Trend Micro

CONTROL MANAGER™

Централизованный мониторинг и управление политиками для защиты данных и предотвращения угроз

В нынешнем многослойном ландшафте угроз сложные атаки осуществляются по многим направлениям, затрагивая конечные устройства, серверы, сети, веб-службы и электронную почту пользователей. Все уровни безопасности должны быть как на ладони для наилучшей защиты организации. С переходом к облачным моделям доставки ИТ-сервисов система безопасности требует управления на местах, в облаке и гибридных средах.

Единая система управления безопасностью поможет устранить ИТ-барьеры, часто разделяющие эшелоны защиты и модели развертывания. Такой централизованный подход улучшает мониторинг, снижает сложность и исключает лишние и рутинные задачи при администрировании. Все это усиливает защиту вашей организации и делает жизнь легче.

Решение Trend Micro™ Control Manager™ для централизованного мониторинга и управления предоставляет единый интегрированный интерфейс для управления, контроля и отчетности на всех уровнях безопасности, а также в моделях развертывания, таких как SaaS и на местах. Настраиваемые информационные панели полностью отражают текущую ситуацию, благодаря чему появляется возможность быстрой оценки состояния, выявления угроз и оперативной реакции на инциденты. Ориентированная на пользователя система мониторинга (в основе которой — интеграция со службами Active Directory) позволяет видеть, что происходит на всех конечных устройствах, личных устройствах отдельных пользователей, а также в их интернет-трафике и электронной почте. Благодаря этому появляется возможность корректировки настроек и внесения изменений во все способы взаимодействия пользователя с сетью.

Если угроза действительно проникла в среду, потребуется абсолютная видимость всех уровней, чтобы отследить ее распространение. Благодаря лучшему пониманию событий в системе безопасности вы сможете лучше подготовиться, чтобы не допустить повторения подобного в будущем. Прямое подключение к базам данных Trend Micro Threat Connect обеспечивает доступ к полезной аналитической информации об угрозах, с помощью которой появляется возможность исследовать сложные связи между вредоносными программами, их разработчиками и методами распространения.

Продукты Trend Micro с поддержкой Control Manager

ЗАЩИТА ГИБРИДНЫХ ОБЛАЧНЫХ СРЕД

- Deep Security

ЗАЩИТА СЕТИ

- Deep Discovery Inspector
- Deep Discovery Analyzer
- Deep Discovery Email Inspector
- Tipping Point

ЗАЩИТА ПОЛЬЗОВАТЕЛЕЙ

- OfficeScan™
- Worry-Free™ Business Security
- Endpoint Encryption
- Endpoint Application Control
- Endpoint Sensor
- Security for Mac
- Vulnerability Protection
- Data Loss Prevention
- Mobile Security
- InterScan™ Messaging Security
- ScanMail™
- Hosted Email Security
- PortalProtect
- InterScan™ Web Security
- Cloud App Security

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

Простой и непрерывный сквозной мониторинг всего предприятия

Ведите постоянный мониторинг и быстро вникайте в ситуацию в системе безопасности, выявляйте угрозы и реагируйте на инциденты — текущее состояние вашей среды ежеминутно обновляется и оценка будет всегда актуальна. В случае атаки вы сможете изучить, насколько сильно она распространилась.

- Интуитивно понятный, настраиваемый интерфейс позволяет увидеть ситуацию в эшелонах системы защиты и устройствах пользователей, а также углубленно изучить необходимую вам более детальную информацию.
- Информационные панели системы безопасности позволяют администраторам задавать приоритет критическим угрозам, важным пользователям или конечным устройствам, позволяя таким образом решать сначала наиболее важные проблемы.
- Настраиваемые информационные панели и отчеты, специфичные запросы и оповещения дают полезную информацию, необходимую как для защиты, так и для соблюдения нормативных требований.
- Интеграция с вашим центром обеспечения безопасности (SOC) осуществляется посредством бесшовной интеграции с ведущими решениями для управления событиями информационной безопасности.
- Предустановленные шаблоны отчетов и настраиваемые отчеты SQL облегчают соблюдение внутренних нормативных требований.

Connected Threat Defense для улучшения защиты

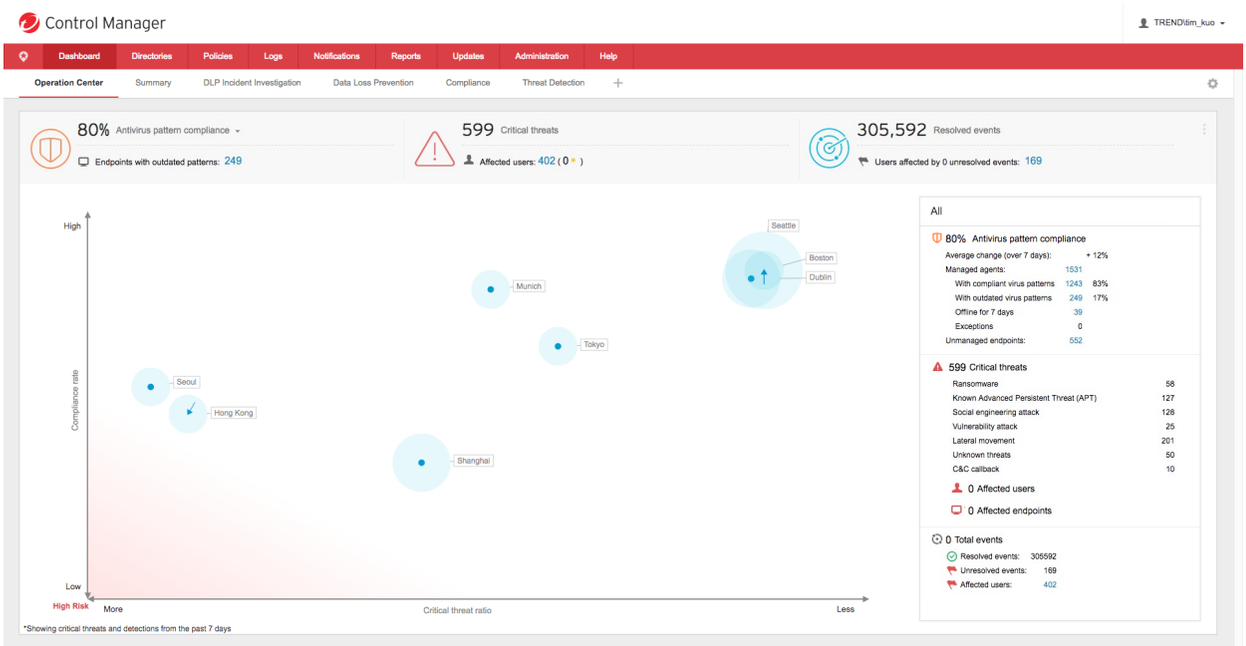
Интегрированное управление и анализ безопасности на всех уровнях защиты крайне важны для защиты от сложных угроз, распространяемых по различным векторам.

- Единая централизованная панель обеспечивает постоянное принудительное применение политик и позволяет выявлять проникновения в сеть, задавать настройки и управлять защитой от угроз и безопасностью данных на всех уровнях: конечных устройствах, мобильных устройствах, при обмене сообщениями, при совместной работе, в веб-сервисах, облаке и центре обработки данных.
- Система Connected Threat Defense позволяет Control Manager обнаруживать подозрительные объекты, которые могли прийти от любого количества локальных векторов угроз, а также предоставляет обновления для быстрого реагирования другим локальным решениям, тем самым ускоряя защиту и уменьшая распространение вредоносных программ и других угроз.
- Реагирование и всесторонне изучение угроз позволяет проследить распространение угрозы в организации в хронологическом порядке и найти полную информацию о ситуации, временной последовательности и параметрах атаки, благодаря чему на нее можно быстро отреагировать.
- Прямое подключение к базам данных Trend Micro Threat Connect обеспечивает доступ к полезной глобальной информации об угрозах. Например, к подробным сведениям об угрозах, которые описывают характерные модели поведения — действия в сети и изменения в системе, а также глобальные, системные и региональные последствия.
- База знаний Trend Micro предлагает рекомендации по восстановлению и предотвращению атак.

Мониторинг, ориентированный на пользователя

Централизованный режим просмотра позволяет проводить мониторинг всех уровней (независимо от модели развертывания — локально или в облаке), а значит, нет необходимости переключаться с одной панели на другую.

- Оптимизированное администрирование системы безопасности позволяет управлять защитой от угроз и безопасностью данных наконечных устройствах, серверах, в сети, на мобильных устройствах, при обмене сообщениями, совместной работе и в интернете через единый консолидированный интерфейс.
- Интеграция со службой Active Directory упрощает использование информационных панелей благодаря базам данных на основе сайта или раздела AD.
- Ориентированный на пользователя режим просмотра позволяет легко управлять безопасностью на всех типах устройств: администратор получает возможность развернуть и просмотреть статус политики для каждого конечного устройства, принадлежащего конкретному пользователю независимо от типа исполнения (настольное или мобильное устройство).



В информационных панелях, отображающих меры безопасности, используются инновационные теплокарты (в основе которых — сайты или разделы Active Directory). С их помощью можно следить за соблюдением нормативных требований и критическими угрозами, что наиболее важно для администраторов ИТ-структур и систем безопасности.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

ТРЕБОВАНИЯ К СЕРВЕРНОМУ ОБОРУДОВАНИЮ
• Процессор: Мин.: Intel™ Core™ i5 с 2,3 ГГц или совместимый; 64-разрядный процессор AMD™ или Intel
• Память: не менее 8 ГБ оперативной памяти
• Свободное дисковое пространство: не менее 80 ГБ (жесткий диск с интерфейсом SAS)

ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ
Операционная система
• Microsoft™ Windows™ Server 2008 Standard/Enterprise Edition с пакетом обновлений 2 (SP2)
• Windows Server 2008 (R2), Standard/Enterprise/Datacenter Edition с пакетом обновлений 1 (SP1)
• Windows Server 2012 Standard/Datacenter Edition (64-разрядная версия)
• Windows Server 2012 (R2) Standard/Datacenter Edition (64-разрядная версия)
• Windows Server 2016 Standard/Datacenter Edition (64-разрядная версия)
Веб-консоль
• Процессор: Intel™ Pentium™ с частотой 300 МГц или аналогичный
• Оперативная память: не менее 128 МБ
• Свободное дисковое пространство: не менее 30 МБ
• Браузеры: Microsoft Internet Explorer™ 11, Microsoft Edge™, Google Chrome (Примечание: при использовании Internet Explorer или Edge отключайте «Просмотр в режиме совместимости»)
• Другие: монитор с разрешением 1366 x 768 и качеством цветопередачи в 256 цветов или более | Adobe™ Flash™ 8 или более поздней версии
Программное обеспечение для баз данных
• SQL Server 2008 Express с пакетом обновлений 2 (SP4)
• SQL Server 2008 (R2) Standard/Enterprise с пакетом обновлений 3 (SP3)
• SQL Server 2008 Standard/Enterprise с пакетом обновлений 2 (SP4)
• SQL Server 2012 Express с пакетом обновлений 2 (SP3)
• SQL Server 2012 Standard/Enterprise с пакетом обновлений 2 (SP3)
• SQL Server 2014 Express с пакетом обновлений 2 (SP2)
• SQL Server 2014 Standard/Enterprise с пакетом обновлений 2 (SP2)
• SQL Server 2016 Express с пакетом обновлений 1 (SP1) или без него
• SQL Server 2016 Standard/Enterprise с пакетом обновлений 1 (SP1) или без него
Поддержка виртуализации
Control Manager обеспечивает поддержку виртуальных платформ, поддерживаемых установленной операционной системой

Ключевые преимущества

- Улучшает мониторинг благодаря панелям управления с инновационными теплокартами, отражающими меры безопасности.
- Упрощает администрирование благодаря единой панели управления для политик безопасности.
- Повышает эффективность защиты данных за счет встроенного модуля защиты от утечек данных (DLP) во всей ИТ-инфраструктуре с единым набором шаблонов правил фильтрации.
- Снижает риски при помощи консолидированных обновлений и оповещений системы безопасности и объединенной защиты от угроз, обеспечивая обмен данными между уровнями безопасности.
- Снижает затраты на управление безопасностью благодаря экономии времени и уменьшению рабочей нагрузки на ИТ-отдел.

TREND MICRO™

Securing Your Journey to the Cloud