

McAfee Security Connected: Enhancing Security While Removing Barriers to Business

by Matt Fairbanks, Senior Vice President of Product and Solution Marketing, McAfee, Inc.

The traditional way of applying security countermeasures has always entailed shoring up infrastructure at one location or another and hoping that attackers will be frustrated or scared off. But this point-specific, reactive approach is bound to fail sooner or later. A good case in point: even the Great Wall of China was eventually breached. Besides, ad hoc security deployments tend to slow down business operations and negatively impact productivity. Today's enterprise needs a better security model, and that's where McAfee® Security Connected comes in.

McAfee Security Connected integrates intelligence into enterprise security to minimize risk while enabling organizations to be more agile than ever before.

- New technologies, such as Web 2.0, mix business and personal communications. IT security must have the intelligence at their disposal to provide protection nonetheless.
- An open platform enables integration and coordination of security defenses. Developers hold the key to all-inclusive enterprise protection.
- To increase operational efficiencies, security countermeasures must get out of the way
- Shared intelligence reduces risk by enabling security managers to observe threats and assess vulnerabilities before they have an impact
- Regulatory compliance can now be automated to a large extent, resulting in more accurate reports (and higher morale)

McAfee Security Connected is the new architectural framework in which security products and services work together to reduce risks while minimizing barriers to agility. It integrates and automates a wide range of security solutions. As a result, performance degradation, error messages, dependence on IT staff to plod through tedious manual tasks, and other work disruptions and delays can become rare events, or be eliminated altogether.

McAfee Security Connected protects enterprise IT infrastructure—with mobile devices and endpoints to mission-critical networks and servers; with hosted services in the cloud to supply-chain processes between partners; and with virtual desktops and servers to applications and databases. It enables employees and IT security to embrace new technological trends such as social networking, virtualization, cloud computing, and mobile connectivity. And, best of all, it redefines enterprise security by simply enabling business.

New Opportunities Present New Challenges

Web 2.0 represents a serious security challenge for everybody except hackers. After all, it's tough to keep company secrets under the best of circumstances. But when people are constantly mixing the technologies they use for business and pleasure—friending, tweeting, emailing, and texting on the company's systems and devices—how do you wall off proprietary data?

The answer is a multifaceted, fully integrated, information-sharing-based approach, and McAfee Security Connected is the model. Its protective shield includes McAfee products and solutions that, in real time, are benefiting from intelligence across solutions and sensors. These include the proactive analysis of cloud-based intelligence powered by McAfee Global Threat Intelligence™ and McAfee Labs™.

Together, they empower IT managers with the knowledge that company desktops, laptops, mobile devices, and data are free of malware and protected against theft, destruction, or mischief—or they alert IT staff to threats that require action.

An Open Platform Closes Security Gaps

There are a number of examples of what an open platform and a thriving developer community can do to enhance and extend the capabilities of a technology. Salesforce.com and the AppExchange and Apple and the App Store are two of the most prominent ones. Suffice it to say that, due to their influence, mobile devices, cloud computing, and Web 2.0 will never be the same.

McAfee is bringing the same open platform concept to security, with similar results. Many of the innovations are coming from the McAfee Security Innovation Alliance (SIA) partner program, and from in-house developers working for McAfee customers. These innovators are using the McAfee open application programming interfaces (APIs) to develop interoperable security products, and

to simplify the integration of these products within complex enterprise environments. Working together, McAfee, its partners, and its in-house developers are building solutions that cover the entire spectrum of enterprise security. Some are even using the McAfee open APIs and software development kits (SDKs) to integrate competitors' security products into McAfee-based security deployments. As a result, attacks and vulnerabilities can be tracked and resolved by all available means.

One new web API for McAfee ePolicy Orchestrator® (McAfee ePO™) software enables integration with Tivoli, Remedy, HP Service Manager, and other systems management frameworks. This added visibility into security threats and the inner workings of the data center allows for more rapid response. What's more, it reduces the training overhead that would otherwise be required due to multiple consoles and incompatibilities among systems.

Gaining Operational Efficiencies

There are many ways to increase operational efficiencies, not the least of which are to:

- Provide employees with secure, consistent access to information
- Streamline communications with customers
- Optimize business processes
- Modernize assets

Two current technology trends that touch on all of the above are virtualization and cloud computing. Regarding virtualization, security was a weak link until recently because it treated virtual machines (VMs) just like physical servers and required anti-virus scans for each VM. As many IT managers know firsthand, this can have a significant impact on performance, and can affect productivity. However, within the McAfee Security Connected framework, McAfee now offers McAfee Management Optimization for Virtualized Environments AntiVirus (McAfee MOVE AntiVirus). It scans VMs at the hypervisor level, so workloads in multiple VMs can now be protected with a single scan.

Cloud-based security can also increase operational efficiencies and reduce costs. McAfee Security SaaS solutions are instantly accessible over the Internet. By managing security on our infrastructure, we are helping enterprises reduce capital expenditures and focus scarce IT resources on other areas of business. McAfee Security SaaS delivers a complete endpoint, email, and web protection solution along with vulnerability management. It is the most comprehensive security solution available in the cloud from a single vendor.

These and other McAfee solutions that are part of the McAfee Secure Connected framework can go a long way toward eliminating barriers to connectivity, performance, and productivity.

Shared Intelligence Reduces Risk

Organizations are at greater risk today than ever before because the volume and sophistication of attacks are on the rise. A global, shared intelligence model is in order, and that's what McAfee is delivering via McAfee Security Connected. Key components include McAfee Risk Advisor that can be integrated into the McAfee ePO console or accessed from a PC, laptop, or smartphone. McAfee Risk Advisor combines threat, vulnerability, and countermeasure information to pinpoint assets that are truly at risk.

McAfee Global Threat Intelligence also adds vital intelligence to risk-reduction efforts. It tracks cyberthreats using real-time, reputation-based analysis and, through the cloud, shares this information across organizations' security infrastructure—from endpoint to network to SaaS.

In addition, McAfee offers anytime, anywhere access to the new McAfee Threat Center. It's a web portal that enables users to search and drill down into threat information across files, messages, IPs, URLs, web domains, DNS servers, applications, and vulnerabilities. There's nothing else like it in the world today.

Automating Compliance

Everyone who works to safeguard confidential data understands the value and necessity of regulatory compliance. But that doesn't make the tedium of reporting any easier to take. In McAfee Security Connected, McAfee delivers an automated security compliance infrastructure based on world-class vulnerability and threat research and policy-driven controls and content. It's a closed-loop system that remediates vulnerabilities related to application and operating system patches, backdoors, misconfigurations, password policies, malware, and more. The result is that reporting is thorough, accurate and automated, thus reducing noncompliance.

With Security Connected, You've Got Connections

Every IT manager knows the score: employees must be free to transact business using the latest digital technologies. However, those technologies must remain impervious to criminals' best-laid plans. It's a tightrope act and a huge responsibility.

At McAfee, we're working for you. McAfee Security Connected is powerful evidence.



Matt Fairbanks is senior vice president of product and solution marketing, where he oversees the global go-to-market strategy and activities for the McAfee portfolio of business security solutions. Prior to joining McAfee in 2008, Fairbanks was vice president of product marketing at Citrix Systems for the Xen virtualization and application delivery product lines.

Before joining Citrix, he led product management and product marketing for multiple business units at Symantec. Fairbanks has more than 15 years of experience in security, virtualization, storage, disaster recovery, and systems management in the IT industry.

