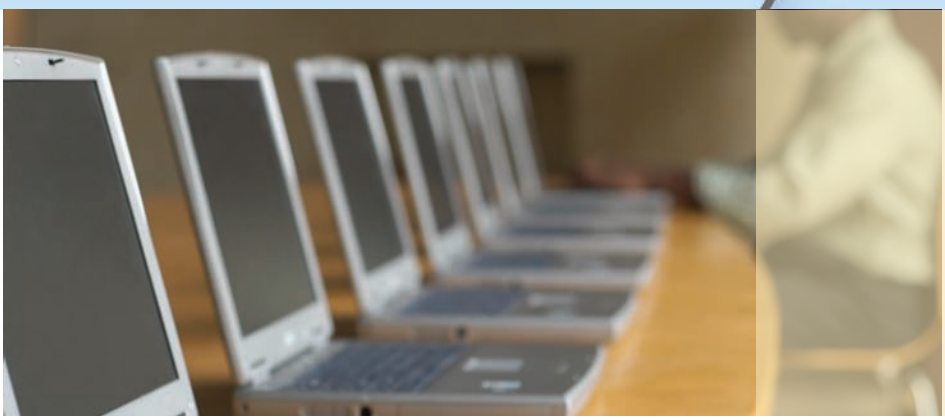
totalsecurity™

Check Point®
SOFTWARE TECHNOLOGIES LTD.



Защита конечных точек сети

Check Point Endpoint Security — единый клиент безопасности для защиты конечных точек сети

Check Point Endpoint Security

Обзор

Check Point Endpoint Security™ - первый и единственный единый клиент, содержащий все необходимые компоненты для комплексной защиты конечных точек сети. Решение обеспечивает высокий уровень защиты и прозрачный режим функционирования для пользователей. Уникальный новый браузер Check Point WebCheck защищает конечные точки сети от постоянно растущего числа интернет-угроз, а система аутентификации OneCheck предоставляет единый доступ ко всем подсистемам защиты компьютера. Кроме того, Check Point Endpoint Security является единственным единым клиентом безопасности, обеспечивающим как защиту данных, так и клиента VPN для организации безопасного удаленного доступа.

Межсетевой экран/ контроль доступа к сети/ контроль приложений	Защищает конечные точки сети с помощью ограничения внешнего и внутреннего трафика, принудительного выполнения политики безопасности (отбора программ, запускаемых на компьютерах), проверки уровня защищенности до предоставления доступа к сети.
Средства защиты от вирусов/шпионского ПО	Обнаруживает и уничтожает вирусы, шпионские и другие вредоносные программы, основанные на комбинировании сигнатур, блокираторах поведения и эвристическом анализе обеспечиваются высокие скорости обнаружения вредоносных объектов и ежечасное обновление сигнатур.
Безопасность данных	Обеспечивает эффективную защиту данных на ноутбуках, стационарных компьютерах и переносных медиа-устройствах с помощью шифрования содержимого диска, контроля доступа, управления портами и шифрования данных на переносных медиа-устройствах.
Удаленный доступ	Обеспечивает безопасный удаленный доступ для конечных пользователей благодаря шифрованию и аутентификации данных, передаваемых во время сеансов удаленного доступа между конечной точкой сети и корпоративной сетью.
Уникальный браузер Check Point WebCheck	Обеспечивает защиту рабочих станций с одновременно удобным и прозрачным режимом функционирования для пользователей. Браузер имеет режим «двойного браузера», позволяющий изолировать корпоративные данные от Интернета и обеспечивать дополнительный уровень защиты благодаря уникальной виртуализации браузера, средств антифишинга и обнаружения сайтов с вредоносным кодом
Система аутентификации Check Point OneCheck	Предоставляет доступ ко всем подсистемам защиты конечных точек сети и к VPN Auto-Connect и упрощает использование системы

ПРЕИМУЩЕСТВА ПРОДУКТА

- Единый клиент для комплексной защиты конечных точек сети
- Свыше 10 интегрированных средств защиты: уникальный браузер, клиент VPN для организации удаленного доступа, средства контроля доступа к сети, шифрование всего содержимого диска ПК и др.
- Клиентское ПО на русском языке
- Прозрачный режим функционирования для пользователей, с удобным интерфейсом (по одной кнопке управления для установки, логина, корзины, проведения обновлений)
- Упрощенное управление и работа с единым клиентом, единый процесс инсталляции управления, централизованное управление
- Благодаря новой системе VPN Auto-Connect обеспечивается непрерывное подключение пользователей при переходе от LAN подключения к беспроводным сетям
- Отсутствие проблем совместимости ПО различных клиентов безопасности
- Снижение совокупной стоимости владения системой безопасности

ЕДИНЫЙ КЛИЕНТ БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ КОНЕЧНЫХ ТОЧЕК СЕТИ

Check Point Endpoint Security™ - первый и единственный единый клиент, содержащий все необходимые компоненты для комплексной защиты конечных точек сети. В итоге, для конечного пользователя работа со средствами защиты упрощается, так как используется меньше приложений безопасности и нет необходимости в большом числе логинов, обновлений и патчей. Для администраторов безопасности использование единого клиента благодаря общей инсталляции и единому процессу проведения обновлений и патчей дает экономию времени и средств.

Check Point OneCheck

Предоставляет удобный доступ ко всем подсистемам защиты конечных точек сети, включая Windows, шифрование содержимого диска ПК (disk encryption), шифрование данных на мобильных носителях (media encryption) и VPN.

Организация удаленного доступа

Обеспечивается защищенный удаленный доступ к корпоративным ресурсам благодаря шифрованию и системы аутентификации передаваемых данных. Новая система VPN Auto-Connect обеспечивает непрерывное подключение пользователей при переходе от LAN-подключения к беспроводным и GPRS сетям, а также незаметно для пользователя выбирает правильную конфигурацию удаленного доступа к корпоративной сети.

Удостоенный наград и лидирующий в отрасли межсетевой экран

Межсетевой экран компании Check Point блокирует нежелательный трафик, делает невидимыми для хакеров конечные точки сети и предотвращает заражение компьютеров вредоносным ПО.

Программный контроль с Program Advisor

Наличие программного контроля позволяет выбирать программы, запускаемые на компьютерах. Средство Program Advisor содержит динамично обновляемую базу данных из свыше миллиона известных программ, в т.ч. вредоносного ПО.

Средства защиты от вирусов и вредоносного ПО

Решение Check Point Endpoint Security обнаруживает и уничтожает вирусы, шпионское ПО, регистраторы клавиш, программы типа «троянский конь», руткиты и иные вредоносные программы, основанные на комбинировании сигнатур, блокираторах поведения и эвристическом анализе. При этом обеспечиваются высокие скорости обнаружения вредоносных объектов и ежечасное обновление сигнатур.

Шифрование всего содержимого диска (Full Disk Encryption)

Благодаря сочетанию аутентификации до загрузки и надежного шифрования всего содержимого диска обеспечивается высочайший уровень защиты данных, хранящихся на переносных и настольных компьютерах.

Управление портами ПК (Port Protection) и шифрование данных на сменных носителях (Media Encryption)

Шифрование данных на сменных носителях обеспечивает защиту ценных корпоративных данных, в т.ч. от вредоносного ПО. Это возможно благодаря шифрованию съемных носителей (USB-устройств, DVD-дисков и др.) и управлению портами и устройствами, при котором осуществляется контроль над записью, чтением, выполнением.

Контроль доступа к сети (NAC)

До предоставления доступа к сети клиент безопасности Check Point Endpoint Security применяет комплексную политику контроля доступа к сети и проверяет, установлены ли на рабочей станции самые последние версии антивирусных программ, свежие патчи и обновления ПО, а также требуемые приложения, в т.ч. браузеры и клиенты VPN.

Централизованное управление

Решение Check Point Endpoint Security обеспечивает централизованное развертывание, конфигурирование, управление политиками безопасности, а также анализ и составление отчетов о событиях системы безопасности конечных точек сети с одной консоли.

Check Point WebCheck

Браузер Check Point WebCheck обеспечивает защиту корпоративных компьютеров с одновременно простым и прозрачным режимом функционирования для пользователей. WebCheck позволяет изолировать корпоративные данные от Интернета и пользоваться всемирной web-сетью благодаря технологии виртуализации браузера, средств антифишинга и обнаружения сайтов с вредоносным кодом.

Виртуализация браузера Check Point WebCheck

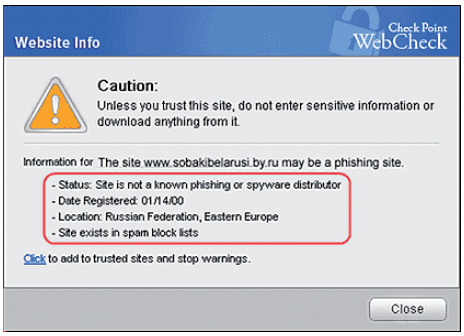
Check Point WebCheck создает изолированную защищенную среду, так называемую виртуальную песочницу, отделяющую корпоративные данные от Интернета. Даже при посещении нежелательных web-сайтов и, в дальнейшем, атак типа незаметной загрузки (drive-by downloads) не происходит никакого ущерба, поскольку все атаки проводятся внутри виртуальной песочницы.

Антифишинг с применением сигнатурного и эвристического анализа

Помимо виртуализации браузера, Check Point WebCheck блокирует посещение пользователями нежелательных сайтов. Check Point WebCheck обнаруживает фишинговые web-сайты благодаря механизму, сочетающему базу данных с сигнатурами фишинговых сайтов и эвристический метод. База данных постоянно обновляется и обеспечивает самую современную защиту от известных фишинговых web-сайтов. Check Point также разработал эвристический метод обнаружения фишинга, позволяющий опознать фальшивые сайты - копии свыше 50 финансовых, социальных, webmail и торговых web-сайтов. Применение эвристического антифишингового метода позволяет Check Point WebCheck идентифицировать угрозы до публикаций информации о них и внесения в черный список баз данных сигнатур.

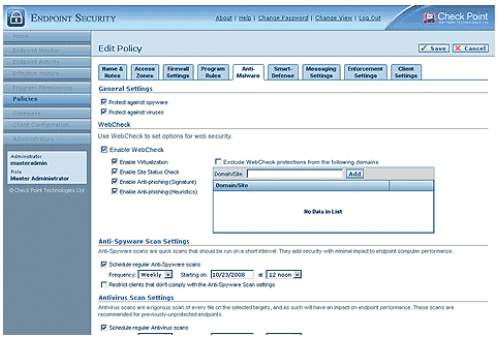
Сообщение-предупреждение о фишинговом сайте

Проверка статуса сайтаCheck Point WebCheck определяет рейтинг каждого сайта, посещаемого пользователем, и предупреждает в случае подозрительного или опасного сайта. Проверяются различные атрибуты сайта, например, возраст домена, зарубежный хостинг, входит ли IP-адрес в черный список серверов-отправителей.



Сообщение-предупреждение о статусе сайта

Централизованное управление политикой безопасности браузера Check Point WebCheckАдминистраторы могут централизовано конфигурировать и управлять Check Point WebCheck в составе консоли управления решения Endpoint Security (защита конечных точек сети). Может быть задано принудительное выполнение политики безопасности браузера для нескольких типов браузеров, в т.ч. многих версий Windows Internet Explorer и Mozilla Firefox.



Консоль управления Check Point Endpoint Security

Централизованные регистрация и составление отчетности по событиям безопасности браузера Check Point WebCheckПрименяя консоль управления на основе web, администраторы могут получить быстрое и централизованное представление по событиям безопасности браузера для всех пользователей компании. Встроенные отчеты и графики помогают администраторам отслеживать и анализировать тренды по событиям безопасности.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПРОДУКТА

	Подробные сведения о защите
Межсетевой экран	
Правила межсетевого экрана	Блокирование/разрешение трафика на основе данных пакетов, источника/получателя, протоколов, портов и времени осуществления действий.
Правила зон	Ограничение/разрешение сетевой активности в зависимости от зоны происхождения или назначения трафика: надежная зона, блокируемая зона, зона Интернета. Пропуск/блокирование трафика в зависимости места в системе безопасности: компьютер, узел, IP-адрес, область IP-адресов, IP-подсеть и маска.
Регистрация в точке доступа сети	Позволяет на время контролируемо обойти правила межсетевого экрана, независимо от накладываемых этой политикой ограничений, для того, чтобы пользователь мог зарегистрироваться в локальной точке доступа сети.
Контроль приложений	
Контроль приложений	Предотвращение появляющихся/новых уязвимостей и атак за счет ограничения доступа к сети для отдельных программ. Управление доступом программ к сети. Для контроля за действием программ используются предоставляемые отдельным программам и группам программ разрешения.
Предоставляемые программам разрешения	Устанавливаются разрешения для отдельных программ или групп программ: разрешить, блокировать, запрашивать, прекращать выполнение.
Проверка подлинности программ	Выполняется проверка несанкционированной модификации программ путем проверки их подлинности с помощью сигнатуры MD5 или заверенных сертификатов.
Средство Program Advisor	Автоматически прекращает выполнение известных вредоносных программ. Автоматизирует принятие решений, связанных с политиками в отношении приложений, на основе поступающих от миллионов расположенных по всему миру ПК данных в режиме реального времени.
Группы программ	Разрешения задаются для групп программ, а не отдельных программ.
Управление доступом к сети (NAC)	
Применение политик рабочих станций и автоматическое восстановление	Исправляются нарушения политик: антивирусное ПО, средства защиты от шпионского ПО, правила межсетевых экранов, исправления ПО, конкретные версии приложений, записи реестра. Устанавливается карантин для небезопасных ПК, и рабочие станции автоматически приводятся в соответствие с требованиями. Ограничивается доступ к сети для неизвестных гостевых пользователей.
Кооперативная безопасность (Cooperative Enforcement®)	Обеспечивает выполнение клиента, наличие конкретной политики, выполнение обязательных правил присвоенной политики безопасности на дистанционно подключающихся к сети рабочих станциях. Ограничивает или прекращает доступ к сети для несоответствующих требованиям рабочих станций.
Контроль доступа к сети на уровне сегментов	Средство Cooperative Enforcement работает со шлюзами VPN-1.
Контроль доступа к сети на уровне портов.	Поддержка протокола проверки подлинности 802.1x, а также коммутаторов и точек беспроводного доступа сторонних производителей. Ограничивается подключение не соответствующих требованиям рабочих станций к изолированным сетям VLAN: ограничение конкретным IP-адресом узла назначения, портами и протоколами.
Контроль доступа к сети VPN	Поддерживаемые шлюзы: VPN-1, Connectra™ и шлюзы сетей VPN компаний Cisco Systems и Nortel Networks. • Обеспечивается принудительная проверка на наличие шпионского ПО, удаление регистраторов нажатий клавиш, а также своевременное обновление антивирусного ПО и исправлений операционной системы. • Контроль доступа к сети VPN и Connectra: включает используемое по требованию решение на основе обозревателя Интернета для обеспечения конфиденциальности сеансов, а также отключает шпионское ПО на гостевых ПК, прежде чем предоставить доступ к сети VPN на основе SSL.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПРОДУКТА

	Подробные сведения о защите
Антивирусное ПО	
Эвристическое сканирование вирусов	Осуществляется сканирование файлов и выявление фактов заражения на основе использования характерного для вирусов поведения.
Сканирование на наличие вирусов при осуществлении доступа	Выполняется сканирование файлов при их открывании, выполнении или закрывании, что позволяет незамедлительно выявлять и устранять вирусы.
Глубокое сканирование	Осуществляется подробное сканирование каждого файла выбранного для сканирования целевого устройства
Сканирование указанных накопителей	Возможность указать каталоги и типы файлов, которые нужно просканировать
Исключения при сканировании	Возможность указать, какие каталоги и файлы с какими расширениями не нужно сканировать
Варианты обработки	Возможность выбора действий, которые необходимо выполнить клиенту при обнаружении вируса: исправление, переименование, отправка в карантин, удаление
Поддержка антивирусного ПО сторонних производителей	McAfee VirusScan, Symantec Norton Antivirus, Trend Micro PC-cillin/OfficeScan, Sophos Anti-virus, Computer Associates eTrust InnoculateIT, Computer Associates VET, Check Point Endpoint Security Antivirus, Kaspersky Antivirus, NOD32 Antivirus, AVG Antivirus, AVAST Antivirus, BitDefender Antivirus, F-Secure Antivirus, Panda Antivirus, Microsoft OneCare Antivirus
Защита от шпионского ПО	
Интеллектуальное быстрое сканирование	Осуществляется проверка наиболее часто использующихся частей файловой системы и реестра на наличие признаков шпионского ПО
Полное сканирование системы	Осуществляется сканирование локальных папок и файлов конкретных типов
Сканирование с глубоким исследованием	Осуществляется сканирование каждого байта данных на компьютере
Сканирование указанных накопителей	Возможность указать каталоги и типы файлов, которые нужно просканировать
Исключения при сканировании	Возможность указать каталоги и расширения файлов, которые не нужно сканировать
Варианты обработки	Возможность выбора действий, которые необходимо выполнить клиенту при обнаружении вируса: автоматическое устранение, уведомление или запрос подтверждения
Check Point WebCheck	
Поддерживаемые браузеры	Microsoft Internet Explorer 6, 7, 8 и Mozilla Firefox 2, 3
Средство управления	
Операционные системы	Windows Server 2003 Check Point SecurePlatform™
Браузеры	Internet Explorer 6, 7 & 8 Mozilla Firefox версии 1.5 и более поздние версии
Клиент безопасности	
Операционные системы	Windows XP Pro (SP2) Windows Vista (32 и 64-битные)
Поддерживаемые языки в клиентском ПО	
Языки	Русский, Английский, Японский, Французский, Итальянский, Немецкий, Испанский
Сертификация	
Сертификаты	Common Criteria Evaluation Assurance Level 4 (EAL4) FIPS 140-2

АДРЕСА И ТЕЛЕФОНЫ CHECK POINT

Международная штаб-квартира
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: +972-3-753-4555 | Факс: +972-3-624-1100 | Эл. почта: info@checkpoint.com

Представительство в России и СНГ
Check Point Software Technologies (Russia) ООО | 109240, Москва, ул. Николоямская, д.13, стр.17 I Тел./факс: +7 495 967 7 444 | http://rus.checkpoint.com