



McAfee System Protection Solutions

Effective Management of Anti-Virus and Security Solutions for Smaller Businesses

Table of Contents

Introduction—Does Size Matter?	3
<hr/>	
Why Is Managing a Security Policy Important?	3
<hr/>	
What Does <i>Managing</i> Mean?	3
<hr/>	
If It's Not Easy to Use, It Won't Get Used	3
<hr/>	
Staying Up-to-Date—The Single Most Important Criterion for Successful Security	4
<hr/>	
Layers of Protection	4
<hr/>	
McAfee Protection-in-Depth Strategy	4
<hr/>	
Ability to Plan for a Security Response	5
<hr/>	
Ability to Respond	5
<hr/>	
Willingness to Invest	5
<hr/>	
The McAfee Management Landscape—Three Ways to Manage	5
<hr/>	
McAfee's Security Management Options	6
<hr/>	
McAfee PrimeSupport	8
<hr/>	
Summary	8

Introduction—Does Size Matter?

When it comes to defending networks against viruses, hackers, and other malicious threats, there are only two categories of users—those who have a defined, implemented, and managed IT security policy and those that do not.

There is good reason why many businesses have no IT security policy. They have limited IT security skills, and those resources they do have are focused on running their commercial operations. Mostly, these are smaller businesses and they need help to fight effectively against the overwhelming number of threats that attack their networks. Most large enterprises will be certain to have IT teams and security specialists. Most small businesses will not.

But rather than concentrating on size, it is more useful to inquire instead about the ability of a user to respond to a security threat. So another way to look at the need for security solutions is to examine the extent to which the customer is able to define, implement, and deploy a security policy. To be security-savvy or security-challenged. Do the security skills exist or not?

Help Wanted—IT Personnel

Looking for a superhuman to instantly deal with 50,000+ security threats. You will support mission-critical applications on all desktops and servers. Environment under constant attack from outside cyber terrorists. Protection to be updated weekly, monthly, or immediately. Must be able to work with tight budgets. Daily reporting to CIO must show 95+ percent user compliance with policy. Fix the threat, and benefits will include weekends off. Free pizza on Sundays.

Let us stop immediately and ask *What is a security policy?* At its simplest it is defining what configuration settings should be applied to the firewall or to the anti-virus updating mechanism to ensure that, on the whole, the user is protected and kept up to date. At its most complex it will be a set of published, systematic rules that apply to all aspects of IT system and data deployment, defining company approved applications, access control and network authentication, approved vendors, user groupings or domains, the configurations for any number of different layers of security, and so on.

If a user has to stop and ask *What is a security policy?*, then no matter how small or large, this user is not going to successfully implement a security solution that requires fully formed, IT security policy management definitions.

Why Is Managing a Security Policy Important?

One challenge that any organization faces when managing its system security and ensuring complete protection is that in order to enforce policy compliance, an administrator must know if there is a problem with a user's system compliance before it can be brought in line.

A single computer lacking appropriately managed protection can be a threat to the entire network, which means that knowledge of all systems connected to the network is critical to successfully protect the enterprise.

So having a security policy is good. Being able to manage it is *much* better.

New threats affect all sizes of customers. Vendors have a duty to get usable management tools to smaller users, so they can respond to threats as effectively as a larger company.

What Does *Managing* Mean?

In the context of IT security the term management refers to the ability to enforce user compliance, deploy updates, run status and exception reports, and keep the network in good security order—from a central point—controlled by one or more authorized persons.

Many security solutions have a degree of self-management built in. All good anti-virus applications contain an automated, virus detection file update process. But even in small networks it becomes time-consuming and ultimately impossible to ensure consistent compliance if each system is running its own independent updating mechanism, with no centralized control mechanism. It only takes one rogue user to change the settings on a single networked PC to expose the entire network to attack.

So managing means having central control of information and action, in order to regulate the use of groups of PCs around the network.

If It's Not Easy to Use, It Won't Get Used

For hard-pressed business owners and non-specialist IT managers in smaller businesses, ease-of-use is an important issue. But so is the demand to adapt to an ever-changing threat landscape.

The dilemma for vendors is how to deliver the necessary functionality in a security solution, balanced by the ease of installation, deployment, and daily maintenance of that functionality. The requirement to change, adapt, or update is fundamental to any security solution, and that is what sets it apart from other commonly deployed office solutions. By its very nature, the security landscape is constantly changing,

so that ease-of-use must not translate into *easy to install, but fails the change test*.

In the IT security industry, where new threats require security solutions to constantly change, there is a vital aspect in successfully running a security policy—*ability to change*—the ability of companies to define their own security policies and to deploy a solution that executes against those policies and enables the threat response to adapt over time.

Change is a difficult process event for most users. Large companies define common operating environment (COE) standards to attempt to make predictable management of their IT infrastructure possible. But a COE definition that precludes the possibility to implement a rapid update to a security application in today's changing threat landscape is a recipe for failure.

For small companies the concept of change is difficult for different reasons. First, the need for change is often not understood. Everyone knows that viruses are bad, but at what point in the average working week for a small business manager does he or she have the opportunity to review the current threat situation and make changes to the network security policy? How can they find out what port to block to deny a new worm its ability to spread? What does it mean when Microsoft® publishes a new vulnerability?

New threats exploit vulnerabilities on the extreme and on the margin, where the standard deployed defense is probably the least well-prepared to deal with the threat. How can you defend against a threat that has not been discovered? Even if a new threat is discovered, how do you know what to do to counter it?

IT security is a constantly evolving environment where threats such as malicious code (viruses, worms, spyware) and exploitation of vulnerabilities (denial of service attacks, hacking, data theft), consistently challenge the security vendors to create more and more sophisticated tools to defend, detect, prevent, and deny these threats.

Staying Up-to-Date—The Single Most Important Criterion for Successful Security

Many users focus in the main on the updating mechanism for their anti-virus software. This is a vital aspect of maintaining a strong defensive stance, but it is not sufficient on its own. A strong defensive stance requires multiple layers of defense, and the ability to control the deployment, timing, distribution, and reporting of these defense layers. In short, the ability to manage the chosen virus protection software is vital.

Layers of Protection

For the purposes of defining a multi-layered approach, most networks can be dissected into the following categories:

- Desktop, file server, and other client devices
- Application servers, such as mail or portal servers
- External Internet gateways

Within each category McAfee has a number of specific anti-virus and security solutions, and aims to provide the customer with best-in-class solutions at the application level. This is no different from the aims of other vendors, and the customer benefits from the highly competitive nature of the industry and the challenges thrown down by the malware writers, in terms of constant innovation and feature improvement to each application.

McAfee Protection-in-Depth Strategy

McAfee® has a strategy to enshrine all McAfee solutions within a framework called Protection-in-Depth™ Strategy. This strategy enables customers to build a multi-tiered and multi-platform security portfolio to enable them to successfully prevent unwanted intrusion, limit the impact of attacks and reduce the cost of cleanup operations.

The overarching issue for successful implementation of a security defense system is a policy management and compliance application. In the world of small business this translates into anti-virus management.



McAfee Protection-in-Depth Strategy.

Ability to Plan for a Security Response

Viruses, worms, and other forms of malware don't discriminate. They infect or proliferate wherever the opportunity exists, using common social engineering (users) or system defense (IT skills) vulnerabilities.

The individuals and companies that get hit hardest are those whose defenses are weakest. The awareness of viruses as a threat is clear to all sizes and segments of users, but the means to do something about defending against viruses with something other than basic anti-virus applications vary dramatically according to the characteristics of the company or user.

Small companies tend to have less IT skills and are least prepared to mount a successful defense against malware or unwanted intrusion. They may have the system capability to deploy an IT security policy, but they do not have the skill set to do so.

Often the vendors in the IT industry characterize their customers by reference to size, generally noted as small, medium, or enterprise business. This is not particularly helpful when attempting to map security solutions to customers. In reality there are only two types of customers in terms of security—those with IT security skills or resources and those without—*IT savvy* and *IT constrained*.

Ability to Respond

Are All of My Users Protected?

Are All of My Users Up-to-Date?

If the answer to either of the above is *I don't know*, then there is a management problem. There is a failure in the management process that likely means an attack or new virus outbreak may be effective.

It's all about managing resources. A failure to manage users' compliance, the update process, or the backup process, makes it likely the customer will suffer damage through infection or intrusion.

Some customers simply cannot respond. This does not mean they are bad customers. It simply means that they need help responding. They are often simply unaware that they need to respond.

Willingness to Invest

One way or another it all comes down to investment—it is the same for all management decisions—either one invests

in one's own resources, or one outsources the requirement to an external provider. Investment of this kind is always going to be geared to fit within constraints, but large returns can be harvested from even modest investments.

Within the IT security industry, all customers benefit from an intensely competitive supply landscape, as vendors battle to do the best for their customers, and of course, win new customers from other vendors.

It is not just price that benefits the customer. Richness of function and usability and quality of support are all vital aspects of solution provision and every new release adds something new for the user.

The McAfee Management Landscape—Three Ways to Manage

McAfee's portfolio of management choices allows users to choose whether to invest in tools that can be self-managed—best suited for those with some or considerable IT skills—or whether it is better to outsource the headache to McAfee's own expertly packaged managed services solutions, and concentrate their time on running the business while McAfee manages the security policy.

1. Outsource the management process
2. Simplified, self-managed
3. Enterprise-scale, self-managed

The goal is to ensure that no matter how scarce or how rich the customer's IT security skills or resources, that customer can be assured that their security defenses are kept at an optimal ready state.

The main trade-off between simple versus sophisticated is the range of additional management options available. The baseline is the ability to maintain at least one valid set of security settings (policy), so that the anti-virus application, the firewall, and the intrusion prevention solution are always operational for all users at all times.

In an ideal world, all threats can be managed by one solution in a style that would suit all types of users. It is not an ideal world. McAfee's experience with companies using ePolicy Orchestrator® to manage enterprise-level organizations is that *one size does not fit all*. Smaller users require a different set of parameters to achieve 98 percent of the same goals, but within a simplified policy framework. For several years McAfee has been operating its managed service anti-virus and firewall solutions to assist smaller users in this goal, and more recently, has released a purpose-built SMB manage-

ment console, McAfee ProtectionPilot™ for users who prefer to manage their anti-virus installation themselves.

McAfee's Security Management Options

Outsource the Management Process

- **McAfee Managed Services**—McAfee Managed Services deliver automatic, always-on, anti-virus solutions that are managed by McAfee experts 24/7
 - Target User—Organizations without the skills or desire to self-manage their anti-virus or firewall configurations; probably 2–100-plus users
 - Customer Needs
 - Simple installation
 - Automatic updating
 - Simple dashboard reporting
 - Single security policy

The great benefit to deploying one of McAfee's managed services offerings is the transference of management decision to an expert body. For many small businesses, McAfee Managed VirusScan® service provides a quietly efficient, transparent anti-virus solution that gets updated automatically at least weekly or more often as the situation requires. The user does not have to make any judgments about the level of risk of a given threat. McAfee takes care of all updating decisions. However the user is able to view the status of all users' compliance via the graphical dashboard interface.



McAfee Managed VirusScan report.

- **Simplified, Self-Managed (with McAfee ProtectionPilot)**
 - Target User—Small- and medium-size organizations that wish to manage their own anti-virus defenses, but with a limited IT security skill set or a simple IT security policy requirement; typically companies between 25 and 250 users
 - Customer Needs
 - Simple deployment
 - Guided configuration and task management
 - Automatically applied updates
 - Simple dashboard compliance reporting
 - Ability to control and customize security policy

ProtectionPilot is a centralized security management tool that provides a simple, proactive approach to the deployment and ongoing management of virus protection for network administrators who manage up to 500 computers. The installation wizard ensures the *path to protection* is simple and straightforward with automatic updates beginning immediately.

For users with some IT skills, ProtectionPilot offers intuitive and wizard-driven task options that enable administrators to deploy and manage an automatically enforced security policy for their users. This form of self-managed defense is made feasible and effective for organizations with few IT skills because the whole design ethos for ProtectionPilot was ease-of-use backed by years of experience delivering enterprise-scale manageability. The result is a range of anti-virus control and reporting functions that match the needs of customers without compromising the delivery of robust compliance throughout the network.

Where other vendors expect the user to trawl through endless reports, McAfee makes it easy to see compliance issues via the reporting dashboard. When new computers are added, McAfee makes it easy to drag the new systems into the managed domain. When rogue users or well-meaning colleagues decide to *adjust* the anti-virus scanning options, ProtectionPilot automatically imposes the proper configuration back onto the user's system. When McAfee publishes an updated set of virus detection signature files (DAT), ProtectionPilot automatically gets them and updates every user on the network.

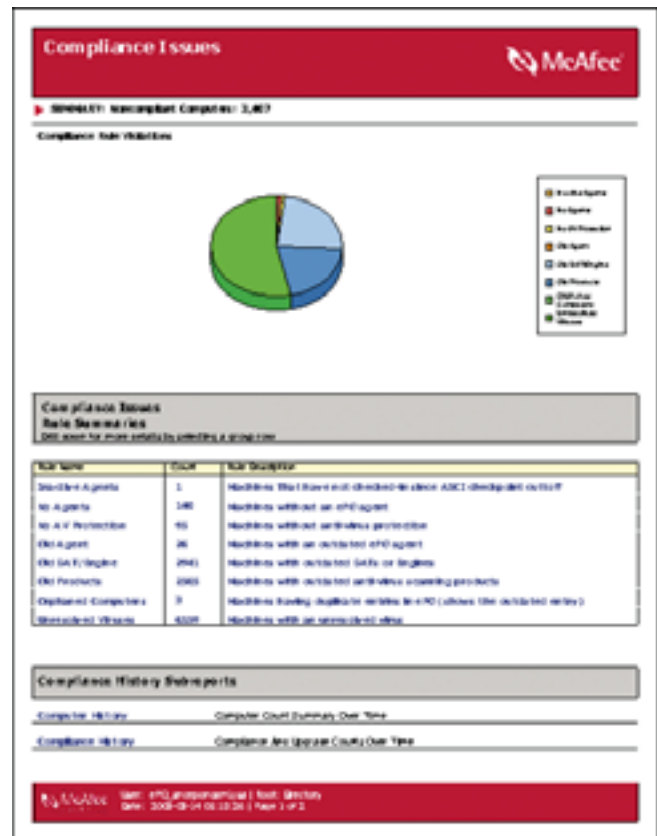


McAfee ProtectionPilot dashboard.

- **Enterprise-Scale, Self-Managed (with ePolicy Orchestrator)**
 - Target User—Medium-size to very large enterprise organizations that wish to implement a comprehensive, scalable anti-virus and security policy management console; suitable for organizations from medium-size up to very large enterprises
 - Customer Needs
 - Centralized deployment capability
 - Bandwidth-friendly packet transmissions
 - Distributed repositories
 - Hierarchical reporting structures
 - Multiple managed domains
 - Rogue system discovery
 - System compliance profiling
 - Customizable compliance and infection reporting
 - Multiple language support within single domain
 - Support for multiple vendor applications

ePolicy Orchestrator is the industry-leading system security management solution delivering a coordinated, proactive defense against malicious threats and attacks for the enterprise. Providing unmatched, comprehensive management of system security at the lowest cost of ownership, it ensures compliance with system security policy and the effectiveness of system protection, preventing costly business disruptions caused by malware infections and attacks. As the central hub of McAfee System Protection Solutions, administrators can proactively mitigate the risk of rogue, non-compliant systems, keep protection up-to-date, configure and enforce protection policies, and monitor security status, 24/7, from one centralized, and truly enterprise-scalable console.

For over four years, ePolicy Orchestrator has established itself as the leading system compliance and security management console for the IT security industry. Many vendors have event recording or reporting capability, but few can deliver the ability to take action to execute corrective action over such a range of applications and with low network performance impact and scalability.



McAfee ePolicy Orchestrator report.

The dashboard approach of ProtectionPilot is replaced by a full, menu-driven, graphical reporting environment. Rogue users are identified, while different security policies can be defined and applied to a wide range of user groups and domains. ePolicy Orchestrator puts the IT security officer in control of the organization's security policy implementation and enables demonstrable compliance to be achieved.

McAfee PrimeSupport

McAfee has pursued a strategy of providing best-of-breed technology for each type of security and performance management application—but the Protection-in-Depth Strategy is more than just deploying and implementing best-of-breed solutions today. Prevention is certainly our first priority, but inevitably, you will have to react to a problem.

The McAfee PrimeSupport® program is essential for making the most of your investment in McAfee System and Network Protection Solutions. McAfee's PrimeSupport team has all the right resources and is ready to deliver your needed service solution. PrimeSupport resources include: delivering authorization to access all available maintenance releases and

product upgrades, access to a comprehensive suite of additional online self-support capabilities, live telephone support accessible 24/7/365, available assigned support account managers, and a range of software and hardware support solutions that can be tailored to meet your needs.

Summary

A simple security policy that is easy to manage will always be more effective than a sophisticated policy that is unmanageable. Perhaps more importantly, a simple security policy is much better than none at all. Customers can look to McAfee to find policy management solutions at both ends of the spectrum, according to their ability to manage or the needs of their IT infrastructure. McAfee security management options enable customers to deploy the most effective, appropriate IT security policies. This means they can maintain control of their network security, without pushing their IT staff beyond the limit. McAfee means management choice.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, Protection-in-Depth, ePolicy Orchestrator, ProtectionPilot, VirusScan, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 Networks Associates Technology, Inc. All Rights Reserved. 6-sps-mgt-001-1104