

Summary and Proof Points

Top 4 Reasons to Select Check Point Endpoint Security

1. Most comprehensive endpoint security solution
2. Secure, fast and simple to use
3. Market-leading data security
4. Optimized total security across network and endpoints

Compatible with Windows 7

Highest Level of Protection

- Most Comprehensive Endpoint Security
- Market-leading Data Security
- WebCheck Secure Browsing

Market-leading Data Security

Single User Interface

Handling Objections

Objection	Response
Check Point is just a firewall vendor.	<ul style="list-style-type: none"> Check Point has been selling market-leading endpoint security solutions to enterprises and consumers for 11 years and has 14+ million seats installed Check Point is recognized as a global leader in both endpoint and network security by leading industry analysts, including: Gartner—9 years as a Leader in the Gartner Magic Quadrant for Mobile Data Protection, Info Security—Product Excellence for Encryption, SC Magazine—Best Mobile Device Solution
Check Point does not offer an endpoint Data Loss Prevention (DLP) solution.	<ul style="list-style-type: none"> Check Point offers a market-leading, comprehensive portfolio of data security solutions: <ul style="list-style-type: none"> ✓ Full Disk Encryption ✓ Media Encryption ✓ Mobile Device Encryption ✓ File and folder encryption Central management, enforcement, updates, logging and alerts for better compliance monitoring
I already have an anti-virus vendor and prefer to consolidate with them.	<ul style="list-style-type: none"> Other endpoint security solutions require multiple agents and are complicated to configure, deploy and manage. Check Point offers a simple, single-agent solution with the flexibility to deploy additional functionality when needed Check Point operates seamlessly with anti-virus solutions from other vendors, while offering the option to consolidate anti-virus into a single, comprehensive endpoint security agent Check Point offers the opportunity to consolidate other security functionality than AV into a simple and cost effective solution—VPN, data security, secure browsing, plus NAC and program control—while preserving your incumbent AV

Key Differentiators and Strategies

Category	Check Point Fact
Highest Level of Endpoint Protection	<ul style="list-style-type: none"> Most comprehensive control of endpoint threats in a single agent unifying over 10 integrated capabilities—including antivirus/antispyware, firewall, full disk and media encryption, VPN remote access, program and network access control Unique virtual browsing security: Block drive-by downloads and phishing attacks with Check Point WebCheck Collaborative network and endpoint security for stronger, simpler security Most comprehensive platform support for data security including Windows, Windows 7, MAC and Linux
Scalability and Low TCO	<ul style="list-style-type: none"> Highly scalable—proven in data security deployments of more than 200,000 seats Rapid deployment—as fast as 50,000 seats per month Powerful central management reduces complexity and TCO Smallest disk footprint after installation
Better Usability and Performance	<ul style="list-style-type: none"> Single agent, update, scan and interface for a transparent, high-performance user experience Fastest anti-virus scan with smallest memory footprint Fastest web page downloads with browser security enabled Single sign-on for all security applications and Windows with Check Point OneCheck Uninterrupted network connectivity with VPN Auto Connect
Compliance	<ul style="list-style-type: none"> Central policy enforcement with rich logging & reporting capability Highest level of security certifications: FIPS-140-2, Common Criteria EAL4, BITS for Full Disk Encryption; FIPS-140-2, CESG CCTM for Media and Mobile Device Encryption

How to Compete Against...

Competitor	Weakness to exploit
McAfee	<ul style="list-style-type: none"> ePO is big, complicated and resource intensive to manage and update Multiple endpoint clients degrade user experience and are difficult to manage No VPN remote access solution NAC not included No centralized logging and alerts for media encryption No support for data security on MAC and Linux platforms
Symantec	<ul style="list-style-type: none"> Mostly focused around anti-virus Weak data security—OEM solution with uncertain roadmap and limited platform support Multiple endpoint clients degrade user experience and are difficult to manage No VPN remote access solution
Sophos	<ul style="list-style-type: none"> Separate endpoint security and data security clients No VPN or browser virtualization—NAC costs extra No Windows 64-bit, MAC or Linux support Multiple logins to endpoint security components
Trend Micro	<ul style="list-style-type: none"> Anti-virus only—no data security, NAC, VPN or browser security
PGP	<ul style="list-style-type: none"> Small vendor with uncertain future Data security only—no anti-virus, firewall, NAC, VPN or browser security Weak management, policy control and scalability in large enterprise environment No MAC or Linux support No wake-on-LAN support

Market Landscape & Challenges

1. Endpoint security concerns increasing

- How do I safeguard intellectual property?
- How do I defend endpoints against new drive-by downloads, phishing sites, spyware, malware and zero-day viruses?
- How do I stop rogue applications and programs from running on endpoint systems?
- How do I prevent endpoint threats from infecting and gaining access to corporate networks and databases?

2. More compliance rules and regulations around data security and privacy

- The number of data breaches and cost-per-record are increasing every year
- PCI, SOX and HIPAA regulations are becoming tougher
- More states and countries are implementing data privacy laws

3. IT budgets shrinking

- Need to optimize security infrastructure and IT security staff productivity while lowering TCO
- Need to consolidate endpoint security and overall security vendors
- Need to do more with less

4. User adoption and satisfaction

- How do I accelerate user adoption?
- How do I ensure security does not hinder end-user productivity?

Check Point Offering

Total endpoint and data security in a single agent that's simple to deploy and use

1. Enable the highest level of endpoint protection

- Unique solution that unifies endpoint security, data security and remote access
- Segregate corporate data from Internet threats with innovative virtual secure browsing protection
- Provide cooperative enforcement across network and endpoint security for stronger protection

2. Prevent corporate data loss with market-leading data security

- Award-winning and leading data security with over 14 million corporate users
- Protects data with the highest levels of encryption and certification
- Proven in large scale deployments on all platforms

3. Reduce complexity and cost with Check Point endpoint and network protection

- Built-in NAC to control endpoint access to corporate network, coordinate endpoint and network security policies
- Security optimization with server consolidation and simple deployment and management
- Smallest disk footprint after installation

4. Transparent, fast user experience

- Simple user experience with single interface and no unnecessary interruptions
- Log in once for encryption, endpoint security, windows and VPN
- Fastest AV scan in the industry with the smallest memory footprint (before, during and after scan)
- Fastest web page downloads with browser security enabled

Questions to Ask

1. Endpoint security concerns

- Q: Considering some of the latest sophisticated attacks, if there were any gaps in your endpoint protections where would they be?
- Q: What historical issues have you encountered from any gaps in your security protection?
- Q: What problems are likely to occur from these gaps?
- Q: What steps have you taken to mitigate these gaps?

2. Data security and compliance concerns

- Q: To what extent are you meeting your SOX, PCI or HIPAA compliance regulations?
- Q: Considering recent trends in threats and regulations, do you anticipate any issues meeting the ever-increasing stance of compliance?

3. TCO reduction and ease of management

- Q: How has the recent crisis affected your general IT and security budgets?
- Q: What initiatives are you taking to reduce OPEX and CAPEX?
- Q: What are your concerns for IT security if any of these initiatives are implemented?
- Q: Which vendors do you currently use and what do you find good and problematic about their management?
- Q: To what extent does managing multiple vendors affect your team's productivity?

4. End-user experience

- Q: To what extent do users complain about their existing endpoint security environment? This can include personal firewall and antivirus, but also data security and remote access.

MCAFEE CLAIM

Check Point does not have a comprehensive endpoint security solution

McAfee total protection is a kluge of components with weak integration

- ePolicy Orchestrator (ePO) is big and complicated
- Multiple user interfaces reduce user productivity
- No single login or single tray icon
- Multiple updates for the endpoint components are disruptive and known to bring the endpoints down

McAfee data security lacks critical controls and support options and is difficult to manage

- No centralized logging or alerts for media encryption
- McAfee Total Protection for Endpoint lacks key endpoint security components like VPN client and NAC
- Full disk encryption is supported on only Windows platform
- Weak browser security with no browser virtualization

REALITY Check Point offers comprehensive endpoint security, with centralized management and policy enforcement

Check Point offers a highly secure and simple-to-use endpoint security solution with a single agent and transparent end-user experience

- Single agent for easy deployment. Simplified central management from a single server
- Multiple platform support for full disk encryption
- Single agent, update, scan and login for a high-performance and seamless user experience
- Meet compliance with integrated reporting and visibility across entire security infrastructure

SYMANTEC CLAIM

Check Point is network security vendor and not an endpoint security vendor

Symantec solution does not offer necessary security components for corporate data

- Data security and VPN not included in single agent
- Weak data security—OEM solution with uncertain roadmap
- Weak application control and no Program Advisor service
- Weak protection against web based threats

Symantec mostly focused around antivirus and lacks integration

- Separate endpoint components require multiple client and policy updates
- Multiple management servers for endpoint components increase TCO

REALITY Check Point offers enterprise class endpoint security, including market-leading data security with the industry's largest installed base

Check Point endpoint security has over 14 million seats deployed and is a Gartner Magic Quadrant leader for 9 years running

- Highest level of certifications for compliance
- Innovative protection from web-based threats with Check Point WebCheck
- Unique program advisor service for program control
- 14 years of remote access VPN leadership

SOPHOS CLAIM

Check Point is not a true endpoint security player

Sophos endpoint security lacks critical features

- No single agent and single deployment package for total endpoint security
- No single interface for management
- No protection against fast growing drive-by downloads
- No support for integrated VPN client
- No real time application control service similar to Check Point Program Advisor
- Not supported on endpoints with third party anti-virus products

Sophos data security is not comprehensive

- No data security support on Windows 64-bit, Mac & Linux OS
- Support for only one encryption algorithm—AES
- Support for two-factor authentication is optional

REALITY Check Point has been offering endpoint security for over a decade, including innovative products like WebCheck

Check Point delivers the most innovative endpoint security in a single, simple solution

- Single integrated UI including NAC management
- Unique browser virtualization technology to protect against exploits like drive-by downloads
- Uninterrupted connectivity with VPN Auto Connect
- Fastest anti-virus scan in the industry with the smallest memory footprint
- Smallest disk footprint after installation