For internal use only

Frequently Asked Questions:

Check Point Endpoint Security

Check Point WebCheck Questions

Can I run Check Point WebCheck along with antivirus, anti-spyware, firewall, or similar endpoint security products?
Yes, WebCheck is designed to compliment other endpoint security functions and technologies.

Is WebCheck part of the Check Point Endpoint Security client?
Yes, WebCheck is tightly integrated and can be deployed with the Check Point Endpoint Security client. It is included with Total Security and licensed separately with Secure Access.

Is Check Point WebCheck centrally managed?
Yes, WebCheck is tightly integrated with the Check Point Secure Access management server providing centralized deployment, policy administration and updates, and logging for security audits and compliance reports.

Will WebCheck slow down or interrupt my browsing?
Even though WebCheck actively evaluates every Web site visited and makes decisions about all data transferred from the Internet to endpoint PCs, end users will notice very little difference in their browsing experience. WebCheck will only interrupt when the user attempts to visit dangerous Web sites, or will launch a new browser session when WebCheck is automatically 'Enabled' or 'Disabled', as configured in the security policy.

Which Web browsers does WebCheck currently support?
Microsoft Internet Explorer version 6 or higher and Mozilla Firefox version 1 or higher

Does Check Point plan to support additional Web browsers?
Not in the near future. The vast majority of enterprises support Internet Explorer or Firefox.

What if I install an additional Web browser, such as Mozilla Firefox, after deployment of WebCheck? Will the new browser be supported automatically?
Yes, if it is a browser supported by WebCheck.

General Product Questions

Does Check Point Media Encryption support Windows CD/DVD wizard?
Yes, seamless integration with Windows CD/DVD wizard enables simplified encryption of critical and confidential data.

Is removable media, such a USB flash drive, fully erased prior to encryption?
Yes, secure device formatting thoroughly erases all data on removable media prior to encryption, ensuring that no data will be left in clear text on the device.

What kind of antivirus/anti-spyware technology is used in Check Point Endpoint Security?
Check Point Endpoint Security uses the same antivirus/anti-spyware technology used in the award-winning ZoneAlarm product that is deployed on more than 60 million PCs worldwide. Recent product reviews and third-party VB100 testing for detection and removal of malware shows the highest detection rates in the industry.

Can Check Point Endpoint Security be used with a different antivirus product?
Yes, Check Point Endpoint Security can be used with other third-party antivirus products and compliments existing antivirus software deployments. For example, Check Point Endpoint Security can ensure that third-party software antivirus software and signatures are up-to-date. Check Point Endpoint Security supports a broad list of third-party antivirus software. For a complete list, please see our technical documentation.

Which VPN-1 gateways support Cooperative Enforcement for internal NAC?
This functionality is supported on VPN-1 gateways with version NGX R65 and higher. Check Point Endpoint Security cooperates with Check Point VPN-1® gateways to provide network-segmentation-level NAC. VPN-1 can be configured for NAC enforcement with Check Point Endpoint Security, allowing administrators to ensure any host initiating a connection through the VPN-1 gateway is tested for compliance.

How many users are supported on a single Secure Access management server?
Check Point Secure Access can support up to 20,000 concurrent users per server out of the box, and up to 40,000 users per server with customizations. With Server Federation, Secure Access can now support more than 100,000 concurrent users. To learn more about this and multiple-server implementations, please contact Check Point.

What is the upgrade path for a customer using legacy products?
The customer will be able to upgrade legacy Integrity, Pointsec (FDE and Protector), and SecureClient products on an individual or multiple-component basis through the unified Check Point Endpoint Security client. The existing individual management systems will continue to control their respective security components in the single endpoint client.

Can I still use the SecureClient VPN for remote access?
Yes. At install you will have the option to deploy the new Endpoint Connect VPN client or the legacy SecureClient VPN.

Note: The legacy SecureClient VPN is only supported on Windows Vista 32-bit operating systems, while the new Endpoint Connect VPN client supports both Windows Vista 32 and 64-bit platforms.

Is an external database required for Secure Access installations?
An external database is no longer needed for Check Point Endpoint Security installations. Logs use a file system instead of a database and are stored in the Check Point log format, which allows you to archive and rotate the logs in the same way as other Check Point logs. In addition for static or transient data, Endpoint Security uses an internal data store that is easy to back up and restore.

Is Malicious Code Protector still included in Check Point Endpoint Security?
No, host intrusion prevention technologies in Check Point Endpoint Security are based primarily on SmartDefense™ protections that have been in use on the VPN-1 gateway for many years. Check Point Endpoint Security allows administrators to enable key protections on the endpoint, such as CIFS worm catcher, Ping of Death, Tear Drop, LAND, Large (Max) Ping, Malformed ANI, SQL slammer, HTTP worm catcher, and HTTP header rejection.

What happened to Integrity? Does this product still exist?
Check Point Endpoint Security Secure Access replaces the Integrity product line. Customers should upgrade from legacy Integrity versions to Secure Access. For details on support policies please see: https://supportcenter.checkpoint.com.

Does Check Point offer Endpoint Security clients for Smartphones and PDAs?
Check Point offers strong data/device encryption solutions for mobile platforms including Palm, Symbian, Pocket PC, and Windows Mobile. There is also SecureClient Mobile™, which is a VPN product for Windows Mobile.

Does Check Point Endpoint Security support Linux and Mac OS?
Check Point Full Disk Encryption supports Windows, Mac OS X, and Linux. In addition, Check Point provides a remote access VPN client for Windows and Mac OS. Please contact a Check Point representative for details.

Does Check Point Endpoint Security have host IPS?
Check Point Endpoint Security embeds a subset of the SmartDefense Application Intelligence that is used on the gateway. Only the protections that are relevant to the endpoint and will not cause false positives are included.

Does Check Point Endpoint Security have server-based antivirus for email servers?
AV clients running on servers are not as important as they used to be, as AV clients are distributed on all agents, scanning files the moment it is accessed by the endpoint. For a customer that would like to protect the server, we offer either using a UTM-1™ device in front of the server or using a layered approach to the AV solutions by using another AV vendor for the server. Secure Access functionality will be certified in 2H09 for Windows 2003 servers. It will be designed for low traffic servers.

How do I handle guests with Check Point Endpoint Security NAC?
For guest access, an SSL VPN device with an on-demand endpoint scanner is required. If firewall enforcement is chosen then guests either will be blocked or served with a Web page, or have specific firewall rules applied that only allow them to go into a specific area of the network.

This area of the network could contain an SSL VPN device that can permit guests to have access back into the network after a clientless security scan (e.g. with Check Point Endpoint Security On Demand on top of a Connectra SSL VPN device). If 802.1X is used, then guests will be shunted into a ‘dirty’ VLAN where an SSL VPN device can then provide access to the corporate network. Reference the NAC Solutions Brief for additional information.

How do I manage printers and VoIP phones with Check Point Endpoint Security NAC?
If a client cannot be installed on the endpoint, then the access scenario will depend on which enforcement method is used - 802.1X or Check Point R65 firewall. If enforcement is done with the Check Point firewall, exceptions are rarely needed as printers, etc. are already within the network segment. Exceptions can be added to Check Point firewalls to allow specific traffic types for some protocols. (For example: allow SIP and control traffic for IP telephones and block all others from an IP range).

If a rogue PC was set in place of the IP phone, the firewall recognizes that the traffic is not VoIP and can block it. In case of a PC that uses the same hub as an IP Phone; if the PC was placed into a restricted state due to non-compliance, firewall rules could still allow IP Phone traffic to pass. If 802.1X enforcement is used, then endpoints that are not running Check Point Endpoint Security need to be excluded from the 802.1X check by device identification, IP address, or VLAN separation in the switch configuration.

Does Check Point Endpoint Security offer port level NAC like CNAC, TNC? Does our 802.1X scale or have a failover option?
Check Point has a long history of support and integration of NAC technology, beginning with VPN device integration (Cisco, Nortel, Check Point) and later 802.1X. Early on it became apparent that 802.1X could only be deployed in certain networks under very controlled circumstances. A NAC solution that leveraged 802.1X therefore only had a limited potential customer base.

To address this, Check Point introduced the Cooperative Enforcement integration with the VPN-1 firewall product. Rather than enforcing policy at the port level like 802.1X, the firewall integration enforces policy at the network segment/gateway level. Turning on the firewall NAC feature in a network using this integration can be done in minutes; in comparison, 802.1X implementations can take months. This firewall NAC integration provides many of the same benefits as port-based NAC without the associated costs.

Sales-related Questions

Can I customize my evaluation deployment?
Yes, Check Point Endpoint Security allows customizable evaluation deployment with user-defined passwords.

Why would I switch from my existing AV vendor when I can upgrade to their endpoint security suite for free?
Check Point Endpoint Security offers a unique value proposition combining endpoint security, full disk encryption, port protection and media encryption in a single agent—eliminating the need to deploy and manage multiple endpoint security agents. Competing product upgrades **do not** include full-disk encryption, media encryption/port protection, or NAC functionality in the free upgrade—and these functions are essential for an enterprise that is serious about endpoint security.

Why would I switch to Check Point Endpoint Security from my existing AV vendor?
For the following key reasons:

1. Check Point has market leading data security products:
   - Positioned as a “leader” in the Gartner Magic Quadrant for eight years running
   - Data security products are based on enterprise-proven Pointsec® technology
   - Highest number and level of certifications including: Common Criteria EAL4, FIPS 140-2, and BITS
   - Many deployments in excess of 200,000 seats
   - Deployment rates in excess of 50,000 seats per week

2. Check Point is the only vendor offering both network and endpoint security solutions:
   - Consolidate network and endpoint security vendors for optimal pricing
   - Proven, interoperable network and endpoint security technologies eliminate conflicts and consolidate patch management

3. Unique NAC solution for better security:
   - Allows administrators to control access to networks and enforce endpoint policy for both VPN-based access and internal network access

- Support for industry-standard 802.1X authentication enables NAC in multi-vendor networking environments

4. Proven Program Control automatically creates an inventory of all PC applications attempting network access, enabling fast, efficient identification, and securing of potential network vulnerabilities

5. Unique WebCheck browser protection:
   - Check Point is the first enterprise endpoint security suite to include browser virtualization, offering pre-emptive zero-day protections against Web-based malware
   - Standard signature based Anti-malware solution are important but are rapidly losing effectiveness against the surging volume of new web based threats, and have very little value against targeted threats.

6. Next generation Endpoint Connect VPN client offers seamless connectivity and enhanced usability features

How does Check Point Endpoint Security rank with Gartner?
Data security components, including Check Point Full Disk Encryption and Check Point Media Encryption, are highly regarded by Gartner and have earned Check Point a “Leader” position in the Gartner Mobile Data Protection Magic Quadrant for eight years running.

How does Check Point Endpoint Security help to reduce TCO?
Traditionally the deployment of multiple endpoint security agents has been required to achieve total endpoint security. With Check Point Endpoint Security, this is no longer the case. Organizations can now deploy a single agent and put in place best-of-breed technologies to protect their PCs and laptops from malware, intrusions, data loss and theft, and other endpoint threats. This reduces capital expenses in the initial procurement as a customer can get all the security he/she will need at a lower price.

A single agent also reduces operational expenses by reducing the administrative effort and cost associated with deploying and managing endpoint security. Additional TCO savings are realized by reducing IT staff resources required to deploy, manage, and update systems, reduced training costs, streamlined incident response and remediation, and lower support and maintenance costs.

How does Check Point Endpoint Security compare to McAfee ePO, which integrates with the domain and can automatically block clients that authenticate to the domain, but are not running the McAfee client? How does Check Point address the detection of rogue systems?
The MSI package that comes with the Secure Access management server can be configured with GPO to automatically push out the client when a new user authenticates to the domain.

For rogue system detection we recommend using Check Point Cooperative Enforcement. Systems that are not running the client are not allowed through the gateway. If the gateway is placed in front of a data center then no real work can be done until the client is installed. A gateway policy can require connecting clients to possess a minimum set of virus definitions or prohibit the use of a specific application (i.e. Skype, AIM, etc.). Clients that fall out compliance with the gateway policy can be disconnected, restricted, or placed into network quarantine.

How does Check Point Endpoint Security compare with Symantec's Peripheral Device control?
Symantec has a very basic set of controls. They only allow control by device type connected to the port and read/write access. Check Point Media Encryption includes rich controls, logging of files transferred, and the ability to encrypt USB drives as well as removable media such as CDs and DVDs. Symantec offers additional features only through an OEM deal with GuardianEdge, which is not built-in.

Does Check Point Endpoint Security provide data loss prevention (DLP)?
There are two major steps in DLP; data protection and content awareness. Data protection guards data at rest from outside threats and controls its movement, while content awareness discovers and categorizes data according to its sensitivity.

Check Point currently offers data protection with Full Disk Encryption and Media Encryption. Content awareness is the second, and also the most complicated step. Check Point has been thoroughly investigating existing content awareness solutions since 2007 and has found the technology to be immature. Actual deployments of existing content awareness solutions have been limited, as they require a great deal of administrative overhead.

As such, Check Point has chosen to develop a content awareness solution in-house. Check Point plans to release content awareness technology for gateways in 2009, with endpoint content awareness technology following soon after. The technology will be integrated into existing Check Point gateway and endpoint client infrastructures.

Pricing and Licensing

What are the main Check Point Endpoint Security offerings?
Check Point Endpoint Security comes in the following packages:

- **Check Point Endpoint Security - Secure Access** - includes firewall, program control, antimalware engine, NAC and VPN. Antivirus / anti-spyware signature updates and Program Advisor service can be added as an optional Malware protection service. Secure Browsing may be purchased separately.
- **Check Point Endpoint Security - Full Disk Encryption** – full disk encryption for laptops and PCs with pre-boot authentication and support for multi-factor authentication scenarios.
- **Check Point Endpoint Security - Media Encryption** - encryption for removable media such as USB drives, CDs, and DVDs combined with port control and device management.
- **Check Point Endpoint Security - Total Security** - package that includes all Endpoint Security technologies, including firewall, program control, NAC, antivirus, anti-spyware, full-disk encryption, port protection, media encryption, secure remote access and browser protection.

How is Check Point Endpoint Security priced? Per seat? Per concurrent user?
Check Point Endpoint Security packages are priced per seat based on the number of endpoint devices protected. For specific pricing details, please contact your Check Point representative.

Is Check Point Endpoint Security management included in the offering price?
Yes, each offering includes both the client and the management applications.

Does a customer still need to purchase SmartCenter™ for Pointsec to manage data security?
No, management of data security is also included in the Full Disk Encryption package price for Check Point Endpoint Security.

Are antivirus and anti-spyware signature updates included in the package price?
No, a customer will need to purchase the SmartDefense Anti-Malware subscription for antivirus and anti-spyware updates. This subscription also includes the Program Advisor service, which provides access to a database of well over a million known good and malicious programs, enabling automation of program control policy.

What support programs are offered for Check Point Endpoint Security? Is support included in the package price?
Support for Check Point Endpoint Security is purchased separately from the offerings, which enable a software license. Check Point offers a number of support programs for enterprises, including Direct Enterprise Support that delivers unlimited support for all Check Point products under a single contract and Collaborative Enterprise Support that combines first-line support from a local Certified Collaborative Support Provider with full back-end support from Check Point. Collaborative Enterprise Support is only available in EMEA and other select regions. For details please contact a Check Point account representative or an authorized Check Point partner.

If a customer has 1,000 seats and wants to buy 50 more, what will they be charged for the new order?
The customer will be charged based on the price-band corresponding to the number of seats purchased in the new order. In this example, they will be charged according to the 1-99 seat price-band.

If a customer wants to buy 1,000 seats of Total Security and 50 seats of Secure Access, how will they be charged?
The customer will be charged under the 100-4,999 price-band for Total Security, and the 1-99 price-band for Secure Access.

Is SSL Network Extender included in the price?
Yes, with Secure Access and Total Security SKUs.

If a customer is using a legacy Check Point Integrity, Pointsec PC, or Pointsec Protector product, can they upgrade to Check Point Endpoint Security?
Yes, a customer will be able to upgrade legacy endpoint products on an individual or multiple-component basis.

Is SmartCenter needed for the Secure Access Management Server?
SmartCenter is a requirement and is installed automatically unless you are going to manage the Check Point Secure Access installation with an existing SmartCenter server.

What happens to the development and/or support of old SecureClient-only binaries?
SecureClient will continue to be released as hot fixes and will continue to be supported for the foreseeable future.

How do I get an Evaluation License for my customer?
Evaluation licenses are available on Check Point User Center and media kits.

If a customer does not need Full Disk Encryption, is there a package that includes only Secure Access plus Media Encryption?
No, Secure Access and Media Encryption packages will need to be purchased separately in this case.

Is the VPN portion licensed on the management server for the VPN gateway, or on the management server for Secure Access?
Users are provided with two certificate keys. One key generates a license that is applied to the VPN gateway. The second key generates a license which is applied to the Secure Access management server.