



LANDesk® Security Suite

Активное управление безопасностью конечных систем

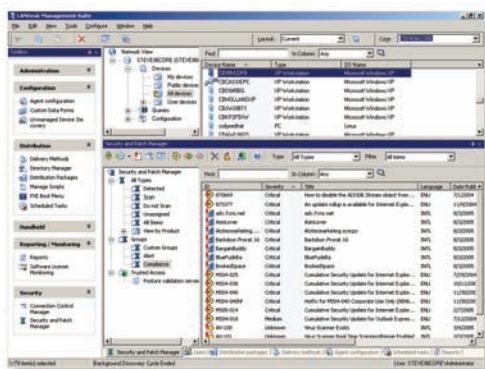
«Когда мы впервые провели анализ поставщиков, самым существенным качеством, которое произвело на нас большое впечатление, была полная интегрируемость продукта LANDesk® Security Suite. В масштабе всего рынка, это было единственное решение, в котором функции управления обновлениями действительно интегрированы с функциями управления безопасностью – в единой, экономически эффективной менеджерской консоли.

... LANDesk Security Suite не только обеспечивает нам предельно ясное понимание степени внедрения патчей, но также теперь мы часто можем достигать их полного внедрения за одну ночь, вместо того, чтобы тратить на это многие дни.»

Джо Риесберг (Joe Riesberg)
Менеджер безопасности и соответствия IT
VCPI

“LANDesk позволяет нам постоянно содержать наши машины в обновленном, согласованном и защищенном состоянии.»

Эдвард Скафф (Edward Skaff)
Менеджер Exempla Healthcare



LANDesk® Security Suite идет дальше простого блокирования – к поддержке мощного функционала обеспечения безопасности конечной системы. Встроенная технология LANDesk® Network Access Control (ранее LANDesk® Trusted Access™) позволяет блокировать и оперативно исправлять устаревшие и непрошедшие обновления среды на компьютерах, снижать риски простоев и заражения вредоносным ПО. Когда машины подключаются к сети, другая встроенная технология — Connection Control Manager (менеджер управления соединениями) — диагностирует систему на соответствие политикам, перед тем как предоставить ей доступ. Далее, LANDesk Network Access Control действует как ловушка для тех неуправляемых систем или гостей в сети, которые могут не соответствовать обязательным политикам. Этот двухсторонний подход обеспечивает непрерывность бизнеса, так как и политики и соответствия стандартам проверяются перед тем, как разрешить подключение к корпоративной сети.

Активная защита конечных систем в корпоративных IT-средах

На современных предприятиях защита данных является одной из наиболее важных задач. Рост разрушительных атак может, в итоге, стоить Вашей организации бесконечных часов и средств на восстановление и приведение в порядок систем, на построение эффективной защиты.

Из последнего исследования Gartner следует, что к концу 2007 года, 75% предприятий будут инфицированы необнаруженным вредоносным ПО, атаковавшим их традиционные периметры безопасности и средства защиты. Агрессивная среда меняется. Финансово мотивированные целевые атаки учащаются, а автоматизированные пакеты позволяют быстро и легко создавать тысячи программных вариаций агрессивного кода. Процессы же и технологии, обеспечивающие защиту, не успевают за этим темпом. Для того, чтобы защита была действительно эффективной, построение сетевой безопасности должно начинаться с фундамента — уровня индивидуального устройства, с защищенными конфигурациями и политиками доступа. LANDesk предоставляет технологии, необходимые для того, чтобы не проиграть в соревновании с современными средствами агрессии.

LANDesk® Security Suite: Спокойствие и удобство единой консоли

LANDesk® Security Suite позволяет автоматически обнаруживать и устанавливать защитные обновления, пользуясь активными средствами управления безопасностью, управляемыми с единой консоли. Прибегнув к этому решению, можно:

- Снизить риски простоя сети и расходы на работу службы поддержки, защитит важные данные и производительность пользователей, обезопасив их от разрушительных атак на уровне конечной системы.
- Ужесточить практику исполнения политик безопасности, заранее определяя и автоматически устраняя потенциальные угрозы.
- Экономить время и сокращать потребности в ресурсах, автоматизируя процесс устранения уязвимостей путем назначения правил и политик безопасности, и организуя частые сканирования систем на соответствие им.
- Защитить системы и важные данные посредством активного контроля за доступом к коммуникациям, портам и носителям информации, с возможностью постановки устройств на карантин.
- Легко привести работу IT-систем в соответствие с корпоративными политиками безопасности. В один прием устанавливая правила защиты, гарантирующие, что все системы в масштабе сети защищены и приведены в соответствие им.
- Осуществлять более глубокий контроль за утечками информации, включающий шифрование, блокирование портов USB, и функции контроля над операциями чтения /записи CD/ DVD. Что позволяет действительно контролировать наиболее важные коммерческие данные.
- Форсировать эффективность и сокращать затраты, посредством мощного, действенного процесса управления патчами, который может быть автоматизирован с помощью функции параллельного обновления, имеющейся в LANDesk® Process Manager.
- Демонстрировать эффективность инвестиций в проекты по обеспечению безопасности с помощью детализованных отчетов.

LANDesk Security Suite обеспечивает централизованное управление и защиту IT активов с единой интегрированной консоли — предоставляя возможность повысить защищенность

Защита предприятия

С LANDesk® Security Suite, сокращаются простои сети, сокращаются затраты на техническую поддержку, осуществляется защита важных корпоративных данных и гарантируется производительность пользователей.

Также, применение технологии LANDesk® Network Access Control в LANDesk Security Suite позволяет предотвратить само подключение инфицированных или незащищенных систем к корпоративной сети. Вы контролируете стандарты соответствия и внедряете политики безопасности, которым конечные устройства должны соответствовать, перед тем, как они получают доступ, и все время, пока они остаются в сети — снижая риски простоев, создаваемые инфицированными машинами или вредоносными проникновениями.

Обнаружение и исправление

Стандартное частое сканирование уязвимостей, производимое LANDesk® Security Suite, позволяет определять, какие обновления срочно требуются для антивирусов, ОС и приложений — на основании Ваших требований и выбранного уровня детализации. Настраиваемое сканирование позволяет назначать специфические условия, по которым будет производиться проверка. Также, анализатор угроз позволяет легко определять конфигурационные риски.

Функции защиты от шпионского ПО защищают системы от атак в реальном времени, с доступом к регулярно обновляемой, обширной базе данных LANDesk известных шпионских, рекламных программ, троянов, сканеров клавиатуры и другого вредоносного ПО. Уведомления в реальном времени позволяют без усилий находиться на высоте требований к безопасности, с учетом новых издаваемых подписей вредоносного ПО, их типов и степеней опасности — так что команда IT может сконцентрировать свои усилия на иных задачах.

Менеджер управления соединениями Connection Control Manager ограничивает доступ к сети, допуская только авторизованные сети или IP-адреса, или блокирует соединения с определенными сетями. Вы контролируете доступ к дискам, каналам связи, портам и модемам, что помогает предотвратить потерю и кражу данных, и защищает от несанкционированного доступа.

Блокировка приложений автоматически предотвращает запуск запрещенных программ. Возможно блокирование приложений, находящихся в обширном списке LANDesk Security Suite, а также можно создавать собственные определения.

Система предотвращения утечки данных повышает уровень контроля над портативными устройствами и уровень защиты ключевых корпоративных данных. Имеется возможность активизировать политики, ограничивающие USB накопители, CD и DVD работой в режиме «только чтение». Вся файловая информация, переданная на устройство хранения USB, автоматически кодируется. Вы можете контролировать подключения к беспроводным сетям, обнаруживая и классифицируя все не одобренные точки доступа (WAP).

Встроенные средства управления антивирусами позволяют управлять выбранным Вами антивирусным решением, активизировать и конфигурировать межсетевые экраны Microsoft XP или Vista напрямую с консоли LANDesk Security Suite. И, пользуясь возможностью LANDesk Security Suite настраивать конфигурацию межсетевого экрана отдельных систем или групп. Можно назначать свои особые политики безопасности отдельным ролям, или, исходя из планируемого использования, конкретным устройствам. Политики управления межсетевым экраном также позволяют назначать различные правила для каждой системы, в зависимости от интерфейса и типа сети, к которой подключены пользователи.

Функции управления обновлениями помогают устанавливать патчи, необходимые для ОС и приложений, быстро находить и назначать приоритеты, автоматизировать их распространение и поддержку. Технология LANDesk® Targeted Multicast™ позволяет ускорять внедрение патчей на множество целевых систем, сокращая нагрузку на полосу пропускания и экономя общий сетевой трафик, без использования выделенного оборудования или реконфигурирования маршрутизаторов.

Также, автоматический процесс внедрения обновлений LANDesk позволяет кэшировать патчи на компьютерах. Когда возникает необходимость их установки, достаточно просто выбрать требуемые из них для исполнения, немедленно защищая ими системы. Без усилий автоматизируйте этот процесс, включив LANDesk® Process Manager Automated Patch Deployment. Назначьте новые обновления для автоматической установки, и включите эту задачу в текущий процесс.

Поддержка и демонстрация соответствия политикам безопасности

Решение для идентификации и устранения угроз делает простой задачей поддержания соответствия требованиям безопасности. Вместо того, чтобы оставлять задачу борьбы со шпионским ПО и решение других проблем конечным пользователям, специалисты по безопасности контролируют, кто имеет доступ к чему-либо, а кто нет. Имеется возможность один раз установить корпоративные политики безопасности, и быть уверенным, что все устройства в масштабе сети защищены и приведены в соответствие, и что все компьютеры, подключающиеся к сети, не привнесут в нее хаоса. А средства базового конфигурирования позволяют контролировать, кто обладает возможностью изменять политики безопасности.

LANDesk® Security Suite позволяет без труда отслеживать и отображать экономическую эффективность работ по организации и поддержанию безопасности. Он имеет множество опций для генерации отчетов. Детальные исторические отчеты по применению политик безопасности и установке обновлений отображаются в удобном для восприятия графическом формате, позволяющем ясно продемонстрировать прогресс применения политик безопасности. Вы можете легко просматривать, из чего состоят Ваши политики безопасности, и быстро обнаруживать пользователей, чьи привычки поведения в Интернете являются постоянным источником угрозы для Вашей сети со стороны шпионского ПО. А индикаторная панель LANDesk® обеспечивает единый графический вид всех существенных параметров, критичных для работы предприятия.



С помощью линейки интегрированных решений LANDesk, Вам предоставляется возможность выбирать, как и когда углублять уровень контроля над системами и безопасностью. Начинаете ли Вы с одного решения или нескольких, они все гладко работают вместе, обладая единым интуитивным интерфейсом управления и обеспечивая свободу функционирования всем решениям в любое время.

	LANDesk® Suite	LANDesk® Antivirus	LANDesk® Management Suite	LANDesk® Patch Manager	LANDesk® Host Intrusion Prevention
Активное управление безопасностью конечных систем	x				
Возможность идентифицировать и ставить на карантин не обновленные компьютеры, или те, обновления на которых устарели	x				
Активный контроль над коммуникациями, портами и доступом к средствам хранения	x				
Антивирусная защита уровня предприятия		x			
Поддержка антивирусов McAfee, Norton, Sophos, Symantec и Trend-Micro	x	x			
Возможность обнаруживать и удалять шпионское ПО, рекламное ПО, трояны, сканеры клавиатуры и иное вредоносное ПО	x				x
Технология обнаружения базовых корневых уязвимостей для установок определенных уязвимостей и создания пакетов или политик их устранения	x		x	x	
Аппаратное и программное управление сложными сетевыми средами			x		
Защита от угроз «дня ноль» и целевых атак					x
Контроль над приложениями и ведение белых списков					x
Автоматизированная оценка уязвимостей, их устранение и текущее управление патчами	x			x	

Примечание: LANDesk Security Suite включает функционал LANDesk Patch Manager, который также может применяться и отдельно, либо с LANDesk Management Suite, или быть расширен до полнофункционального LANDesk Security Suite. LANDesk Antivirus и LANDesk Host Intrusion Prevention могут быть использованы в качестве расширений к LANDesk Security Suite или LANDesk Management Suite.

Ключевые свойства

Возможности управления сетевым доступом

- Обнаружение и постановка на карантин управляемых и неуправляемых компьютеров с устаревшим или не обновленным ПО — посредством LANDesk® Network Access Control.
- Совместимость функционала доступа к сети Cisco и LANDesk DНСР.

Усовершенствованные функции обнаружения уязвимостей

- Запуск стандартных, специальных и высокочастотных сканирований — для поддержания уровня контроля, скорости и частот, необходимых для мониторинга статуса антивирусов в реальном времени, использование своевременно обновленных файлов подписей — для соответствия требованиям безопасности.
- Автоматизированное, без непосредственного участия пользователей, внедрение на тестовых машинах новых патчей, по мере их появления.
- Формирование настраиваемых определений и уязвимостей — для приведения систем в соответствие с корпоративными и отраслевыми стандартами.
- Обнаружение шпионского и рекламного ПО, троянов, сканеров клавиатуры и иного вредоносного ПО.

Инструменты для восстановления

- Обнаружение и удаление шпионского и вредоносного ПО в реальном времени — с использованием базы LANDesk®.
- Контроль доступа к дискам, модемам, USB портам, беспроводным каналам, таким, как 802.11x и Bluetooth, включая Bluetooth PAN.
- Остановка неавторизованных и запрещенных приложений, даже на системах, отключенных от сети, и даже в случае, если конечный пользователь переименует файл.

Организация антивирусной защиты и межсетевых экранов

- Управление выбранным антивирусным решением от McAfee, Norton, Sophos, Symantec или Trend-Micro непосредственно с консоли LANDesk® Security Suite.
- Активизация и конфигурирование межсетевого экрана XP и Vista с консоли LANDesk Security Suite, и обнаружение незащищенных машин, с проводным или беспроводным подключением.
- Конфигурирование одного межсетевого экрана для всех систем, либо настройка конфигурации межсетевого экрана для отдельных систем или групп систем.

Инструменты управления обновлениями

- Автоматическое определение потребностей в обновлениях для ОС и приложений — с использованием обширной базы данных уязвимостей и патчей LANDesk.
- Автоматизированное обновление всех систем — с использованием автоматического процесса распространения патчей LANDesk.
- Осведомленность о том, какие новые новые уязвимости могут привести в систему конкретные обновления — благодаря контролю над тем, какое влияние одни патчи оказывают на другие.
- Управление тем, по каким уязвимостям будут генерироваться предупреждения, и получение уведомлений о новых появляющихся определениях.
- Создание собственных пакетов обновлений для обнаружения и устранения любых обнаруженных уязвимостей. Защита сконфигурированных патчей от вмешательства в них, с помощью защищенного алгоритма MD5.

- Получение и распределение обновлений по приоритетам, с их последующим распространением в масштабе предприятия — с применением эффективной технологии LANDesk® Targeted Multicast™.
- Быстрейшее осуществление полного обновления компьютерной системы. Только необходимые патчи получаются из базы данных LANDesk®, при этом устаревшие сохраняются, на случай необходимости.
- Анализ взаимозависимости патчей позволяет составить правильный порядок обновлений.
- Поддержка преемственности обновлений позволяет получать и распространять те из них, которые необходимы, и отфильтровывать ранние или устаревшие, ведя к сокращению времени достижения полной защищенности. Устаревшие патчи сохраняются на случай необходимости.

Обеспечение безопасности

- Поддержание безопасных конфигураций, основанных на политиках инструментов управления.
- Контроль над тем, кто может изменять корпоративную политику безопасности.
- Мониторинг и классификация точек беспроводного доступа.
- Предотвращение утечек данных, с помощью мониторинга и применения политик на пользовательских USB-устройствах, CD, DVD и иных портативных носителях.
- Контроль над тем, кто может получать доступ к определенным приложениям, по группам или по уровню пользователя, для обеспечения соответствия требованиям безопасности.
- Идентификация систем, использующих беспроводный доступ к сети, или применяющих независимые антивирусные продукты.
- Возможность генерации отчетов, включающих графики тенденций, данные по политике безопасности и по шпионскому ПО.

Системные требования и поддерживаемые платформы

С полным списком требований, предъявляемых к серверам и рабочим станциям, операционным системам, перечнями поддерживаемых баз данных, Веб-серверов и программ генерации отчетности, а также с последней информацией по поддержке языков и клиентских платформ Вы можете ознакомиться на сайте www.LANDesk.com.

Цены

Для получения информации о расценках на узел за LANDesk® Management Suite, пожалуйста, свяжитесь с Вашим поставщиком решений LANDesk. Настоящая информация предоставлена в отношении продуктов LANDesk®. Никакой лицензии, явной или подразумеваемой, безусловной или иной, или гарантии, данный документ не предоставляет. LANDesk не гарантирует того, что в настоящем материале не содержится никаких ошибок, и LANDesk оставляет за собой право обновлять, корректировать или модифицировать данный материал, включая любые спецификации описания продуктов, в любое время, без уведомления. Для получения наиболее свежей информации, пожалуйста, посетите сайт <http://www.landesk.com>.

www.landesk.com

Копирайт © 2007 LANDesk Software Ltd. и ее дочерних компаний. Все права защищены. LANDesk, Peer Download и Targeted Multicast являются зарегистрированными торговыми марками LANDesk Software Ltd. или ее дочерних компаний в Соединенных Штатах Америки и/или в других странах. Другие названия или бренды могут являться собственностью других сторон. Результат, получаемый каждым конкретным клиентом, может варьироваться в зависимости от уникального набора факторов и конкретной ситуации.

Центральный Офис
698 West 10000 South
Suite 500
South Jordan, Utah 84095
www.landesk.com
www.landesk.ru

Информация о продуктах
Brazil + (55 11) 5105-5800
Canada and U.S. + 1-800-982-2130
China + 8610-8518-3138
France + 33 (0) 810 000 212
Germany + 49(0) 89/90405740

Ireland + 353 (0)1 809 4268
Italy + 39 (02) 407 9884
Japan + 03-35234750
Mexico + 52 (55) 533005633
Russia +7 (495) 2234322
U.K. + 44 (0) 118-902-6200


LANDesk® | make IT happen
An Avocent® Company