



# THINKING SECURITY CONNECTED



The essential guide to  
**MITIGATING RISK AND OPTIMIZING YOUR ENTERPRISE**

It's time for enterprises to rethink their security and move beyond point products to protecting their entire IT infrastructures with connected solutions. Not only for greater protection but also to address today's business challenges and drive enterprise ambitions.





Unprecedented demands are being placed on enterprise security. The definition of a network is being stretched far beyond the traditional firewalled infrastructures of only a decade ago. Data has been joined by voice and video. Users want to connect to applications and data with a variety of new and innovative mobile devices. Any time, anywhere access is becoming the norm not the exception. Cost-efficiencies are driving enterprises towards virtualization and subscription-based services in the cloud.

The increasing acceptance of Web 2.0 technologies adds to the pressure. Or should that be the confusion? And while all of this is happening, the threat from cybercrime is rising, changing, and becoming ever-more complex and targeted.

The answer for many enterprises is to deploy an increasingly complicated patchwork of independent security systems. We consider the challenges this presents and examine the McAfee Security Connected framework, the industry's first alternative for optimizing security technologies.

## CONTENTS

<b>INTRODUCTION</b>	<b>5</b>
<b>THE CHALLENGES</b>	<b>6</b>
Global threats	8
Consumerization of IT	10
Web 2.0	12
Virtualization	14
Compliance	16
<b>THE OPPORTUNITIES</b>	<b>20</b>
Know the threats you're facing	20
Have an answer for everything	22
Control everything from one place	24
Adopt an open platform	26
<b>THE ROADMAP</b>	<b>28</b>
Plan your route	28
Choose an optimized approach	30
Calculate your ROI	32

From: david@mcafee.co.uk  
 Date:  
 To: john@acme.co.uk  
 Subject: Re: How can security management make people more effective?

Hi John,  
 No problem.  
 As you know, we're seeing more and more demand for remote working.  
 In the past, we restricted access because our security wasn't up to the mark.  
 With McAfee security management, we can now secure every end-point and any device.  
 So we can grant access to laptops, mobile devices, across the Web or through the cloud.  
 Threat intelligence is also part of the package and works in the background, automatically updating and tracking the latest threats, correlating and sharing that protection across all security solutions.  
 So whatever our people come across, we're already protected against it.  
 Hope that sums it up.  
 Regards  
 David

>>David,  
 >>  
 >>We had a brief conversation in Friday's meeting regarding the new security management  
 >>solution. Could you give me a brief reminder of the efficiency benefits we can expect from  
 >>this and also tell me how we protect our people in the future — I've got a major HR presentation  
 >>coming up and I need some highlights.  
 >>  
 >>Thanks and regards  
 >>John

From: david@mcafee.co.uk  
 Date:  
 To: Lawrence@acme.co.uk  
 Subject: Subject: Re: security management and OPEX

Hi Lawrence,

- **Reduction in staff overheads** — fewer IT staff are required because with centralized security management, we no longer have to learn and operate different security consoles
- **Fewer meetings** — less interactions are needed between network, endpoint, and data teams when a breach occurs
- **Reduced time researching security issues** — security updates are now automatic, as is our security compliance infrastructure
- **Lower costs** — for support and licensing
- **Less support time** — virtual elimination of the 80 percent of IT problems previously caused by unauthorized changes

Regards  
 David

>>David,  
 >>  
 >>I know one of the big reasons for investing in the new security  
 >>management solution is that it will reduce our OPEX.  
 >>Could you give me some bullet points for the annual  
 >>report on how the savings will be achieved.  
 >>  
 >>Thanks  
 >>Lawrence

**ENTERPRISES TODAY ARE FACING A NEW ERA WHERE SECURITY THREATS ARE RISING, TECHNOLOGIES ARE CHANGING, USER EXPECTATIONS ARE INCREASING, AND REGULATORY PRESSURES ARE MORE STRINGENT.**

For years, securing enterprises has been a task driven by technological needs rather than business demands. It has also been relatively straightforward, even with ‘network creep’ extending networks beyond LANs and WANs into the remote and mobile arenas.

The result? A siloed, complex, costly, and reactive approach with security often regarded as a grudge purchase rather than a business imperative. Security products have been purchased in a piecemeal fashion, typically to recover from a security incident. Enterprises are left with a patchwork of security solutions across different levels of the business and IT architecture that can take days, sometimes weeks, to integrate and correlate. It makes enterprises harder to secure and pushes up administrative support costs, and also compromises what enterprises really need to achieve.

#### **That was then**

Enterprises today are facing a new era where security threats are rising, technologies are changing, user expectations are increasing and regulatory pressures are more stringent.

In light of this, security professionals need to have a business as well as a technology perspective. They must be able to say yes to projects that improve productivity, efficiency, and meet other challenges. By allowing staff to use Apple iPads or other consumer devices that can improve productivity, or by opening up networks and systems to the supply chain to raise efficiency and retain partners.

This comprehensive guide to next generation security looks at the drivers and considerations for a

more mature approach, with all the benefits that can result:

- ▶ Aligning security operations with rapidly-changing business demands
- ▶ Supporting and driving business innovation and opportunities
- ▶ Enabling a progression to optimized security
- ▶ Delivering the best security performance and value

It’s an integrated, connected strategy that enables organizations to manage day-to-day security issues more efficiently. By moving from a reactive mode, they can respond in real time to real world threats, divert resources to more valuable work, and stop saying no to things that can take the business forward. They can also evolve into a business enabler that can help enterprises improve day-to-day processes, enhance productivity and meet business objectives.

At the same time, the actual costs of implementing an integrated, correlated security approach can actually reduce costs by 62 percent\*, making it a business as well as an IT initiative. That’s the promise, but before a roadmap to next generation security can be planned, we need to look at the challenges—and the opportunities that can be realized by facing them.

## THE CHALLENGES

For every enterprise, there are five major security challenges that need to be considered. The implications of each need to be assessed because even if four out of the five are addressed and resolved, there will still be a weakness in any security solution.

### GLOBAL THREATS

Every day, hundreds of new websites and thousands of new users come online—and the threats increase even faster.

### WEB 2.0

New applications are opening up unexpected risks as well as welcome opportunities.

### CONSUMERIZATION OF IT

A growing wave of personally-owned IT devices and applications are being connected to networks, both locally and remotely.

### VIRTUALIZATION

Virtualization requires a different security approach in order to maintain performance yet protect a wide range of operating systems, applications and data.

### COMPLIANCE

The growing compliance burden is further complicated by the need to manage and track data on personal devices.

# Social Networks

## **SOCIAL NETWORKING SITES ARE FACING MORE SOPHISTICATED THREATS AS THE NUMBER OF USERS GROWS.**

### **The changing threat landscape**

- ▶ 50,000+ new, increasingly complex threats per day (approx 1 every 1.5 secs)
- ▶ New threat risks from Web 2.0
- ▶ New consumer devices extending corporate boundaries
- ▶ Growth of organized cybercrime
- ▶ High cost of security failure

## **GLOBAL THREATS**

The Internet is still growing at a phenomenal rate. Every day, hundreds of new websites are launched, thousands more users come online, and the volume of data and multimedia content that can be accessed increases.

But with that growth comes a rise in the threats that exist.

**The top threats for 2010 according to research conducted by McAfee Labs™ were:**

- ▶ Social networking sites are facing more sophisticated threats as the number of users grows
- ▶ The explosion of applications on social networking sites is becoming an ideal vector for cybercriminals to take advantage of friends trusting friends to click links they might otherwise treat cautiously
- ▶ HTML 5.0 blurring the line between desktop and online applications, creating more opportunities for malware writers to prey on users

- ▶ Email attachments containing malware continuing to be targeted at corporations, journalists and individual users
- ▶ Adobe software, particularly Acrobat Reader and Flash being used to deliver malware
- ▶ Banking Trojans becoming more clever, sometimes interrupting legitimate transactions to make unauthorized withdrawals
- ▶ Botnets, used for spamming and identity theft, switching to less vulnerable methods of commands including peer-to-peer setups

This increase in the number and variety of threats leaves enterprises with a problem because the blanket approach of the past is increasingly becoming unrealistic. What do they focus on? How do they target their efforts? What is important and what is simply a media story?



**58 PERCENT OF ORGANIZATIONS BELIEVE THAT EMPLOYEES FIND PERSONALLY-OWNED IT ASSETS AND APPLICATIONS EASIER TO USE.\***

## CONSUMERIZATION OF IT

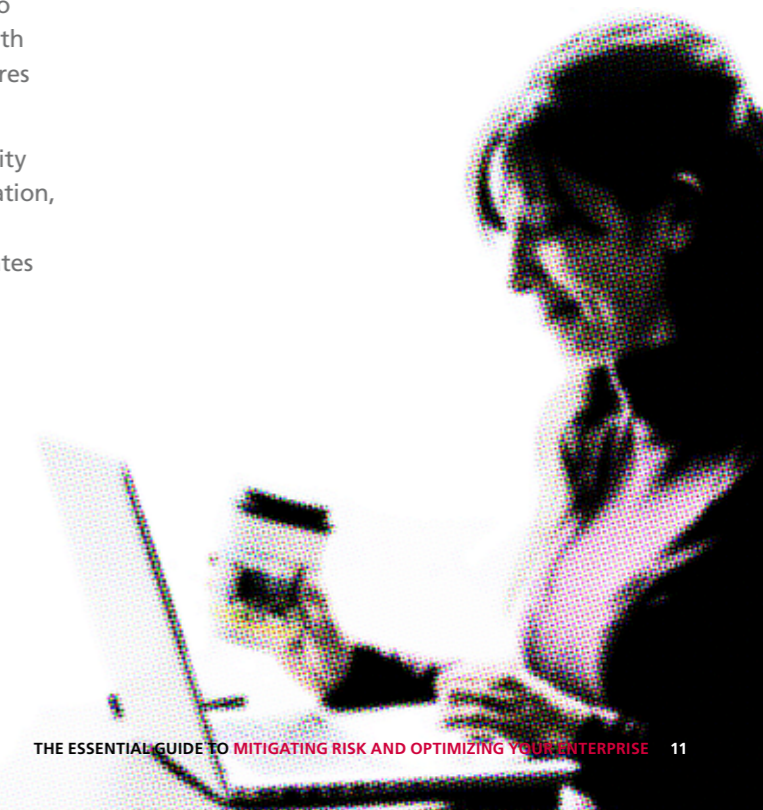
A major challenge for security teams in every enterprise is how to control the growing wave of personally-owned IT devices and applications that are being connected to networks, both locally and remotely.

Users want to access the PDAs, Apple iPads, smartphones, and other devices they are familiar with to make their working life more productive. While enterprises gain because productivity increases at little or no cost, the cost to enterprise security can be very high indeed. Especially when seen in light of the key findings from a consumerization of IT survey\*:

- ▶ Of the total organizations surveyed, 41 percent allow employee-owned IT devices access to the enterprise network on a need basis with appropriate approvals and security measures in place
- ▶ Increased productivity and greater flexibility drives organizations to adopt consumerization, cited more than half of the respondents; 58 percent believe that ease of use motivates

employees to use personal IT devices at work

- ▶ Over 50 percent of organizations consider increased employee productivity and greater flexibility and turn-around time to be the driving force behind adoption of consumerization
- ▶ 58 percent of organizations believe that employees find personally-owned IT assets and applications easier to use.\*



\* McAfee report: *Consumerization of IT: Where Are We Headed?* December 2010



**TWITTER, APPLE IPADS, AND FACEBOOK HAVE CHANGED TECHNOLOGY DRAMATICALLY. YET SECURITY STRATEGIES HAVE CHANGED VERY LITTLE.**

## WEB 2.0

There is a new generation of digital natives who are extremely familiar with the latest consumer technology.

Some have grown up alongside it and recognized its value to business. Others are new users who expect Web 2.0 style applications to be delivered to any device at work just as they are at home. They want the rich functionality and are unconcerned about the implication and risk.


These are the people who are becoming more demanding about the look and feel of applications and the availability and performance of different devices that they want to bring into the business such as personal laptops, Apple Macintoshes, and iPads.

While devices like these are easy to use, potentially improving productivity and reducing hardware and support costs, they also bring major compliance, security and risk challenges when connected to the enterprise. While technology has changed

dramatically in recent years with the launch of initiatives like Twitter, Apple iPads, and Facebook, security strategies have changed very little.

With the right level of security in place, organizations can use Web 2.0 technologies such as social networking sites to reach out to new and existing customers to drive revenues and enhance their brand image—without the fear that their brand image will be damaged through security incidents such as information leaking out of the organization or derogatory comments being placed on websites.





**WITH LOW RISK VIRTUAL SERVER SOLUTIONS NOW SITTING ALONGSIDE CRITICAL SYSTEMS IN A MULTI-TENANCY ENVIRONMENT, THE RISK PROFILE CHANGES.**

## VIRTUALIZATION

Smart devices and the consumerization of IT are causing the biggest revolution in the IT arena since the launch of the PC—and virtualization is the technology that has become the key enabler.

Server farms can be reduced in size, server utilization rates can be increased, and different operating systems and applications can co-exist without conflict.

Virtualization requires a different security approach to leverage the full benefits and ensure availability. With low risk virtual server solutions now sitting alongside critical systems in a multi-tenancy environment, the risk profile changes. How do enterprises define security policies when mixed risk models share common hardware?

Even while this challenge is being identified, considered and resolved, the next stage of virtualization—the cloud—is having a major impact on the IT and security environment.

Cloud computing provides a real opportunity to accelerate innovation and improve business processes, but it can also increase risk in terms of compliance because of the lack of clear, accountable security controls.

Security must therefore work beyond traditional boundaries and impose policies on the parties responsible for the cloud that secure the information flowing between the cloud and the business and extend protection to applications delivered and stored in third party cloud environments.





**COMPLIANCE IS ALSO  
COMPLICATED BY THE  
GROWING USE OF  
UNCONTROLLED PERSONAL  
DEVICES TO ACCESS  
CORPORATE INFORMATION.**

## COMPLIANCE

Organizations today face a wide range of compliance challenges, from internal governance that help to define the policies and processes that control the flow of information through a business, to the requirements of government regulations and industry standards.

Additional demands come from customers—there is a compliance issue that says ‘What is the risk in doing business with you, what are your network and data policies and management processes before I agree to do business?’.

That means securing information flows with customers, suppliers, partners and service providers of hosted, cloud and outsourced services. Compliance is also complicated by the growing use of uncontrolled personal devices to access corporate information.

To achieve compliance, organizations must collect a wide range of data and certify that the right security measures are in place. Collecting data from a range of non-integrated point products, however, is for many impossible and for others a hugely time-consuming task that may require manual intervention to ensure all data points are captured and adequately reported on.

### The growing compliance burden

- ▶ Sarbanes-Oxley
- ▶ Internal governance
- ▶ ISO 2700X
- ▶ Data Protection Acts
- ▶ PCI
- ▶ Customer standards



What impact will security management have on NPD?

Message

Reply Reply to All Forward Delete Move to Folder Create Rule Block Sender Safe Lists Other Actions Not Junk Categorize Follow Up Mark as Unread Junk E-mail Options

From: david@mcafee.co.uk  
 To: melissa@acme.co.uk  
 Cc:  
 Subject: Re: How will the SRM affect my NPD programme?

Sent: Wed 10/11/10

Message

Melissa,

It will make it easier.

We no longer have to configure security for each application on a case by case basis and manually configure the firewall to allow access via ticketing.

We can now map applications to the NPD user group, regardless of where they are or what device they're using.

Rather than adding to your workload, it will take weeks out of the project lifecycle.

Regards  
 David

>>Hi David,  
 >>  
 >>We're about to start another New Product Development programme with  
 >>the usual mix of freelance designers in Europe, developers in India, and  
 >>contract staff here. I'm a bit worried about the new security management  
 >>program. How will it affect the way we share files, documents, etc?  
 >>  
 >>Kind regards,  
 >>  
 >>Melissa

Security management and business process improvement

Message

Reply Reply to All Forward Delete Move to Folder Create Rule Block Sender Safe Lists Other Actions Not Junk Categorize Follow Up Mark as Unread Junk E-mail Options Find

From: david@mcafee.co.uk  
 To: jim@acme.co.uk  
 Cc:  
 Subject: Re: Security management and business process improvement

Sent: Wed 10/11/2010 09:23

Message

Jim,

**Automation** — Threat intelligence, which is part of the package and is global, automates security by tracking the entire threat lifecycle in the background.

**Centralization** — Now that everything is handled through one security management console, we need less time, training and resources to handle day to day issues.

**Compliance** — The security compliance infrastructure means we can cope with ever-increasing compliance requirements, yet reduce OPEX and achieve greater efficiencies

**Integration** — Integrated protection across the most common threat vectors means operational efficiencies can be maintained without compromising on security.

**Flexibility** — We can now connect faster and easier to staff, customers, suppliers and partners because the new system means we're dealing with polices not technical issues.

**Future-ready** — Some people are already talking about our move into the cloud. When it does happen, we'll be prepared to handle it.

David

>>David,  
 >>  
 >>Now the new security management solution is in place,  
 >>could you give me the topline improvements in business  
 >>that we can expect.  
 >>Simon has been asking about them.  
 >>  
 >>Jim



**EVERYONE WANTS TO  
COMMUNICATE EVERYWHERE,  
INCREASING FREEDOM—BUT  
ALSO INCREASING RISK.**

## **KNOW THE THREATS YOU'RE FACING**

With the increasing diversity of the IT landscape, there are many, security threats to enterprises, some deliberate, others malicious, and all of them worrying. The key point to remember is that these threats change every day.

New ones emerge, evolve and are adapted as hackers and cybercriminals seek novel ways of attacking business.

Rather than taking a blanket approach, next-generation security must therefore adopt a dynamic threat intelligence stance that focuses on the most important threats, enabling predictive solutions to guard against the latest vulnerabilities, ensure regulatory and internal compliance, and lower the cost of remediation.

It must provide protection against the latest vulnerabilities by scanning the Internet in real time to detect new and emerging threats such as advanced persistent threats, zero-day exploits, and malicious zombie senders generating spam and web attacks.

It should also offer predictive security to protect business information and reduce business risk while supporting user productivity and widespread use and adoption of high risk next-generation technologies and Web 2.0 applications.

And it should contribute to reduced costs by providing instant visibility of threats relative to your environment and prioritizing remediation efforts in the shortest possible time with minimum use of resources.

Rather than taking a blanket approach, next-generation security must therefore adopt a dynamic threat intelligence stance that focuses on the most important threats.

**ANY NEXT GENERATION NETWORK  
MUST ADOPT A COMPREHENSIVE  
THREAT INTELLIGENCE SOLUTION THAT  
TRACKS THE ENTIRE THREAT LIFECYCLE.**



**THE NEW TECHNOLOGIES, DEVICES AND APPLICATIONS THAT ARE EMERGING ACTUALLY ENHANCE THE ABILITY OF EMPLOYEES TO COLLABORATE.**

## **HAVE AN ANSWER FOR EVERYTHING**

Information is now becoming the real currency of competition. Enterprises that use the information they have intelligently gain a competitive advantage. The challenge is no longer about where to store it—it is how to access it differently.

Where enterprises once had fixed perimeters and controls, users now expect to access information and applications from any device, anywhere at any time.

Crucially for enterprises, the new technologies, devices and applications that are emerging actually enhance the ability of employees to collaborate effectively with colleagues and business partners by delivering the information they want in a quick and efficient manner.

Next-generation security must therefore be able to secure every endpoint, wherever it may be, whatever device is being used, and however information and applications are being accessed.

Any threat to that security must be recognized, assessed and responded to within a matter of minutes, not days or weeks.

**COLLABORATION IS THE NEXT BIG THING. SO SECURING ANY TIME, ANY DEVICE, ANYWHERE ACCESS IS CRUCIAL.**



**NEXT-GENERATION SECURITY NEEDS  
A CENTRALIZED MANAGEMENT  
PLATFORM THAT CAN REDUCE  
THE COST OF IMPLEMENTING,  
ADMINISTERING AND MANAGING  
A WIDE VARIETY OF CONTROLS  
FROM DIFFERENT VENDORS.**

## **CONTROL EVERYTHING FROM ONE PLACE**

Enterprises, traditionally, have a siloed approach to security. Different security measures and often different technologies are used for different endpoints because security is purchased at a local rather than central level in response to particular threats.

While this works on a day-to-day level, it can never be regarded as a sustainable solution because managing such a disparate and disorganized security approach takes up time and is open to risk.

Next-generation security needs a centralized management platform that can reduce the cost of implementing, administering and managing a wide variety of controls from different vendors. This can lower the costs of procuring the technology controls and services, as well as ongoing support and administration by up to 62 percent\*. It can also ensure that controls can more efficiently and effectively work together to reduce the management burden of protecting the enterprise.

The resultant visibility and control over all information flowing into or out of the enterprise through any communications channel, supports and simplifies internal governance and regulatory compliance, helping enterprises avoid fines and other sanctions for data breaches.

This enables enterprises to see how data moves anywhere in the business and deploy and manage security policies that can be applied to personally-owned consumer devices as well as corporate assets.



**THE KEY TO MOVING FORWARD IS NOT TO START AGAIN BUT TO CONSOLIDATE CURRENT ASSETS AND THEN OPTIMIZE THEM IN STAGES.**

## **ADOPT AN OPEN PLATFORM**

The final opportunity for creating a security approach that secures the enterprise also frees it to be open. Not to every security solution out there, but in terms of the platform that connects them together, making them easier to manage—and making risks easier to handle.

The biggest issue for many enterprises is that they have a plethora of endpoints, each secured in a different way with a solution from a different vendor.

When a risk is recognized, it can take weeks—sometimes months—to quantify it and manage it. When the opportunity for a merger or acquisition or partnership arises, it can be almost impossible to move forward because, with so many unconnected parameters, the question of risk is too difficult to resolve. When new technologies like the cloud enter the picture, the whole issue of security becomes even murkier.

One way to resolve the problem is to take a single-vendor approach. Whatever the endpoint or device, application, or user, stick with one vendor because everything is bound to work together.

Another way is to insist on pure open standards, only using solutions that are based on the same standard which can be tailored and adapted as required. Again, a great approach, but one that has no central hub or control in place, so even though each solution is based on the same standards, it is configured, controlled and managed differently. Sometimes, open can be too open.

The route that is becoming trusted by more and more enterprises is the connected route, where enterprises trust in a vendor who has already done the hard work by creating open alliances with lots of different endpoint, application and device security platforms. In this instance, a trusted management platform sits in the middle, offering a single interface to every solution.

**IT'S NOT A QUESTION OF CHOOSING ONE VENDOR. IT'S A QUESTION OF CHOOSING A VENDOR WITH LOTS OF CONNECTIONS.**





**YOU SHOULD AIM TO WORK WITH YOUR EXISTING SOLUTION, BUT PHASE OUT ELEMENTS THAT DO NOT FIT YOUR STRATEGY.**

## PLAN YOUR ROUTE

For organizations that are currently deploying point solutions, the road to a consolidated and optimized security approach follows a number of clearly defined stages with significant benefits at each stage:

**Reactive**—An incident occurs and the organization tries to respond. It deploys as little security as possible to handle the most basic threats. Risk is higher and spend is high compared to a sub-optimal level of protection.

**Compliant**—The organization demonstrates emerging policy and process definitions to meet internal compliance controls as well as external compliance requirements. Costs increase but threat levels remain.

**Proactive**—The organization begins to look at potential efficiencies from centralized management. Business processes are more mature and the organization is prepared for upcoming compliance regulations. Security measures themselves, however, are still not reactive, processes are not leveraging each other and costs remain comparatively high in line with multiple point solutions.

**Optimized**—The overall level of protection increases dramatically and the organization can respond to business requirements confidently. Threat information is updated in real time and correlated.

Information from one sensor/vector benefits other vectors. Levels of security are higher, driven by automation. Risk awareness, management and policy definition are fully centralized, and defenses are automated, multi-layered and correlated. Costs reduce significantly.

If you want to deploy a next-generation approach, there is a choice of flexible migration options. The key is to start with a centralized framework, consolidate any point solutions and integrate any future developments or purchases within that framework.

The focus of the initiative can be an event or driver like saving money, reducing data loss or opening a new data center. You should aim to work with your existing installation, but phase out elements that do not fit your strategy. New projects form convenient staging posts that can be carried out within your overall strategic framework.



**A SECURITY CONNECTED APPROACH DELIVERS REAL-TIME VISIBILITY INTO THE SECURITY AND RISK MANAGEMENT PROFILE OF ENTERPRISES.**

## CHOOSE AN OPTIMIZED APPROACH

The primary role of security is not just to protect information, but to allow enterprises to embrace change by enabling new technologies that can improve competitive performance.

The McAfee Security Connected framework protects businesses by integrating security across the extended enterprise and utilizing centralized management and real-time McAfee Global Threat Intelligence™ to mitigate risk. By taking this approach, enterprises can add value, not cost, make security operations smarter and leaner, and achieve savings of up to 62 percent in their security operations\*.

Importantly, it also helps enterprises meet the new critical security challenges:

- ▶ Protecting critical network assets
- ▶ Optimizing the data center
- ▶ Enabling new network applications
- ▶ Securing cloud infrastructure

- ▶ Securing virtualized environments
- ▶ Protecting data
- ▶ Ensuring and streamlining compliance
- ▶ Securing the productive workforce
- ▶ Securing the mobile enterprise

A Security Connected approach delivers real-time visibility into the security and risk management profile of enterprises, with self-securing networks, automatic deployment of countermeasures based on risk policy, an open platform that integrates existing business processes and security investments, and comprehensive threat intelligence that keeps security countermeasures up to date.

**MCAFEE SECURITY CONNECTED PROVIDES A STRATEGIC FRAMEWORK FOR PROTECTING BUSINESS BY INTEGRATING SECURITY ACROSS THE EXTENDED ENTERPRISE.**

\* Insight Express survey, June 2007

## CALCULATE YOUR ROI

The business benefits of moving to a next-generation security are many, but still need to be justified in terms of the results they deliver to the bottom line.

The table opposite shows the typical cost of security breaches to organizations and the calculation of risk can be compared to insurance. You can assess the number of events that occur, identify the related costs and calculate the rate of increased risk. By reducing risk, you will have fewer events and less likely costs.

However justifying security spend can be difficult, particularly for organizations that have not had a security incident and where the tendency is to discount the cost of security. In this instance, the return can be calculated based on business process improvement.

**YOU CAN ASSESS THE NUMBER OF EVENTS THAT OCCUR, IDENTIFY THE RELATED COSTS AND CALCULATE THE RATE OF INCREASED RISK.**

The results of implementing a next-generation security strategy can be measured in four areas:

- ▶ The ability to rapidly enable the business
- ▶ Greater control and management of risk
- ▶ Efficient, streamlined compliance
- ▶ Efficiencies in security operations

**THE BIGGEST CHALLENGE FOR SECURITY IN THE MODERN, DYNAMIC BUSINESS ENVIRONMENT IS TO RECOGNIZE AND UNDERSTAND THE RISK OF NEW TECHNOLOGIES AND THREATS WITHIN MINUTES, NOT DAYS OR WEEKS.**



**THROUGH THE FIRST THREE QUARTERS OF THE YEAR WE HAVE ANALYZED AND CATALOGUED MORE THREATS THAN IN ALL OTHER YEARS COMBINED, AND THE GROWTH IN BOTH VOLUME AND SOPHISTICATION OF MALWARE AND ATTACKS SHOWS NO SIGNS OF SLOWING.\***

Overall costs of an organization's worst security incident in the past year

	Organizations with up to 25 employees	Organizations with more than 250 employees
Business disruption	\$23,000 to \$31,000 Over 2 to 4 days	\$315,000 to \$610,000 Over 2 to 5 days
Time spent responding to incident	\$960 to \$11,200 2 to 5 man days	\$40,000 to \$64,000 15 to 30 man days
Direct cash spent responding to incident	\$4,800 to \$8,000	\$40,000 to \$64,000
Direct financial loss (loss of assets, fines)	\$8,000 to \$16,000	\$24,000 to \$32,000
Indirect financial loss (theft of intellectual property)	\$5,000 to \$10,000	\$15,000 to \$20,000
Damage to reputation	\$160 to \$1,600	\$24,000 to \$320,000
Total cost of worst incident on average	\$44,000 to \$89,000	\$448,000 to \$1,100,000
2008 comparison of total cost of worst incident on average	\$16,000 to \$32,000	\$144,000 to \$270,000

Source: PricewaterhouseCoopers, Information security breaches survey 2010, based on conversion rate of £1/US\$1.6



#### **McAfee Corporate Headquarters**

2821 Mission College Boulevard  
Santa Clara, California 95054  
U.S.A  
1.888.874.8766  
[www.mcafee.com](http://www.mcafee.com)

#### **Asia Pacific**

Level 20  
201 Miller Street  
North Sydney NSW 2060  
Australia

#### **Europe, Middle East and Africa**

Building 2000  
City Gate  
Mahon  
Cork, Ireland

#### **Japan**

Shibuya Mark City West 20F  
1-12-1 Dougenzaka Shibuya-ku  
Tokyo 150-0043  
Japan

#### **Latin America**

6205 Blue Lagoon Drive  
Suite 600  
Miami, Florida 33126  
U.S.A.

This 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.

McAfee and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other brands and names may be claimed as the property of others. Copyright (c) 2010 McAfee, Inc.