КОНТРОЛЬ И ЗАЩИТА РАБОЧИХ МЕСТ В КРУПНЫХ ОРГАНИЗАЦИЯХ

Защита нового поколения от сложных угроз, нацеленных на IT-инфраструктуру и пользователей

Взрывной рост количества и сложности киберугроз подвергает критически важные бизнес-процессы, конфиденциальные данные и финансовые ресурсы все большему риску, связанному с атаками нулевого дня. Чтобы свести его к минимуму, необходимо обладать не только новейшими инструментами защиты, но и самыми актуальными данными об угрозах.

Кроме того, важно помнить о том, что большинство кибератак на предприятия начинается с использования уязвимостей устройств сотрудников. Только эффективная защита каждого рабочего места — как стационарного, так и мобильного — создает надежную основу для реализации стратегии обеспечения безопасности.

МАКСИМАЛЬНАЯ ЗАЩИТА

Обеспечить максимальную защиту от всех типов известных и неизвестных киберугроз — масштабная задача, которую невозможно решить исключительно традиционными антивирусными средствами. Чтобы надежно защитить каждое рабочее место как внутри корпоративного периметра, так и за его пределами, нужна многоуровневая платформа безопасности.

МАКСИМАЛЬНАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

Защита рабочих мест должна быть естественной и незаметной. Уникальная интегрированная платформа безопасности «Лаборатории Касперского» обеспечивает надежную защиту рабочих мест, оказывая при этом минимальное воздействие на производительность и ресурсы системы. Это единая, полностью масштабируемая, интегрированная платформа, которая обеспечивает оптимальную производительность, отсутствие конфликтов с другим ПО и безупречную защиту.

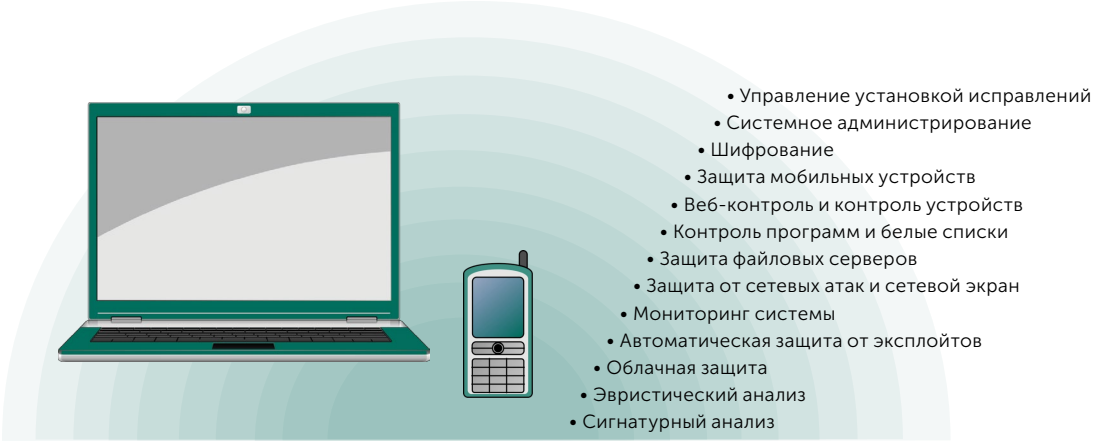
МАКСИМАЛЬНОЕ ИНФОРМИРОВАНИЕ ОБ УГРОЗАХ

Глобальная репутационная база «Лаборатории Касперского» обновляется в режиме реального времени и содержит сведения о новейших угрозах. Это позволяет защищать бизнес от самых актуальных угроз, включая эксплойты нулевого дня. Ориентируясь в своей стратегии обеспечения безопасности на мирового лидера в обнаружении сложных угроз, вы делаете выбор в пользу лучшей в своем классе защиты рабочих мест.

МАКСИМАЛЬНАЯ УПРАВЛЯЕМОСТЬ

Централизованное управление защитой различных платформ и устройств осуществляется из единой консоли. Это позволяет повысить уровень контроля системой безопасности и прозрачность инфраструктуры без внедрения дополнительных технологий.

Многоуровневая защита



Новый уровень защиты и предотвращения угроз

В центре вашей стратегии обеспечения безопасности — мощная и эффективная платформа для защиты рабочих мест. Это подтверждается результатами независимых тестов[1] .

Проактивные интеллектуальные технологии «Лаборатории Касперского» обеспечивают надежную защиту от всех видов киберугроз, в том числе сложных и неизвестных.

Ключевые возможности

- **Эвристический анализ** дополняет традиционные сигнатурные технологии и позволяет обнаружить неизвестное вредоносное ПО.
- **Облачная репутационная база Kaspersky Security Network (KSN)** помогает распознавать и блокировать в режиме реального времени вновь появляющиеся вредоносные программы.
- **Автоматическая защита от эксплойтов** проактивно защищает от сложных угроз, блокируя эксплойты, используемые киберпреступниками.
- **Мониторинг системы** блокирует неизвестные угрозы, обнаруживая подозрительное поведение приложений, и восстанавливает ключевые файлы, в случае если вредоносная программа внесла изменения в систему.
- **Контроль программ** позволяет осуществлять мониторинг программ, используемых на рабочих местах, и использовать технологию динамических списков.
- **Сетевой экран** ограничивает сетевую активность.
- **Защита от сетевых атак** блокирует вредоносные действия в корпоративной сети.
- **Защита файловых серверов** обеспечивает безопасность хранящихся на них данных.

Каждое рабочее место под контролем

Решение «Лаборатории Касперского» позволяет свести к минимуму риск для каждого рабочего места и одновременно повысить производительность. Оно контролирует доступ, блокируя и ограничивая работу нежелательных программ, веб-сайтов и плагинов и разрешая те из них, которые безопасны и необходимы сотрудникам.

Все средства контроля интегрируются с Active Directory® и для них доступна возможность простого (в том числе автоматизированного) создания и применения политик — централизованно или на основе ролей.

СНИЖЕНИЕ РИСКА АТАК ЧЕРЕЗ ПРИЛОЖЕНИЯ

Основанный на технологии динамических белых списков Контроль программ значительно снижает риск, связанный с атаками нулевого дня, обеспечивая полный контроль над тем, какие программы могут выполняться на рабочих местах. Приложения, входящие в черные списки, блокируются. Программы, совершающие подозрительные или ненадлежащие действия, выявляются и дополнительно анализируются. В то же время разрешенные и заслуживающие доверия приложения продолжают беспрепятственно выполняться.

Созданная экспертами «Лаборатории Касперского» облачная технология белых списков позволяет создавать политики по сценарию «Запрет по умолчанию» с возможностью предварительного тестирования.

БЕЗОПАСНЫЙ ПРОСМОТР САЙТОВ В БРАУЗЕРЕ

Веб-контроль обеспечивает контроль доступа сотрудников компании к сайтам, а также позволяет осуществлять мониторинг и фильтрацию адресов. Это помогает повысить производительность труда и минимизировать уязвимость организации перед атаками, связанными с проникновением в систему через веб-сайты и социальные медиа.

КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ВНЕШНИХ УСТРОЙСТВ

Контроль устройств позволяет предотвратить ущерб, вызванный потерей корпоративных или клиентских данных, хранящихся или передаваемых с помощью неодобренных устройств, или загрузку зараженных данных с таких устройств.

[1] ТОП-3 независимых тестов, kaspersky.ru/top3.

Защита данных с помощью шифрования

Инструменты шифрования, работа которых незаметна для пользователей, обеспечивают максимальную защиту конфиденциальных данных на мобильных устройствах и рабочих компьютерах. Встроенная технология позволяет централизованно шифровать корпоративные данные на уровне файлов, дисков или съемных устройств с помощью эффективных политик безопасности, создаваемых как для групп рабочих мест, так и для отдельных устройств.

Устранение уязвимостей

Использование уязвимостей в доверенном приложении, — один из наиболее часто используемых киберпреступниками способов получения доступа к IT-инфраструктуре через устройства сотрудников. Организация эффективного процесса своевременного исправления уязвимостей требует глубокого понимания того, как работают эксплойты и на какие мишени они нацелены. Встроенные инструменты мониторинга уязвимостей и установки исправлений «Лаборатории Касперского» основаны на обновляемых в режиме реального времени сведениях об активности эксплойтов в глобальном масштабе. Они позволяют своевременно устранять критические уязвимости, не оказывая влияния на работу пользователей и приложений.

Управление мобильными устройствами

Сегодня доступ к корпоративным данным возможен со смартфонов и планшетов в любое время и из любой точки мира. Безопасность мобильных устройств преследует две главные цели. Во-первых, это защита от угроз, нацеленных на передаваемую конфиденциальную деловую информацию. А во-вторых, это защита от использования брешей в безопасности корпоративных и персональных устройств для проникновения в систему.

Возможности решения

- **Эффективная многоуровневая защита** от вредоносных программ для ведущих мобильных платформ.
- **Технология антифишинга** блокирует опасные ссылки в сообщениях и на веб-страницах, а фильтрация звонков и SMS-сообщений защищает от нежелательных коммуникаций.
- **Контейнеризация приложений** обеспечивает шифрование и возможность отдельного хранения и удаления корпоративных данных на личных устройствах сотрудников.
- **Контроль программ и Веб-контроль** используют сведения облачной репутационной базы данных Kaspersky Security Network, позволяя блокировать доступ к несанкционированным программам и веб-сайтам.
- **Анти-Вор** включает такие функции, как удаление данных, блокировка, GPS-поиск, SIM-контроль, получение фотографии с фронтальной камеры и звуковой сигнал для обнаружения устройства. Эти функции позволяют оперативно заблокировать устройство и удалить с него секретные данные в случае потери или кражи, а также помешать злоумышленникам воспользоваться устройством.
- **Обнаружение устройств, на которых получен привилегированный контроль (Root/Jailbreak),** и отправка уведомлений об этом администратору.
- **Централизованное управление** включает функционал управления мобильными устройствами и управления мобильными приложениями (MDM/MAM). Из единого интерфейса возможно применение политик к группе устройств под управлением различных мобильных платформ.

Оптимальная эффективность благодаря единой консоли управления

Решение «Лаборатории Касперского» предоставляет специалистам по безопасности полную информацию о состоянии защиты и дает возможность управлять каждым рабочим местом независимо от того, является оно стационарным или мобильным, где находится и какую работу выполняет. Решение обеспечивает широкие возможности масштабирования и предоставляет доступ к данным инвентаризации, лицензирования, удаленному управлению и управлению работой сети. Весь этот функционал управляется из единой консоли управления — Kaspersky Security Center.

Централизованное управление из единой консоли дополнено функционалом управления на основе ролей, что позволяет при необходимости назначать конкретным специалистам по обеспечению IT-безопасности определенные права доступа и обязанности.

Широкие возможности защиты для любых потребностей бизнеса

Контроль и защита рабочих мест — это первый шаг к построению надежной системы безопасности. «Лаборатория Касперского» предлагает широкий спектр решений в области обеспечения безопасности крупных компаний, которые могут работать совместно или отдельно друг от друга — в зависимости от требуемой производительности и поставленных задач. Решения, разработанные для виртуальных и физических систем, серверов и инфраструктур, дополняются решениями, которые помогают бороться с разными видами атак — например, с атаками на онлайн-банкинг, целенаправленными атаками и DDoS-атаками, а также сопровождаются экспертными сервисами.

Сервисы и техподдержка

Специалисты «Лаборатории Касперского» в режиме 24/7/365 оказывают расширенную техническую поддержку в рамках соглашения о сервисном обслуживании (Maintenance Service Agreement). Набор услуг варьируется в зависимости от потребностей бизнеса и масштаба инфраструктуры и выбранного пакета. Кроме того, «Лаборатория Касперского» предлагает профессиональные услуги, которые охватывают все аспекты развертывания, настройки и обновления продуктов «Лаборатории Касперского» в вашей IT-инфраструктуре.

Решения для крупного бизнеса: kaspersky.ru/enterprise

KASPERSKY lab