Is Security Driving How You Run Your Business?

Empower your organization with strategic security

"The CSO job is one of the toughest in any organisation—proving business value out of IT security is a huge challenge. The best CSOs are able to implement security solutions that are all but invisible to the business—an almost impossible task with solutions from multiple vendors. A one-vendor solution that covers all needs is the holy grail of IT security, and McAfee is striving to make this a reality."

Nigel Stanley
Practice Leader, Security
Bloor Research

It's not easy to keep an enterprise successful and secure these days. The great challenge is to create and support opportunities to thrive and improve the security posture of the enterprise. Businesses all over the world are faced with a host of challenges: an unsteady economy, growing competition, volatile global markets, shrinking budgets, and consumer uncertainty. Chief security officers (CSOs) and chief information officers (CIOs) everywhere are feeling the pressure. Their business stakeholders have a sense of urgency to trim the cost of doing business, expand into new channels, and leverage Web 2.0 technologies used on sites like Twitter and Facebook to do more business online as they cut travel expenses. Overworked IT departments are not only expected to respond to the demands of anxious business teams, they're also responsible for securing the organization and its valuable data against a raft of sophisticated new threats they've never seen before; proving their processes are internally and externally compliant; and being fiscally responsible.

That's a tall order by any measure, but visionary CSOs and CIOs are ready to adopt a new mindset about security, and the technology is available today to help them recast security as a proactive, future-driven business enabler rather than a tactical, threat-driven business inhibitor. McAfee understands that successful CIOs and CSOs no longer see procurement of security as a niche-driven activity. Instead, they are finding new ways to both deliver on business initiatives and improve the security and compliance posture of their entire organization.

Lock Down and Deny or Enable and Empower?

As a CIO or CSO, are you ready to step back from the fray and do some soul searching? Do you view security as a necessary evil or a business enabler? Do the security controls in your enterprise lock down technologies, paralyze users, and prevent them from accomplishing their business goals? Or are users encouraged and supported as they adopt new technologies to do what they need to do in various environments—with all the necessary security in place to enable them to go about it safely and freely?

Because of the way security has evolved over the years, it's rarely looked upon or fulfilled the role as a strategic business enabler. Some see it as an inescapable and often costly necessity. The approach to security is generally driven by the latest threats; it's reactive rather than proactive, tactical rather than strategic. In addition, mounting compliance regulations are forcing IT to spend more time on tedious manual processes to respond to audits and prove compliance. In a typical enterprise, security

risk management consists of a jumble of disparate products from different vendors that solve one or two threats at a time, are difficult to manage, and offer poor visibility to the company's overall security posture. In fact, the average large enterprise often has dozens of different security products and services from point product vendors. Security management becomes complex due to siloed security products and processes that drain resources, increase costs, and create security gaps. In addition, external regulations and internal policies have forced IT to spend more time on tedious manual processes to prove compliance through audits and governance. At best, this approach is costly and inefficient; at worst, it hinders IT's ability to deliver what the business needs.

Take a Quantum Leap

Security should never have been this way, and, thankfully, it won't be like this for much longer. A major shift in how security is perceived and implemented is occurring today. For many CSOs and CIOs, the opportunity to move toward an optimized security architecture is a sensible strategic direction. Imagine enterprise security that has the depth and breadth of protection to combat today's most virulent threats. Imagine enterprise security that enables optimization of security across the entire infrastructure—all devices and all networks. Imagine all of this from a single vendor. In fact, this is already a reality—with McAfee leading the charge.

As Bloor Research analyst Nigel Stanley suggests, there is light at the end of the tunnel through a single-vendor approach to optimized security. It is *the way* to ease the tension and strike a balance between seemingly competing needs with limited budgets and resources. And you can take the leap today, but what exactly are the requirements for optimized security?

"… it is the role of IT security to step up to the mark and support the safe and secure use of … business tools using a strategic approach. This is far more cost effective than tactical endpoint solutions that address the problem piecemeal."

—Nigel Stanley, Bloor Research, *Market Update: Endpoint Data Protection*, March 2009

Here are the fundamentals that support a strategic optimized approach to security rather than the tactical approach you may be accustomed to:

- *First, make security multilayered by connecting processes and intelligence across systems and networks*—Deploying a different security product for each threat that comes along is no way to ensure protection and reduce costs. Point products make multilayered protection difficult, if not impossible. Protecting data can't be limited to securing just the endpoint where it resides; comprehensive data protection requires consistent security for all devices, across all networks, data systems, and end-user devices. Think of enterprise security as a complex military defense strategy consisting of an interlocked system of weaponry and vessels along with tight coordination of personnel across all military branches. This type of integration fuels successful military operations and accomplishes so much more than any single element alone possibly could. Applying this strategy to the enterprise truly enables IT to fulfill the growing number of business requirements more efficiently while responding to threats swiftly and effectively.
- *Next, integrate compliance into your security process*—What good is security when you can't prove that you have done it right or if you don't know what data to protect so that you're in compliance with PCI DSS and other regulations? Whether driven by internal audits or external regulations, IT organizations spend an inordinate amount of time collecting data and building reports to prove they have the right security measures in place. These tedious processes are often manual and are outside the normal IT workflow. Compliance and the ability to prove compliance should be built right into your everyday security processes, so that reporting and auditing is simply an output of the work your IT team already does.
- *Take a predictive approach to new threats with real-time threat intelligence*—Moving from a reactive to an optimized state can only occur when an organization doesn't feel they are under attack all the time. Known threats can be managed, but as recent news has brought into sharp focus, new exploits are being developed around the world at an alarming rate and are increasingly more hostile. Getting an understanding of the threat horizon is critical to moving beyond a reactive approach to a proactive approach.

"Central management of a full suite of data loss and leakage prevention tools is key to a cost effective solution."

—Nigel Stanley, Bloor Research, *Protecting Enterprise Data on the Endpoint, A Strategic Approach*

- *Finally, manage security from a centralized platform*—IT organizations spend an inordinate amount of time creating and enforcing policies, performing patches and updates, and creating reports. When issues arise, siloed security products with separate management consoles lead to a string of ad-hoc communications, manual responses, and workarounds that tie up resources and introduce unnecessary levels of risk. To efficiently manage these security processes, the IT organization needs enterprise-wide visibility across systems and networks, regardless of where those systems and networks are located.

One Vendor. Many Benefits.

From the foregoing, it's apparent how optimized security makes the CSO or CIO's job easier with broad and deep protection that spans the entire IT infrastructure, automated compliance, reduced costs, and improved operational efficiency through integrated, centralized management. Through extensive global threat research, advanced technologies, and interoperable products, McAfee, the world's largest dedicated security company, is the only vendor that offers optimized security. Let's take a deeper dive into how McAfee accomplishes all this.

- *Integrated defense across networks, systems and data*—McAfee offers a broad and deep security portfolio that can "snap into" your existing architecture, leaving IT with the time and the budget to invest in new business requirements. Our best-in-class solutions, along with integrated third-party products, provide multilayered, defense in depth that spans your entire infrastructure—endpoints, networks, and data, and end-user devices.
- *Risk management and compliance solutions*—McAfee solutions automate processes such as audit reporting; policy implementation and enforcement; and vulnerability assessment and remediation. Also, through McAfee data discovery and behavioral analysis, policies dealing with information access are defined and enforced more effectively.
- *Global threat intelligence*—Through continuous, real-time detection of known and unknown threats all over the world, McAfee Avert Labs pushes updates to McAfee customers in milliseconds rather than hours or days. This predictive approach keeps protection current and helps IT act quickly when threats emerge.
- *A single, open platform to centrally manage security processes*—IT departments are more efficient when they can manage interconnected products from multiple vendors from a single platform. The architecture of our management platform, McAfee® ePolicy Orchestrator® (ePO™) software, facilitates integration of both McAfee products and products from McAfee partners. Deployment and administration of these products and communication of security data is simplified through automated processes, and the operational costs of managing security—including training—are greatly reduced.
- *Global partnerships and services*—We are committed to providing greater threat protection and operational excellence through innovation and services, including world-class implementation, training, and support delivered by us and our global partner ecosystem. The McAfee Security Innovation Alliance fosters partnerships and technology integration with strategic vendors. This further increases the depth and breadth of your protection, expands your visibility, lowers costs by taking the integration burden off your shoulders, and increases agility because our partnerships allow IT teams to respond to business needs more quickly.

Benefits of Optimized Security

- Unparalleled protection and visibility across your entire infrastructure
- Confidence in an automated compliance model
- Greater cost efficiencies
- Ability to be more agile in addressing needs of the organization

In a business context, McAfee helps you transform security from an often drama-provoking obstacle into a supportive, dutiful business enabler. Agility increases because IT can deliver on business needs—like using Web 2.0 technologies and enterprise social networking—without constraint. Business stakeholders can use the devices and access the data they need to conduct business and do so securely. And, since optimized security can be turned on when it's needed and where it's needed, it clears the path for opening new channels and new markets and communicating with customers and partners in new ways.

"During one of the greatest budget crises our nation has ever seen, cost savings must be a focal point with every transaction. McAfee solutions have not only enabled the State of New York to realize unprecedented cost savings, but McAfee security suites meet our unique needs and provide higher levels of protection at a lower cost to the taxpayer."

—Melodie Mayberry-Stewart, Ph.D.
Chief Information Officer
State of New York

A Real-World Success

The State of New York is a prime example of how optimized security from McAfee resulted in dramatic cost savings with improved endpoint protection and compliance. Facing a multibillion dollar budget shortfall, the State was looking to reduce costs yet protect its endpoints from viruses and malware as well as data breaches. To protect their endpoints, New York State agencies had implemented anti-virus solutions from a variety of vendors, but this was far from efficient and didn't give them the depth and breadth of protection they needed.

As part of its new approach to IT governance and procurement, the State standardized on McAfee across its 250,000 servers, PCs, and laptops spread throughout 106 offices and agencies statewide. This decision led to a reduction of expenses for all endpoint security licenses by 75 percent, saving the State $20 million over a three-year period. It also increased endpoint protection tenfold while decreasing long-term total cost of ownership (TCO); simplified management of endpoint security with a single, centralized console; and enabled fulfillment of the State mandate to encrypt all desktops.

The Best of All Possible Worlds—Agile and Secure

With an open, optimized security architecture, C-level executives involved in security and IT can loosen the reins and respond to business demands while confidently and efficiently meeting its responsibilities to safeguard the organization. It's time to make a bold shift and stop treating the enterprise like a maximum security prison and start treating your business like a well-guarded VIP, facilitating it as it ventures into new markets, adopts new channels, and reaches new customers in innovative ways. Optimized security creates the best of all possible worlds, a world that's secure yet agile, a world where organizations of all sizes—from 20 employees and growing to 20,000—are free to step out into the brave new world of business-enabling technologies while they stay protected. Are you ready to take the leap?

About the Author

Colin Dover, Senior Director, Interlock Marketing, McAfee, Inc.

Colin Dover is responsible for driving and communicating the McAfee enterprise strategy and vision to organizations ready to view security as a strategic, business-enabling imperative and a key architectural component in a demanding global economic landscape. A software professional with more than 16 years of domain expertise in enterprise solutions, Dover was formerly a director with Oracle's Enterprise Performance Business Unit where he worked with the world's top corporations.

About McAfee Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

6575brf_mie-osa_0609_fnl_ETMG