Technology Blueprint

McAfee®
An Intel Company

ESSENTIAL PROTECTION FOR PCs

Match your endpoint protection with today’s risks

Match your endpoint protection with today's risks

The Situation

Many managers don't see the need to invest more in endpoint protection. Skeptics make comments such as "If the machines get infected, we will simply rebuild it," and "It's just an endpoint machine—how much impact can it really have?"

They think you already have sufficient protection with antivirus. Why then have you been infected recently? Why did your antivirus not stop Zeus or that FakeAV? The reality is that hackers and malware these days are using multiple vectors and complex methods to get to your PCs. Back in the old days, a single antivirus solution was enough, but today you need to protect all vectors of infection.

Driving Concerns

"How many layers do I really need? How many computing resources will protection consume on my endpoints? How much effort is required?" These are all valid questions when it comes to protecting your endpoints. There are tens of thousands of new threats every single day. Signatures need updating multiple times a day, and signatures are no longer enough to fend off common malware. If you do not invest appropriately, the reality is that it's not only the endpoint that will be affected, but your whole infrastructure can be compromised in many ways. And you may not even know the impact at first. You may lose sensitive information and infect or compromise other devices throughout the network before you detect and stop the problem. It's not the endpoint infection you see at first that is the big problem; it's the broader impact that you do not see.

- **First contact.** Threats gain access to your systems by physical access via a USB key, by a malicious user, by email, or by a visit to a malicious website
- **Local execution.** Once first contact is established, the attack requires some kind of local execution, some exploit or social engineering designed to get vital information from the user or get authenticated access to the system in order to establish a presence inside your network
- **Establish presence.** Next, attackers take control of the system by downloading malware, getting a higher level of privilege (such as a guest turning into an admin), creating backdoors, using stealth techniques, hiding their actions, and protecting themselves in ways that make it very difficult to disable them when you find out about them
- **Malicious activities.** With control of the system, the attacker can do anything: steal sensitive files on the machine, take over the user's identity and access privileges (such as access to financial applications, customer databases, and critical systems), reconnoiter the network to look for vulnerabilities, or integrate the system into a botnet as a spam relay

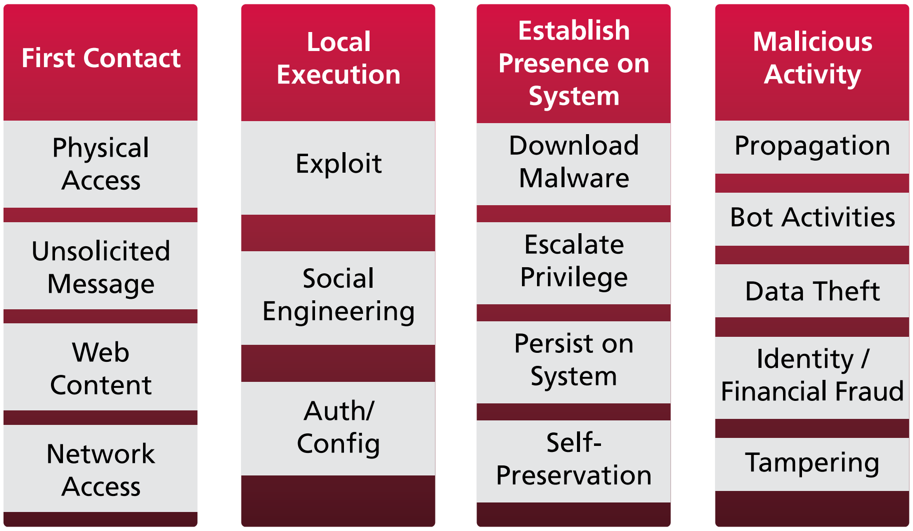
Here's a good example:

- **First contact.** A user goes to a website and receives a warning stating that his account is about to expire and that he needs to enter his credentials along with some validation information
- **Local execution.** The user, thinking that everything seems normal, enters the information and presses "OK." He is then redirected to his normal web page and proceeds to surf, ignorant of any illicit activity.
- **Establish presence on system.** However, when the user pressed the OK button, the malicious website downloaded the appropriate malware for the user's browser; installed itself in stealth mode, perhaps in memory or as a rootkit; disabled the task manager and registry editor so that an admin could not stop or remove it; and then used that information to gain elevated access to the system
- **Malicious activity.** The malware now contacts its "command and control" center and awaits instructions to defraud/scam/steal from the endpoint or other devices on the network. It may look for credit card numbers and login credentials, or it may hunt mailing lists so it can propagate the malware. It may copy itself on network shares the endpoint can access. Meanwhile, backdoors and Trojans will have been installed on that endpoint as well as other machines across the networks, thanks to the

Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

replicating abilities of the threat. Network shares allows for easy distribution, since most of them stay poorly protected. The criminals can monitor activity and exfiltrate information, such as intellectual property, private financial information, trade secrets, personal files, and sensitive customer information.



First Contact	Local Execution	Establish Presence on System	Malicious Activity
Physical Access	Exploit	Download Malware	Propagation
Unsolicited Message	Social Engineering	Escalate Privilege	Bot Activities
Web Content	Auth/ Config	Persist on System	Data Theft
Network Access		Self-Preservation	Identity / Financial Fraud
			Tampering

Endpoints are more vulnerable today than in the past because of the multiple stages and tactics used in attacks.

Decision Elements

These factors could influence your architecture:

- What desktop AV vendor do you use today, if not McAfee?
- Have you been infected recently?
- Do you give administrative rights to your end users?
- How do you manage the recycling of your current hardware?
- Are you using a web gateway solution based on categorization only?
- How are you controlling external devices and removable media?
- Do you verify the health of the devices connecting onto your corporate network?

Solution Description

Because of these multi-stage attacks, securing the desktop is more complex than just slapping a simple antivirus program on it. Antivirus solutions are essential, but are only a single component in the chain required to secure a machine properly. More than I/O needs to be protected. For instance, if a traditional antivirus product just looks for disk access, it will miss threats from the network or from memory. Preventing first contact, exploits, and malicious activities necessitates layers of defense for each of the components of the system. Further, each of your defenses must stay current as threats evolve.

- **I/O.** Everything that is read from disk or written to disk needs protection, and that is the job of a traditional, typical antivirus solution. Every time that a user accesses a file, it is scanned by an antivirus for known threats. This is the basic protection that everyone knows and understands.
- **Network.** Data flowing in and out of a machine, either through a wired or wireless connection, needs to be analyzed for intrusion and for contact with permissible destinations. A desktop firewall will provide protection against these threats. Any packet passing through the firewall should be analyzed against rules that your company defines, such as permitting certain applications only when connected through a secure VPN or your local corporate network while limiting access to any other interfaces (wireless, 3G USB key) your machine may have. This control helps restrict users from working around perimeter security and protection policies. Perhaps your office does not have a wireless network, but neighboring businesses do. Policies could allow you to block employee use of a neighbor's wireless network.
- **Memory and processes.** Many of today's threats are buffer overflows. They happen in memory. They sneak their way in, corrupt the memory, and execute arbitrary code, all unbeknownst to the user. Traditional antivirus solutions will not see these threats, as AV solutions typically concentrate on the I/O, not the memory. An antivirus or a firewall will not see a SQL injection. A firewall or antivirus cannot stop an escalation of privileges either. However, Host IPS will. A Host IPS solution looks into the memory, analyzes its patterns, and detects threats such as buffer overflows.

- Signatures. Antivirus, Host IPS, and other defenses usually operate with some type of signature. Signatures stop what is known and are time dependent, meaning that your protection is only as good as your last update. Today, it is important to get real-time protection on top of signatures. A cloud-based intelligence service becomes an essential part of your protection against fast moving exploits and threats. With the increase in tenacious, sneaky attacks such as rootkits, protections also need to start looking for threats before the operating systems loads.

Another important factor when it comes to protecting an endpoint is the end user. Most users suffer from "Acute Clickitis." This is a condition where end-users will click on everything they see, no matter what it says, because a) they don't read what it says, b) they want to go to the next level no matter what, or c) they are doing it by force of habit. This is how first contact is established most of the time.

- Content control. There are filtering solutions that will prevent users visiting certain categories of sites, but what about the content? A site may be deemed "appropriate" as a category, but the files, scripts, and downloads overtly and covertly located on that site may be malicious. How can you know? You should complement your categorization with content protection, a solution that will not only know that the site is an adult site or a gambling site, but also that the downloads are dangerous, that a browser help object will install without your consent, or that its affiliations are questionable.

What if someone loses a laptop or has it stolen? What if you send the machine for repair? It becomes quite important to protect the data in such a way that it can't be compromised if the machine leaves the boundaries of your enterprise.

- Endpoint encryption. Encrypted devices are less sensitive to losses or theft. When the data is encrypted and the device is lost, the device becomes just a hunk of metal, leaving your data secure. The same can be said when a device is being repaired or replaced. When a machine is decommissioned, very often companies use a shredder to destroy the information, which is a long and costly process and not very green. However, when a device is encrypted, the information is secured. It can then be disposed of in any way you can think of, including donations to charity, without fear of having your data exposed.
- Device control. A simple USB key can create mayhem. Personal USB keys often share data and files with machines owned by friends or family members, machines already compromised by malicious code. When that USB key is connected to your corporate machine, Autorun will execute whatever exists on that key. Your security depends on your being able to limit access to your endpoint to the USB devices you trust. You should also be able to prevent data from being transferred to a USB key. Maybe you want to allow users to plug-in their iPods, but only to recharge them or to run "read only" for playing music. This fine-grained control allows some device flexibility while preserving data confidentiality.
- Endpoint health. Making sure you check managed machines for proper health before they connect to your network is a very important part of preventing first contact. Is the machine connecting to your network healthy? Does it contain the latest patches, the same ones you require on your corporate environment? Is it up to date? Does it have all the protection products (such as active AV and a firewall) that are necessary before it joins your network? An effective solution will answer these questions and either permit, block, or quarantine systems based on their compliance with policy. Quarantined systems should be directed to a remediation site where they can obtain the required updates.
- Visibility. Now that you have all the pieces in place, can you have a top view that will show you your security posture? The solution should tell you if you are at risk with a few clicks, rather than requiring juggling of massive amounts of data and spreadsheets. It should help you gauge compliance with regulations by presenting auditor-ready reports. Executives should be able to see security status on-demand, with up-to-date information.

Technologies Used in the McAfee Solution

In order to achieve this level of security, McAfee recommends using a combination of technologies for defense in depth. Preventing first contact is the ideal, but if you can't, reinforcing security layers will come into action. With this endpoint solution, McAfee protects all vectors: encryption, access control, safe browsing, malware, network (wired and wireless), memory, I/O, processes, and more. McAfee modules can be implemented as an integrated suite, or added as your risks and budget allow.

The products we suggest are centrally managed by McAfee® ePolicy Orchestrator® (McAfee ePO™). McAfee Global Threat Intelligence provides real-time protection through reputation engines built into the different products.

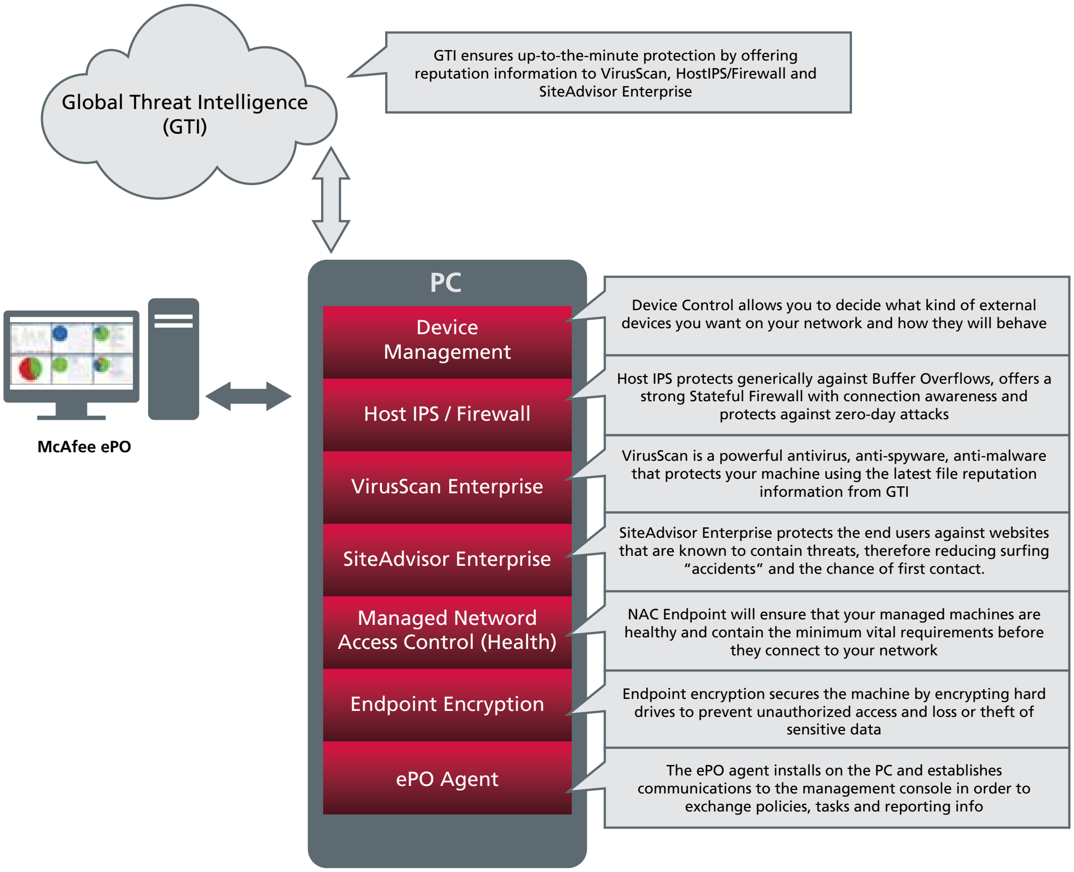
Start where it makes sense. Install McAfee VirusScan® Enterprise as the basic foundation, including antivirus, and quickly add McAfee SiteAdvisor® Enterprise to prevent accidental surfing to risky or inappropriate websites. Secure the network vector with McAfee Host Intrusion Prevention and its desktop firewall. Protect data with encryption of each device (McAfee Endpoint Encryption for PC).

Complement core system protection with McAfee Device Control in order to prevent unwanted and dangerous devices in your network (USB keys, 3G network keys, mobile devices, etc). Use McAfee Network Access Control to check the health of your managed machines before they connect.

Using this combination, you will be able to protect the I/O, network, memory, and processes of the endpoint, enable safe use of the web, and encrypt the data on your machines. These layers reduce the chance of a successful attack by thwarting first contact as well as each of the steps following it. Users can be connected at the office, as they travel, or at home, and will be protected equally. Policies are enforced even if the machine is not connected to the corporate network. Of course, policies are flexible and can be connection-aware as well.

For real-time protection before signatures are available, McAfee Global Threat Intelligence integrates directly with McAfee products. Since McAfee Global Threat Intelligence (GTI) is in the cloud, it will work wherever there is an Internet connection. McAfee VirusScan Enterprise uses GTI real-time file reputation to enhance signatures and close the gap between updates. McAfee Host IPS uses GTI to assess IP reputation outbound AND inbound to prevent communication with systems and sites known to be malicious. This control is very effective against botnets, as most bots use outgoing connections to command and control centers, taking advantage of the absence of outbound scanning in most enterprises. Leveraging GTI, McAfee SiteAdvisor Enterprise evaluates the reputation of URLs within a website and classifies them accordingly, preventing users from establishing first contact in the first place.

When a machine connects to McAfee ePO, you have complete visibility into the device. Details on its hardware inventory such as CPU, disk space, memory, operating system type and version, time zone, risk level, threats detected, countermeasures, and more are visible through the McAfee ePO management console. This visibility is not limited to PCs. McAfee ePO can also provide visibility on Mac, Linux, Solaris, and mobile devices such as Apple iPads, iPods, and iPhones, Androids, and RIM Blackberry devices where a McAfee agent is installed (McAfee agents are available for these platforms using optional McAfee products; visibility varies by device.)



GTI ensures up-to-the-minute protection by offering reputation information to VirusScan, HostIPS/Firewall and SiteAdvisor Enterprise

Device Control allows you to decide what kind of external devices you want on your network and how they will behave

Host IPS protects generically against Buffer Overflows, offers a strong Stateful Firewall with connection awareness and protects against zero-day attacks

VirusScan is a powerful antivirus, anti-spyware, anti-malware that protects your machine using the latest file reputation information from GTI

SiteAdvisor Enterprise protects the end users against websites that are known to contain threats, therefore reducing surfing "accidents" and the chance of first contact.

NAC Endpoint will ensure that your managed machines are healthy and contain the minimum vital requirements before they connect to your network

Endpoint encryption secures the machine by encrypting hard drives to prevent unauthorized access and loss or theft of sensitive data

The ePO agent installs on the PC and establishes communications to the management console in order to exchange policies, tasks and reporting info

McAfee VirusScan Enterprise

McAfee VirusScan Enterprise is not your typical, run of the mill antivirus. It contains advanced, proactive technologies to counteract unknown attacks. VirusScan Enterprise safeguards your systems and files from viruses, spyware, worms, Trojans, and other security risks. It detects and cleans malware, and allows easy configuration of policies to manage quarantined items.

Real-time scanning protects all your systems, including remote locations, from current and emerging threats. McAfee Global Threat Intelligence file reputation service will detect and block malicious files based on a cloud lookup, instead of waiting for a signature. This up-to-date risk assessment helps stop zero-day attacks in their tracks. VirusScan Enterprise also guards against buffer overflow exploits that target vulnerabilities in Microsoft applications. Access Protection Rules stop unwanted behavior such as the disabling of the registry editor or the task manager and prevent mass-mailing worms from sending mail, all without signatures. For extra control, you can apply categories to stop unwanted programs: spyware, adware, remote admin tools, dialers, password crackers, jokes, keyloggers, and others.

McAfee SiteAdvisor Enterprise

Simple categorization of websites leaves your users and their systems at the mercy of unsafe and compromised websites, and unsafe web pages within an approved site. Instead, McAfee SiteAdvisor Enterprise can assess the risk of visiting a website before users arrive. If it is too risky (based on a policy set by the enterprise), the page will be blocked before it loads or installs malware. Since the user does not access the malicious code to begin with, IT will not have to clean it up afterward.

Users suffering from "Acute Clickitis" will be prevented from surfing to places that are not safe, reducing exposure to malware. Using McAfee Global Threat Intelligence, SiteAdvisor can verify if the website you are visiting is safe. "Safe" means that the site does not contain known malware, is not a known spammer, will not compromise your browser, and does not have excessive popups. To help warn users against phishing, SiteAdvisor provides warning messages of potentially dangerous links within your Outlook 2007/2010 client. It supports Internet Explorer, Firefox, and Google Chrome.

McAfee Host Intrusion Prevention with Firewall

Although most users have a desktop firewall built in with Microsoft Windows, it is turned off or minimized by users who want to avoid inconvenient interventions. Most everyone has dialed down enforcement to the point the firewall has become like Swiss cheese—a determined attack can work its way through the holes. However, the firewall within McAfee Host Intrusion Prevention (Host IPS) lets you centrally enforce appropriate protection without getting in each user's way. The McAfee desktop firewall contains rules built for the enterprise. For example, it understands that VPN connectivity is essential when remote users connect, and that some applications should not be used when the employee is outside the walls of the corporation.

The McAfee desktop firewall has "connection awareness" with "connection isolation." Rules will be in effect according to the location of the connection. If a system connected to the enterprise network has multiple network interfaces, the firewall will not listen to any network interfaces except the one the policy permits. For example, imagine your machine has two network interface cards (NICs), one wired and the other wireless, and you connect to the corporate network via the wired NIC. With connection isolation, the firewall would only listen and allow traffic to the wired NIC, dropping and blocking all traffic on the wireless NIC. The firewall will not let you connect wirelessly to another network that is not defined as acceptable by your corporation. When you get home, a separate set of rules will help keep your machine secure while allowing access to the Internet.

The dynamic stateful firewall with global reputation is unique. McAfee Global Threat Intelligence (GTI) provides communication reputation that guards traffic outbound and inbound. If a botnet tries to connect to a protected system, GTI will see that the reputation of the incoming traffic is bad, and the firewall will not allow the connection to occur, saving the machine and your network from an outside attack. In a similar fashion, if a bot tries to connect to its command and control center from inside your network, the GTI will see the outgoing reputation of the traffic as bad and will block the bot from contacting its control hosts.

The Host IPS adds another dimension to the mix. It provides signatures and behavioral analysis. Host IPS will prevent attacks with signatures, as well as those without signatures, right on zero days. Generic protection against buffer overflows uses signatures to protect against a majority of vulnerabilities out there.

Even if you are diligent about patching your Microsoft products, it is hard to keep up with patching all the other endpoint products and plugins: Adobe, Mozilla, IBM, RealNetworks, and others. With Host IPS, three layers of protection (signature analysis, behavioral analysis, and dynamic stateful firewall with global reputation technology) prevent intrusions, protect assets, and defend your company against known and emerging exploits, including zero-day attacks.

McAfee Endpoint Encryption for PC

McAfee Endpoint Encryption for PC (EEPC) is your first line of defense against data loss and theft as well as risks when you recycle or retire your hardware.

Normally, when the user turns on the machine in the morning, it loads its operating system and then asks for authentication—user ID and password. The user identifies to the OS and then proceeds to a regular workday.

With EEPC, the operating system does not load until the user has authenticated. With this model, all the attacks that are known to crack a password become useless to the hackers. EEPC uses Pre-Boot Authentication with an optional second factor authenticator (such as a SmartCard) in order to prevent access to the data by unauthorized users. What if a thief decides to take the drive and put it in another machine? Nothing bad happens. The data is encrypted and unreadable by third parties. Not only is it safe if lost or stolen, it is safe to release for repair or other green initiatives such as recycling your hardware.

McAfee Device Control

McAfee Device Control gives you control over what devices can and cannot be connected to your PCs. You can make devices read only. You can allow only certain brands of USB keys, or even a specific key using its serial number. You can allow mobile devices to connect—but only for charging their batteries. McAfee Device Control will give you flexible ways to manage what devices can be connected and controlled in your PC environment.

McAfee Network Access Control

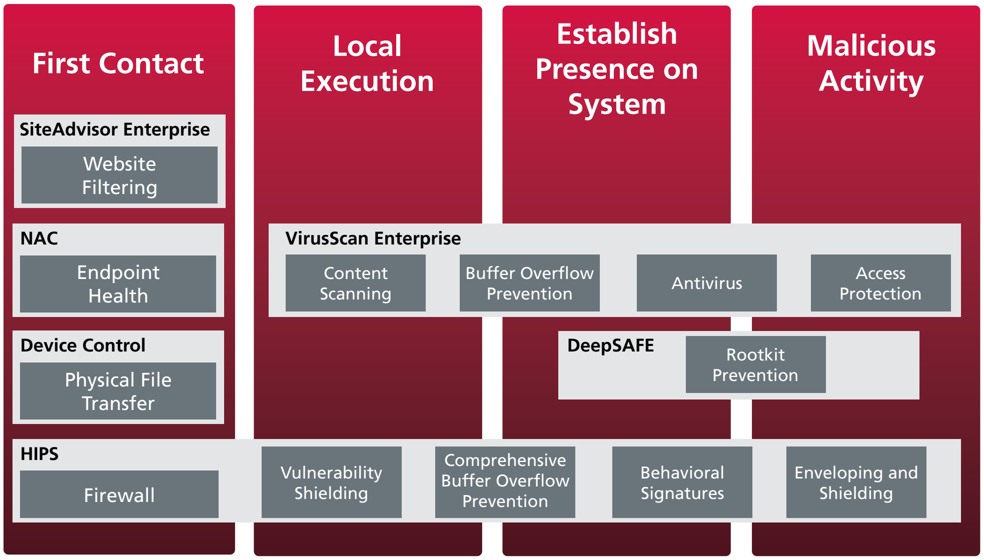
McAfee Network Access Control software for managed endpoints enables the benefits of access control adapted to your business and infrastructure. McAfee Network Access Control software supports managed users, including employees, contractors, and remote users, and offers endpoint health assessments to ensure that managed systems are compliant prior to admission. McAfee ePolicy Orchestrator and Network Access Control software can be used together to help you detect rogue and unknown devices and remediate security issues.

McAfee ePolicy Orchestrator (McAfee ePO)

For easy implementation and management, all of these endpoint protection modules are centrally managed and deployed. With McAfee ePolicy Orchestrator, you have one console, one agent, and one place to consolidate, view, manage, organize, and report on your environment. McAfee ePO can manage a mix of PCs running Microsoft Windows, Linux, and Mac, presenting status of these systems within a single console. Your management will be simplified, your visibility enhanced, and your protection will be unsurpassed.

Optional Integrations

McAfee Site Advisor Enterprise Web Filtering for Endpoint module is an optional categorization module that allows you to limit surfing to sites that you deem acceptable. It is also McAfee Web Gateway-aware, meaning that if you are connected in the office, McAfee SiteAdvisor will let McAfee Web Gateway do the filtering, and when you leave the office, SiteAdvisor will operate filtering controls on its own.



The four phases of attacks and where McAfee products fit into each one

Impact of the Solution

Imagine walking into the office in the morning knowing exactly where you stand. McAfee endpoint protection will show you if you are at risk, where you are at risk—in real time. It will tell you how many threats you have prevented in the past week or month. You will know which portion of the solution protected you. You will know that you stopped a FakeAV installation by preventing a user from browsing a malicious website with SiteAdvisor. You will know that on the last "Patch Tuesday," when new vulnerabilities were announced, your systems were protected proactively from most of them by Host IPS, from the rest by the antivirus and through McAfee Global Threat Intelligence.

You know that you no longer have the problem of users coming back from vacations and spreading infection because McAfee Network Access Control will make sure that all the proper patches and updates are applied and that the machine is healthy before it connects to the network. That machine the new maintenance crew stole last night? You can rest assured that you only lost the hardware, because the corporate data was encrypted using Endpoint Encryption for PC. The same encryption lets you give older PCs to charity complete with hard drives, without compromising your data.

You no longer have to worry about individuals leaving home with corporate data on their iPods, because you know that policies ensure that users cannot copy anything confidential to these devices. You do not have to worry about that new botnet, because the Host IPS firewall would prevent compromised hosts connecting to the botnet's command and control center. Although a brand new threat appears in the morning, you do not feel stress. You know that Global Threat Intelligence will take care of it via the antivirus, the firewall, or SiteAdvisor without deploying any emergency signatures.

By using these layered McAfee endpoint protection solutions, you will be able to reduce your operating costs by centralizing multiple functions under one umbrella. You will also increase your security against threats by having protection on all the different layers: I/O, network, memory, and web content. And you will secure each machine's data in case of loss, theft, or hardware replacement. By stopping threats before they take root on your PCs, you may never have to rebuild another endpoint.

Q&A

Do I need to install all the modules mentioned?

While you do not have to install every single module, each additional module that you install will increase your level of protection, and using them together will provide maximum protection. Keep in mind that each vector that is not protected places you at additional risk. To help you make the best decision possible, McAfee has combined many of these modules into suites that are very cost-effective compared to the standard a la carte model.

Will McAfee GTI affect my network bandwidth?

GTI uses very little bandwidth, since it uses simple DNS requests to perform its lookups. In the case of file reputation analysis, GTI is not used for every file being accessed. It is used only when a file is deemed suspicious and where there are no entries in the signature files.

What is the difference between GTI on the McAfee Host IPS firewall and McAfee SiteAdvisor Enterprise? Are they both checking the same thing?

Not quite. Host IPS firewall is a complete firewall solution and has GTI integration for IP reputation inbound and outbound. SiteAdvisor Enterprise is a web content filter that has integration to GTI at the URL level. Host IPS firewall will check to see if the IP address you connect to has a good or bad reputation. The main IP address may be good, but some areas within that website may not be. Site Advisor Enterprise will verify each URL within that IP address as you browse to it.

Additional Resources

www.mcafee.com/virusscan-enterprise
www.mcafee.com/siteadvisor-enterprise
www.mcafee.com/hips-desktop
www.mcafee.com/endpoint-encryption
www.mcafee.com/devicecontrol
www.mcafee.com/nac
www.mcafee.com/epo

Interactive Endpoint Security Suite Selection Tool:
www.mcafee.com/endpoint-product-tool

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Author

Sylvain Dumas is a Senior Sales Engineer for McAfee in Canada. He has over 25 years of experience in the computer industry. In the 1990s, Sylvain was with Wang and Banyan Systems, where he helped put in place the largest networks of the time. Sylvain joined McAfee in 1999 and has specialized in the management aspects of the product lines since then. He specializes in assisting customers to take advantage of and tie together vulnerability management, network intrusion, and risk management into a single coherent ecosystem. Sylvain is a Certified Information Systems Security Professional (CISSP).

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.