White Paper | June 2007

Minimize Business Risk and Streamline Security Management with McAfee Total Protection for Enterprise

Table of Contents

Minimize Business Risk and Streamline Security Management with McAfee Total Protection for Enterprise

Computer security has changed dramatically since the first computer virus emerged about 25 years ago. It is now far more complex and time-consuming than ever. Viruses have been joined by a constant stream of worms, Trojans, spyware bots, hackers, exploits, identity thieves, and other attacks that threaten your entire network and the endpoints that connect to it. And as networks expand to include remote and mobile users, the potential for gaping holes in your security becomes greater. Companies are looking for ways to streamline their IT processes to improve operational efficiencies while still maintaining control.

Now that a greater number of security technologies are needed to combat a broader range of threats, it's more critical than ever that organizations find an easy and pragmatic way to manage these technologies to minimize operations cost and business risk. McAfee® Total Protection™ for Enterprise solutions provide a single management console that allows you to centrally manage a wide range of security technologies, including anti-virus, anti-spyware, anti-spam, safe searching, host intrusion prevention, desktop firewalls, and network access control. Using this single console, you can efficiently manage endpoint security throughout the enterprise.

Organizations must combat blended threats that can potentially disrupt networks and place corporate assets at risk. Managing security and policies across multiple groups becomes particularly challenging when fragmented management tasks are replicated in fragmented solutions that are complex and costly to administer. McAfee Total Protection for Enterprise is the first comprehensive, integrated solution to deliver inclusive protection that is easily managed from a centralized console.

An integrated solution like Total Protection for Enterprise saves time and resources, frees up IT to concentrate on other important tasks, strengthens enterprise security, and reduces the total cost of ownership (TCO) of security investments. Organizations need the ability to centrally administer a wide range of security management tasks, and it is inefficient and expensive to rely on multiple consoles to do so. Total Protection for Enterprise can protect your business from the latest threats, allow you to improve operational efficiency, and receive a rapid return on your investment in enterprise security.

Endpoint Security Challenges

Security threats are evolving quickly. Just a few years ago, hackers would often deface high-visibility web sites primarily for the notoriety, but we no longer see public outcries over high-profile security violations. That's because the hackers' motivation has changed dramatically. They don't violate enterprise resources or create new virus strains as much for the visibility anymore, but instead focus their resources on theft. Cybercriminals make money by stealing information, and the mainstream media regularly reports on online theft. The U.S. Internal Revenue Service (IRS), TJ Maxx, and BJ's Wholesale Club are just a few of the many organizations that have been victims of cybercriminals.

Enterprises worldwide struggle with managing complex and evolving online threats, including those posed by:

- Spyware
- Rootkits
- Phishing
- Insider attacks
- Bots
- Viruses
- Exploits

Today's cybercriminals rely on stealthy attacks to penetrate corporate security and gain illegal access to information. Industry analysts estimate that a large percentage of enterprises will likely be infected with undetected, financially motivated, and targeted malware that evaded their traditional perimeter and host defenses.

Meanwhile, end users are increasingly demanding Internet and email access beyond the controlled environment of the LAN. Moreover, they do not want to be bothered with managing the security of their PCs. Companies increasingly centralize security to manage access control according to policies, but this often results in reliance on too many management consoles, which constrains the organization's ability to swiftly respond to threats and efficiently manage enterprise security.

A company potentially can have one management console for virus protection, another to prevent spyware intrusion, another for establishing a protective firewall, and yet additional management consoles to protect enterprise resources. This prevents organizations from gaining the benefits of centralized security management from a single console and restricts IT from having easy visibility into security and compliance status. It becomes impractical for organizations to implement centralized control of policies and difficult to quickly assess and respond to security outbreaks.

"Swivel-chair management" requires a security administrator to manage multiple consoles to protect the enterprise. This approach leads to a lack of consolidated reporting and limited visibility into the enterprise-wide security posture, and is an impractical and inefficient way to to manage security. An organization instead must be able to centrally implement, administer, and report on security to manage security in accordance with clear policies.

Implementing a Foundation of Security Risk Management

McAfee's approach to security risk management (SRM) helps an organization apply business discipline to proactively manage risk. What does this mean? We simply help customers by presenting a pragmatic approach to managing security risks and compliance. It starts with discovering assets, evaluating and understanding risk, protecting and enforcing from threats, and finally remediating and reporting compliance.

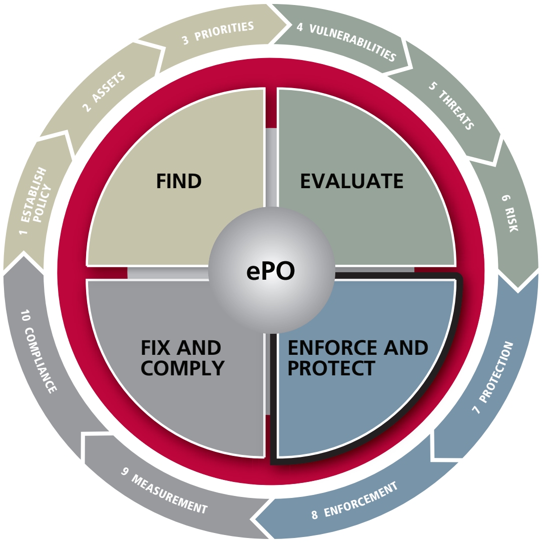

Figure 1. Total Protection for Enterprise is a critical element of the "enforce and protect" component of McAfee's Security Risk Management strategy.

We provide a complete and integrated SRM process with a common architecture and management infrastructure. McAfee's SRM approach integrates multiple threat prevention and compliance management tools to provide comprehensive solutions that work better, save time, and cost less. McAfee ePolicy Orchestrator® (ePO™) is the proven underlying architecture that helps deliver our SRM and integration strategy.

Our SRM strategy solves real security problems by integrating all the functionality customers need—from threat protection to compliance—to provide knowledge-driven security that's automated, actionable, and that empowers you to be efficient and effective. McAfee's collaborative SRM framework bridges network and system security to save you money, improve your protection, and provide a security and compliance solution that's greater than the sum of its parts.

The system security component of McAfee's SRM strategy is delivered through our Total Protection for Enterprise solution. It enables companies to secure their critical infrastructure, including desktops, laptops, and servers. At the center of McAfee's SRM strategy is ePO, which bridges threat protection with security and compliance technologies to enable companies to mitigate security risk.

Total Protection for Enterprise allows you to implement broad protection without the complexity, expense, and headaches of relying on multiple standalone endpoint products. This solution gives you full coverage—anti-spyware, anti-virus, anti-spam, safe searching, desktop firewall, intrusion prevention, safe web browsing, and network access control—with simplified single-console management. You can ensure enterprise-wide compliance with security policies and make sure that all computers deployed on the network are equipped with comprehensive protection threat.

Our SRM strategy eliminates the need to rely on unmanageable standalone products that do not offer sufficient coverage and cannot scale to support enterprise security and compliance goals.

An Overview of Total Protection for Enterprise

It is impossible to implement a successful SRM strategy without protecting endpoints throughout the organization. Total Protection for Enterprise is an integrated solution that provides proven, comprehensive protection so organizations can protect from known and unknown threats and mitigate business risks. McAfee offers two solutions, McAfee Total Protection for Enterprise and McAfee Total Protection for Enterprise—Advanced. Both deliver centrally managed, integrated anti-virus, anti-spyware, anti-spam, safe searching, host intrusion prevention, and network access control capabilities.

Although you could patch together a collection of individual products, McAfee integrates proven technologies for a total solution that is more effective than the sum of its parts. Total Protection for Enterprise and Total Protection for Enterprise—Advanced offer unmatched protection. You can finally minimize risk by continuously and proactively blocking threats while enforcing endpoint policies. A single management console deploys and manages comprehensive protection—anti-virus, anti-spyware, anti-spam, safe searching, desktop firewall, intrusion prevention, and network access control—with a single point for security management and reporting.

With Total Protection for Enterprise solutions from McAfee, organizations benefit from network access control that limits network access to only systems that comply with your security policies and renowned virus protection for the hardest part of your system to manage—desktops and file servers.

Desktop anti-spyware uses true on-access scanning to identify, proactively block, and safely eliminate unwanted programs so you can stop spyware before it has a chance to install on a machine and spread throughout the network. Desktop host intrusion prevention provides zero-day protection to avoid urgency in patching, and it proactively monitors and blocks intrusions by combining signature and behavioral protection with a desktop firewall. Also, email server anti-spam and anti-virus components protect your messaging servers with comprehensive virus protection and content filtering. McAfee SiteAdvisor™ Enterprise allows your end users to safely use the web for research and business projects without the need to impose restrictive policies. You can prevent security threats—such as spyware

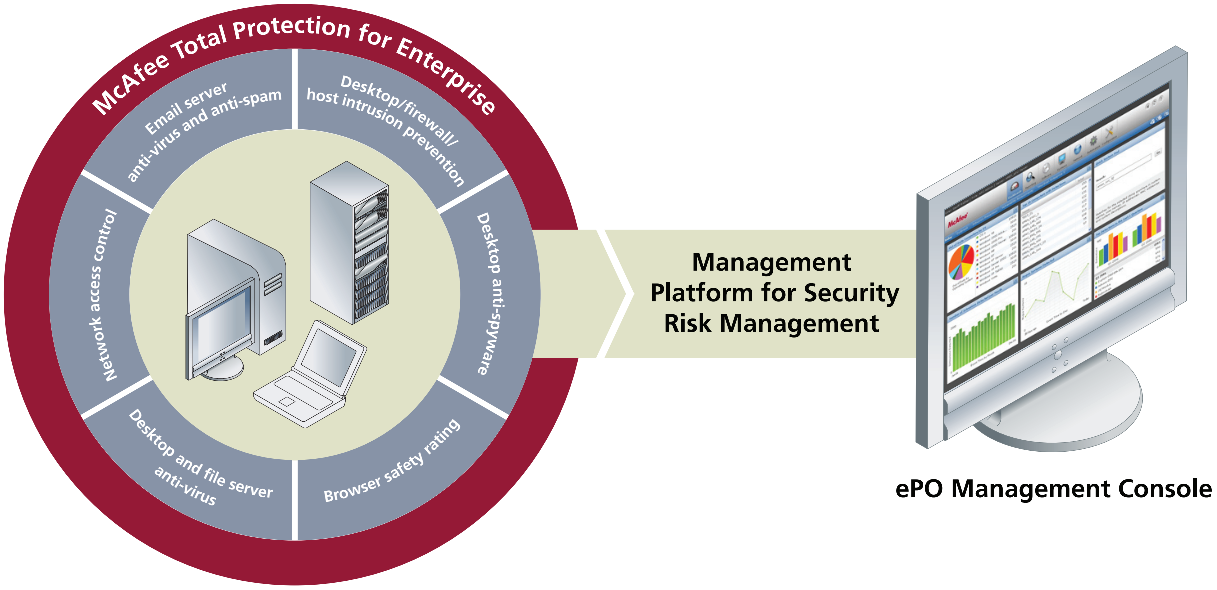
McAfee Total Protection for Enterprise
Email server anti-virus and anti-spam
Desktop/firewall/ host intrusion prevention
Desktop anti-spyware
Browser safety rating
Desktop and file server anti-virus
Network access control
Management Platform for Security Risk Management
ePO Management Console

Figure 2. Total Protection for Enterprise provides comprehensive protection via a single console.

or keyloggers—and increase user awareness about the dangers of surfing the Internet. Anti-spam allows you to increase user and IT productivity by removing the spam from inboxes.

ePO is a centralized single console that manages security and enforces protection. It provides unmatched, cost-efficient system security management, including graphical reports that continually inform you of your security posture. It also ensures compliance with system security policy—regardless of location—and helps prevent costly business disruptions caused by today's sophisticated attacks. ePO administers multiple security technologies and offers unified reporting so you can swiftly gain insights into enterprise security and identify and respond to attacks or threats. ePO is a proven management solution used by over 30,000 customers worldwide to protect over 50 million nodes.

The Business Value of Integrated Management

Remember when all you had to worry about was virus infections? It's a different world today. You are constantly barraged with new breeds of sophisticated threats. To compound the problem, networks have expanded to include remote and mobile access systems, which increase the potential for security breaches. Gaps in your security can put your valuable assets at risk, disrupt your network, and even shut you down. And with the tough requirements for regulatory compliance, the pressure's on to beef up your defenses.

Adding standalone products to combat targeted security attacks isn't the most efficient and cost-effective answer. McAfee Total Protection for Enterprise combines proven McAfee technology, up-to-the-minute threat research from McAfee Avert® Labs, and a single, scalable management console. It all comes together in a single solution that's like no other on the market today.

We cover all the bases with enterprise-level threat protection for your servers, email servers, and desktops. On-access scanning blocks spyware and other malware from propagating on your systems. Automatic threat-signature updates shield you from zero-day attacks. Advanced rootkit protection detects and disables deeply hidden rootkits before hackers can use them for malicious purposes. For an added measure of confidence, our security experts at our global research centers work around the clock, tracking emerging threats and researching cures. And SiteAdvisor Enterprise allows your employees to surf and search the web safely and steer clear of threats like spyware, adware, and phishing scams.

We've made it easy to manage all of these layers of protection and minimize business risks with ePO. From one central hub you can enforce policy, monitor your security, make updates, and get a picture of your security status with detailed graphical reports 24/7. McAfee Total Protection for Enterprise is an investment that continues to pay dividends in the future—along with comprehensive protection and improved operational efficiencies with centralized management. It's built to accommodate growth and change, so when new threats appear, you don't have to start all over. As your infrastructure expands and evolves, it adapts to your needs.

All of this advanced protection is available for a small incremental investment that leverages the security infrastructure that you already have in place. And the extensible architecture of both Total Protection for Enterprise and Total Protection for Enterprise—Advanced allows you to leverage your infrastructure as a foundation for future security and risk management initiatives.

Enhanced operational efficiencies

Instead of having to manage multiple consoles, train staff on multiple management interfaces, scramble for pockets of systems operations expertise in the event of staff turnover, and deal with multiple technical support organizations, you can take advantage of a dramatically reduced learning curve and a single point of contact for technical support. ePO makes life easier for your security staff and they can rely on a single console for security management, policy enforcement, and reporting.

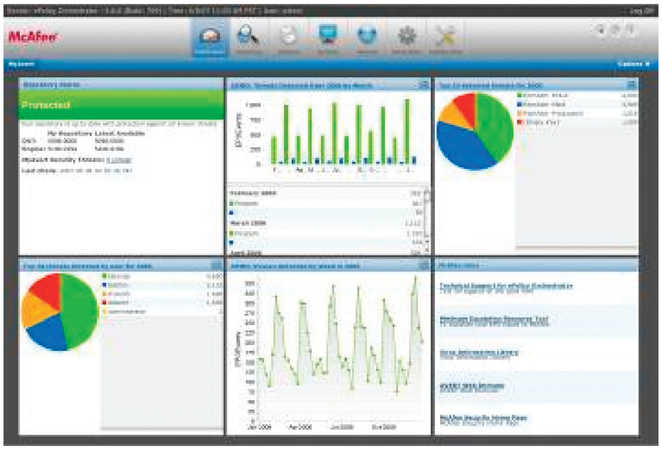

Figure 3. With ePO as a central management hub, users get an enterprise-wide view of their system security.

Access to consolidated information about threats and possible intrusions accelerates outbreak response times and provides the centralized mechanisms to swiftly identify and respond to threats. Organizations can reduce the burden on IT for installing, configuring, and maintaining security technologies on computer platforms and implement and monitor protection enterprise-wide from a single console. With ePO, you can centrally deploy software according to corporate security and compliance policies. Advanced installers detect the presence of third-party security products and you can establish policies to address them. For example, you can establish a policy that instructs ePO to delete third-party anti-virus software on all machines to streamline operational efficiencies and enhance enterprise security.

Organizations no longer need multiple security specialists and can benefit from a single interface to enable uninterrupted end-to-end protection. You can make more efficient utilization of IT personnel by enabling simplified security management from a single console that allows you to improve security while streamlining security administration. IT personnel that would otherwise be forced to monitor multiple management interfaces and correlate reports from multiple consoles can be redeployed to support other IT initiatives.

Improved security

Companies can rely on a single agent framework and a single console to manage enterprise security and make more efficient use of IT personnel. You can minimize vulnerabilities in your networks and systems and benefit from continuous, broad protection that keeps up with the latest threats. ePO allows you to centrally manage multiple security technologies, including the technologies of our competitors, and quickly determine which systems are out of compliance with enterprise security and compliance policies.

You can reduce your exposure to zero-day attacks, fend off new exploits, save time with automatic vulnerability patching on desktops and servers, and protect your network by scanning, filtering, and cleaning incoming and outgoing email, viruses, spam, phishing scams, and other unwanted content. You can also detect deeply embedded rootkit infestations capable of leading to identity theft, spyware, and other malicious exploits, and wipe them out before hackers have a chance to use them to cause damage.

Centralized reporting provides a single management view of diverse security technologies, and organizations can better protect information resources while redeploying IT personnel and benefiting from a single console that simplifies management and streamlines security operations.

Improve ROI via a Single Management Console

Total Protection for Enterprise allows companies to improve their return on investment (ROI) for security technology by providing an integrated solution, a single agent framework, and a single management console. Instead of acquiring technologies from multiple vendors and relying on separate management consoles for administering anti-virus, anti-spyware, anti-spam, safe searching, firewalls, intrusion prevention systems, and network access control technologies you can reduce the capital cost of acquiring discrete solutions and the operational costs of managing them. ePO will help your company better understand and respond to threats, and IT will benefit from a single management console for a global view of enterprise security.

> *According to McAfee customer John Arsneault, Director of Operations for Harvard Business School, "in three years, the school has freed up staff and stabilized costs, resulting in savings of $220,000 a year."*
>
> —Network World*, September 25, 2006.*

Total Protection for Enterprise allows organizations to reduce hardware costs by avoiding the purchase of multiple hardware platforms to support multiple management consoles, and it allows companies to train IT professionals on a single interface, avoiding the downtime and cost of training them to administer multiple management consoles. You can take advantage of best practices for SRM and compliance reporting, and rely on a single vendor to call for support—and a single renewal contract to protect the entire enterprise.

Total Protection for Enterprise saves you time and money by delivering integrated security and compliance technologies that can be managed from a single console. It allows customers to more effectively secure enterprise resources from a broad range of threats, including rootkits, malware, viruses, spyware, exploits, hacker attacks, and phishing attempts. Our proactive technology can protect your company from unknown as well as known threats, with behavioral-based technology that quickly stops unknown threats before they have a chance to compromise your system security.

Vulnerability shielding provides automatic update signatures that shield you from vulnerabilities on desktops and servers. Proactive protection from vulnerabilities allows you the flexibility to protect desktops and servers from exploits with minimal deployment of patches and updates.

Keeping up with security patching to protect against vulnerability exploits can cost precious IT resources. A survey estimated that the average cost of patching a system is roughly $254 per system. For example, if a company has 1,500 systems to patch every month, it will cost about $381,000 per month, or about $4.5 million a year. But Total Protection for Enterprise allows you to reduce the number of patch cycles from every month to once a quarter and still remain protected from most zero-day threats. By moving to patching systems once a quarter, IT personnel can properly test and deploy the patches while reducing costs. In this example the customer would save over $3 million in a single year.

We took proven technology and built it into the industry's first integrated security solution that is:

- Effective
- Comprehensive
- Practical
- Proven

Consolidating software can help you streamline security and save time, money, and resources. Investing in McAfee Total Protection for Enterprise means you won't have to start from scratch when new, previously unknown, threats appear. It's built upon a platform that can evolve as the threat environment evolves so not only will your systems be guarded, but your security investment will also be protected.

Learn More about McAfee Total Protection for Enterprise

Visit *www.mcafee.com* or call us at 888.847.8766, 24 hours a day, seven days a week. McAfee Total Protection for Enterprise and McAfee Total Protection for Enterprise—Advanced are part of the McAfee family of business security products and services. McAfee provides a comprehensive portfolio of dynamic risk-management and mitigation solutions that secure your business advantage.