управления позволяет осуществлять детальный контроль благодаря использованию ролевой модели администрирования и многоуровневому наследованию политик. Функции автоматизации задач, такие как Recommendation Scan («Сканирование по рекомендации») и Event Tagging («Присвоение тегов событиям»), упрощают администрирование безопасности. Мультиарендная архитектура позволяет изолировать политики отдельных арендаторов и делегировать управление безопасностью их собственным администраторам.

Анализ глобальной информации об угрозах. Платформа Deep Security интегрируется с Smart Protection Network для обеспечения защиты от возникающих угроз в режиме реального времени, непрерывно оценивая и сопоставляя глобальную информацию об угрозах и данные о репутации для веб-сайтов, источников электронной почты и файлов.

Deep Security Scanner — это модуль, предназначенный для защиты систем SAP путем интеграции с интерфейсом NetWeaver Virus Scan

SAP Partner

СЕРТИФИКАЦИЯ ДЛЯ ПАРТНЕРОВ УРОВНЯ CSP

Trend Ready для поставщиков облачных служб — это глобальная программа тестирования, с помощью которой поставщики облачных служб могут проверить и подтвердить совместимость своих решений с передовыми продуктами компании Trend Micro для защиты облачных сред

РАЗВЕРТЫВАНИЕ И ИНТЕГРАЦИЯ

Быстрое развертывание: воспользуйтесь преимуществами имеющейся информационной инфраструктуры и систем безопасности

- Программное обеспечение агента может быть с легкостью развернуто с помощью стандартных механизмов распространения ПО, таких как Chef, Puppet, AWS OpsWorks, Microsoft System Center Configuration Manager (SCCM), Novell ZENworks и Symantec Deployment Solution.
- Подробные данные о событиях в системе безопасности на уровне сервера предоставляются SIEM-системе (включая HP ArcSight, Intellitactics, IBM QRadar, NetIQ, RSA Envision, Q1Labs, Loglogic и другие системы) с помощью нескольких вариантов интеграции.
- Интеграция с корпоративными службами каталогов, включая Microsoft Active Directory

СИСТЕМНЫЕ ТРЕБОВАНИЯ
Microsoft® Windows®
• Windows XP, Vista, 7, 8, 8.1, 10 (32- и 64-разрядные версии)
• Windows Server 2003 (32- и 64-разрядные версии)
• Windows Server 2008 (32- и 64-разрядные версии), 2008 R2, 2012, 2012 R2, 2012 Server Core (64-разрядная версия), 2016 (64-разрядная версия), 2016 Server Core (64-разрядная версия)
• XP Embedded (32- и 64-разрядные версии)[1]
Linux[2]
• Red Hat® Enterprise 5, 6, 7 (32- и 64-разрядные версии)[3]
• SUSE® Enterprise 10, 11, 12 (32- и 64-разрядные версии)[3]
• CentOS 5, 6, 7 (32- и 64-разрядные версии)[5]
• Ubuntu 12, 14, 16 (64-разрядная версия, только LTS) [4, 5]
• Oracle Linux 5, 6, 7 (32- и 64-разрядные версии)[4, 5]
• CloudLinux 5, 6, 7 (32- и 64-разрядные версии)[2,4]
• Amazon Linux (32- и 64-разрядные версии)[4, 5]
• Debian 6, 7 (64-разрядная версия)[2,4]
Oracle Solaris™ 6, 7
• OS: 10, 11 (64-разрядная версия SPARC), 10, 11 (64-разрядная версия x86)[7, 8]
• Super Cluster через поддерживаемые операционные системы Solaris.
UNIX6
• AIX 5.3, 6.1, 7.1 on IBM Power Systems[7, 8]
• HP-UX 11i v3 (11.31)[7, 9]
VIRTUAL
• VMware® vSphere: 5.5/6.0, View 4.5/5.0/5.1, ESX 5.5, 6.2.X, 6.5, NSX 6.2.X, 6.3
• Citrix®: XenServer[11]
• Microsoft®: HyperV[11]

[1] Из-за возможности индивидуальных настроек в Windows XP Embedded мы рекомендуем нашим клиентам проверить активность служб и портов, необходимых для запуска агента Deep Security, чтобы гарантировать правильность работы системы в их средах.
[2] Для получения списка поддерживаемых ядер см. документацию.
[3] Поддержка защиты SAP доступна только в системе Red Hat 6 (64-разрядная версия) и SUSE 11 (64-разрядная версия) на стороне агента. Для правильной работы функции защиты SAP модуль защиты от вредоносных программ должен быть активирован на стороне агента.
[4] Защита от вредоносных программ поддерживает только режим сканирования по требованию.
[5] Для получения списка поддерживаемых версий см. примечания к последнему выпуску.
[6] Мониторинг защиты от вредоносных программ и проверки репутации веб-служб не поддерживается.
[7] Поддерживается агентами версии 9.0.
[8] Защита от вредоносных программ не поддерживается.
[9] Только функции проверка журналов и мониторинг целостности.
[10] Система vCloud Networking and Security поддерживает защиту от вредоносных программ и мониторинг целостности файлов без установленного агента.
[11] Защита только с помощью агента Deep Security Agent.

НА ОСНОВЕ ТЕХНОЛОГИИ XGEN™ SECURITY

Deep Security является частью решения Trend Micro Hybrid Cloud Security на основе технологии XGen™.

Основные сертификаты и партнеры

- Amazon Advanced Technology Partner
- Certified Red Hat Ready
- Сертификат Cisco UCS
- Common Criteria EAL 2+
- Сертификат EMC VSPEX
- HP Business Partnership
- Microsoft Application Protection Program
- Microsoft Certified Partnership
- Сертификат NetApp FlexPod
- Oracle Partnership
- PCI Suitability Testing для HIPS (NSS Labs)
- SAP Certified (NW-VSI 2.0 и HANA)
- Сертификат VCE Vblock
- Виртуализация VMware

awsmarketplace

vmware

Microsoft Azure

TREND MICRO READY

TREND MICRO™

Securing Your Journey to the Cloud