

# I Want Security—I Just Don't Want to Live and Breathe It

by Brian Contos, Director of Global Security Strategy, McAfee

You're being pulled in a hundred directions. You're being asked to stop this attack, support that service, talk to this auditor, and turn the Internet back on. Your budget is limited and your resources constrained. Sound familiar? If so, this brief is for you. It will highlight some of the ways McAfee has created solutions specifically to address the needs of organizations with limited IT security resources.

Regardless of the size of your business, geography, or what you do, attacks happen. Maybe you are being targeted because you have valuable information. Or maybe you will suffer an opportunistic attack—not because of the information you keep—but simply because you have the audacity to have computers and network connections, which to bad guys, means more muscle for their botnets.

We have accepted that security needs to comprise complex silos of independent controls, each requiring its own care and feeding. Every issue, every trend, and every mandate seems to have a technical point solution. The downside is that this approach has led to an explosion of disparate agents and consoles dependent on far too many resources. But it doesn't have to be this way. Complexity can be eliminated.

## Moving from Complexity to Connectedness

There are many great security products. Even though I'm from McAfee and have a scarlet letter "V" (for "vendor") emblazoned on my chest, I have no problem saying that some of these great security products are from us and some aren't. But without a connected framework across all security products, the value of each solution or product is overshadowed by complexity. For example, I like cars. If I had to understand the complexities of building cars in order to drive them, my bike wouldn't be collecting so much dust in the garage. Businesses are realizing that they have to look beyond having the right tactical point product to a more strategic, connected framework that brings together controls for endpoints, email, web, and related solutions within a centralized management console. This results in three business advantages:

- Simplified deployment and operations
- Cost effectiveness
- Improved security posture

## Simplified Deployment and Operations

Picking the right management model is essential for allowing your business to function optimally. IT capabilities and the availability of resources vary widely among businesses. Regardless of the situation, deploying and maintaining security for all desktop computers, laptops, and other endpoints, along with securing user interactions with the web and email, is essential for mitigating threats, embracing trends, and demonstrating regulatory compliance. For most employees, these IT capabilities are essential to business operations in the same way landline telephones, file cabinets, and fax machines were twenty years ago. As such, keeping them secure is a business priority for every business.

### Hackers Watch CNN

Within hours of the disasters in Haiti and Japan, there were hundreds of fraudulent websites soliciting donations.

McAfee offers two solutions that are optimized with rapid deployment and easy operation in mind: cloud-based Security-as-a-Service (Security SaaS) and self-managed, on-premises solutions. The Security SaaS model is generally well suited for businesses that have few IT resources or none at all



### With Connected Solutions, the Sum Is Greater Than Its Parts

McAfee solutions span across endpoints, email, and the web:

- Anti-spam
- Anti-spyware
- Anti-virus
- Compliance reporting
- Content filtering
- Desktop firewall
- Desktop host intrusion prevention
- Device control
- Encryption
- Network access control
- Safe web searching, web surfing, and Web 2.0 use

in-house, no desire to invest in security hardware, a large number of remote users, and little time for managing security.

The self-managed model is generally more appropriate for businesses that have sufficient IT resources and infrastructure, fewer remote users, a need for more granular control, and detailed reporting demands.

#### **Solution Delivery the Way You Want It**

McAfee offers flexible solution delivery models that include a cloud-based SaaS management model and a self-managed model.

With either choice, the various endpoint, email, web, and related controls are connected by the centralized management platforms—either on premises or in the cloud. Like an air traffic control tower, reporting, alerting, and analysis are accomplished through a single console and management, across all the solutions, has a common look and feel that's tightly integrated. This simplifies deployment and operations even for distributed environments. But simplification is only one variable, and customers everywhere are being asked to manage cost more efficiently.

#### **Botnets by the Numbers**

Today's botnet armies are a significant source of attack. To understand their size, consider these comparisons. Amazon has about 160,000 systems with 500 Gbps of bandwidth. Google has around 500,000 systems with 1,500 Gbps of bandwidth. One of the most successful bots—Conficker—had around 6,400,000 systems unwittingly under its control with an aggregate bandwidth of 28 terabits across more than 230 countries.

#### **Cost Effectiveness**

Having a centralized management solution across various security controls for more simplified deployment and operations is intuitive. But the cost effectiveness of a connected security framework might not be as obvious. Aligning security with cost effectiveness and return on investment (ROI) has always been opaque. For

decades, security companies have strived to build a better ROI calculator, and most of those calculators are now littering marketing bone-yards around the world. However, working with customers, we've discovered a number of areas where measurable financial benefits have been gained beyond the typical return on security investment calculations for measuring risk.

It's simple really. Fewer agent types yield fewer specialized consoles. And fewer consoles means a reduction in dedicated hardware, operating systems, supporting applications and databases, network utilization, and other infrastructure components. With fewer "things" running, support, licensing, and maintenance contracts are minimized. From a human resources perspective, that's less time spent on dealing with contractual and legal issues related to vendor solutions. For technical staff, that means less training is required since operations has been simplified and, because the solutions are easier to use, employees can refocus their efforts on other initiatives. So having a connected security framework really does have a positive impact on the bottom line, and as I mentioned earlier, it simplifies operations. But this is a security brief from a security company after all, so let's get into the security posture improvements.

#### **Improved Security Posture**

What good is a solution if it's easy to use and saves you money but doesn't also make you more secure? Back to another car analogy—what if you had a car that looked great, was inexpensive, but was just missing an engine? That's not an option, is it? McAfee offers a wide range of security controls for endpoint, email, web and related solutions. As discussed earlier, they wouldn't be nearly as beneficial if they didn't leverage a connected framework.

#### **Dangerous Searching**

According to McAfee® Labs™, half of the top search terms today now link to sites designed to target your system opportunistically with malware. The most dangerous searches in 2010 were:

- Cameron Diaz
- Julia Roberts
- Jessica Biel
- Gisele Bündchen

The Security Connected framework centralizes management, reporting, and alerting across all the McAfee solutions. In addition, investigations and policy setting is centralized. By itself, this is a huge advantage that reduces the time associated with discovering, analyzing, and remediating risks. But there is another layer of value that McAfee has introduced: intelligence.

McAfee has integrated its industry-leading global threat intelligence service—which enriches McAfee products with real-time threat information aggregated by millions of sensors worldwide and hundreds of dedicated McAfee engineers—into its Security Connected framework. Through this service, malware and reputation information across emails, URLs, IP addresses, domains, files, and more are analyzed, and the output is automatically made available to update McAfee products. This capability is a fundamental shift in how businesses—from the largest government organizations and global 2000s to the smallest startups—can better combat Internet attacks with virtually no user involvement required.

#### Threats

McAfee identifies one new malicious web server every 60 seconds, 60,000 new pieces of malware daily, and 5 million new zombies a month.

With the Security Connected framework, enriched with global threat intelligence, a business's security posture is improved across multiple areas, ranging from protecting endpoints against malware, safeguarding sensitive data, and removing email threats to securely searching the web, surfing the web, and using Web 2.0 services. But don't take my word for it—take McAfee solutions for a test drive, and see for yourself.

#### Next Steps

McAfee solutions are designed for affordability, practical usability, and turnkey deployment. Talk to your McAfee representative today to receive a complimentary demo or free trial and see how you can spend less time on tactical security issues, and more time on the business of doing business.

To learn more, visit [www.mcafee.com/smb](http://www.mcafee.com/smb).



**Brian Contos**, CISSP, is director of global security strategy at McAfee. He is a recognized security expert with close to two decades of security engineering and management expertise. Brian is an author of two books: *Enemy at the Water Cooler—Real Life Stories of Insider Threats* and *Physical and Logical Security Convergence*. Brian is a Ponemon Institute Distinguished Fellow and graduate of the University of Arizona.

