McAfee

The Security Paradox

The First Global Study that Quantifies the Cost of Reactive Versus Proactive Security in a Midsize Organization

The Security Paradox

CONTENTS

Foreword

Medium organizations around the globe are increasingly concerned about cyberthreats, and the rising number of incidents shared publicly certainly justifies their worries. In the first half of 2009, for example, McAfee® Labs saw almost as much new malware as it did in all of 2008. At the same time, most organizations have frozen or cut their IT security budgets. Threats up, budgets down. This is what we call the "security paradox."

Those realities are exploited by cybercriminals, who use the downturn to step up the pace. Disgruntled employees are also walking away with valued information assets, while businesses scale back on defense in an effort to get lean. And it's happening at a time when businesses can ill afford downtime, decreased productivity, stolen data, lost sales and a damaged corporate reputation.

This report quantifies security spending within midsize organizations (those with 51 to 1,000 employees). As these companies grow into larger enterprises, we wanted to examine how they allocate their security resources and dollars, particularly as they react to a growing threat landscape. In the last year, one in five midsize organizations had a security incident that directly caused their organization to lose revenue—$41,000 on average. In China, 38 percent of businesses had an incident with an average loss of $85,000. Some 70 percent of businesses believe there is some chance a serious data breach could put their company out of business. About the same number froze or cut their IT security budgets to focus their resources on building or retaining their businesses. When revenues are down, so are budgets.

The good news is that being proactive costs far less than what companies spend during remediation resulting from a cyberattack. With the right solutions in place, midsize organizations can reduce the complexity and cost of deploying and managing security—during a time when doing more with less is the number one priority.

Darrell Rodenbaugh
Senior Vice President
Global Mid-Market Business Unit
McAfee, Inc.

Methodology

For this report, McAfee surveyed companies in Australia, Canada, China, France, Germany, India, Spain, the United Kingdom and the United States. The results were then compared to previous studies conducted in Europe and North America.

The study was conducted by MSI International. Medium-sized business members of an online Internet panel were recruited to participate in an Internet survey. To qualify, the person completing the survey had to meet the following criteria:

- Be employed in a company with 51 to 1,000 employees worldwide
- Be involved in the management of IT products and services or have decision-making responsibilities for their company concerning IT and security issues
- Be employed in a company that was not considered a government-sector or non-profit organization

Approximately 100 surveys were collected in each country. The data was weighted by employee size to reflect the proportion of companies within the employee range of 51 to 1,000.

MSI International is a full-service marketing intelligence firm headquartered in Philadelphia, and has been in business for more than 15 years. In 2004, the company launched a joint venture, MSI-ITM B.V., based in Amsterdam, to specialize in Web-based marketing intelligence solutions. MSI's current clients include leading global, national and regional firms. To learn more, visit www.msimsi.com and www.msi-itm.com.

Key Findings Worldwide

56%

of midsize organizations are seeing more security incidents this year than last

29%

of midsize organizations suffered from a data breach in the last year

71%

of midsize organizations think there is some chance a serious data breach could put them out of business

37%

of midsize organizations globally spend three or more days recovering from an IT security attack

65%

of midsize organizations worldwide spend less than three hours a week on IT security

78%

of midsize organizations around the world are concerned about being a target of cybercrime

19%

of midsize organizations had an IT security incident that directly caused their organization to lose on average $41,000

40%

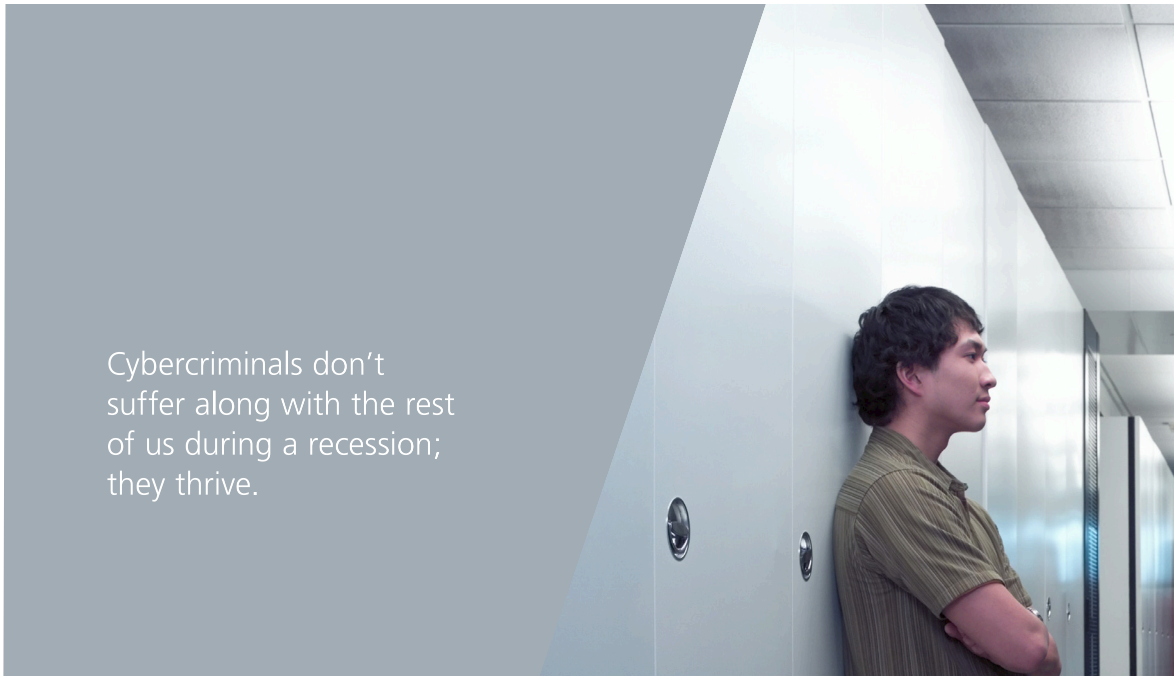
of the data lost in a security breach is the private information of customers, employees, and partners

75%

of midsize organizations cut or froze their IT security budgets in 2009

322%

the percent increase from 2008 to 2009 of average cyberattacks against midsize organizations in the United States in the last three years

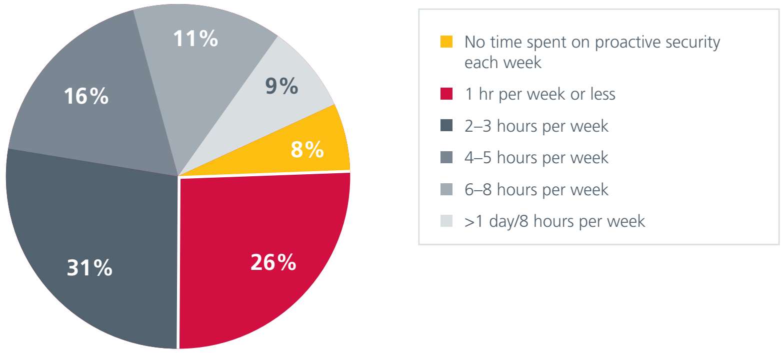


Cybercriminals don't suffer along with the rest of us during a recession; they thrive.

Threats Rise, Budgets Fall

It's far easier for cybercriminals to hack away at under-protected systems than the more-fortified ones they might have confronted in a stronger economy. They don't care if their easiest prey is a large corporation or a smaller business; hackers are equal-opportunity offenders and they can get the same payoff for a patient or customer database, regardless of where they get it.

Time Spent Weekly on Proactive Security



Even more concerning is the fact that during a recession, security threats are just as likely to come from within. Disgruntled employees who have lost their jobs in a layoff might decide to leave a virus behind or take some sensitive data on their way out.

Between threats from within and threats from the outside, companies stand to lose more to hackers than ever before. According to McAfee's *Unsecured Economies* report, companies lost more than $1 trillion last year to cybercrime. McAfee Labs believes this number will climb still further as 2009 progresses. The research team has seen almost as much unique malware in the first half of 2009 (1.2 million unique samples) as it did in all of 2008 (1.5 million).

Companies are well aware of the threats. They're not in denial. More than three-quarters of companies around the world are concerned about being a target of cybercrime. Fully 71 percent think there is some chance a serious data breach could put their company out of business. Still, an even greater number have not grown their IT security budgets this year. Nearly 40 percent of companies who are decreasing their IT security budgets in 2009 plan to eliminate or cut down on the purchase of new security products. More than a third plan to reduce IT staff, and the same number are switching to cheaper stand-alone products, while realizing that this approach sacrifices protection.

Sacrifice they do. More than half of the midsize organizations surveyed in France spend an hour or less on proactive security each week, with the result that 73 percent took longer than 24 hours to recover from a security breach. Likewise in China, 40 percent of the midsize organizations surveyed spend mere minutes on proactive security weekly and 86 percent find themselves still in clean-up mode 24 hours after an incident. Our research shows that in the past year midsize organizations in the United States have spent a total of $17.2 billion fixing IT security incidents. On average, in 2008 a single midsize organization in the United States spent more than $75,000 a year on IT security incidents.

This is what creates the "midsize paradox"—a long list of threats and the cost of ignoring them weighed against a resource investment rarely up to the challenge. Since IT professionals are cognizant of the increasing risk to their companies, not to mention its potential impact on the business's bottom line, why are security budgets still negotiable? We have a few ideas.

Worry Tempered by Size

As worried as midsize companies are about the threats to their organizations, they expect that bigger businesses are more likely targets. Almost half of midsize organizations around the world think companies with more than 500 employees are most at risk for a security attack. Many smaller organizations believe that their data is nowhere near as valuable as their larger counterparts.

There is also a feeling that "we have the right things in place for a company of our size. Let's not overbuild our security architecture." More than 90 percent of people surveyed in companies with 500 employees or fewer feel protected from cyberattacks, even though the evidence is hardly on their side.

The truth is that companies with fewer than 500 employees suffer more attacks on average than their larger counterparts. Of the midsize organizations that have had security breaches, those with 101 to 500 people have had roughly 24 incidents in the past three years, compared to only 15 incidents for organizations with 501 to 1,000 employees.

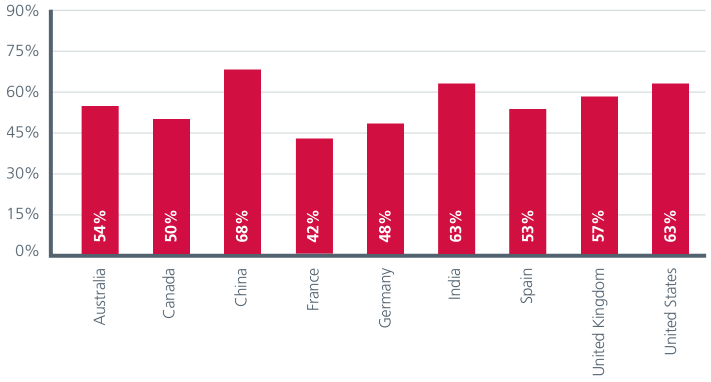
From the perspective of the criminal, this only makes sense. The bigger and more-prepared the company, the more likely it can identify the perpetrators of a high-profile attack and can afford to take legal actions against them.

The notion that larger organizations have more to fear from hackers also fails to take into account the disproportionate hit that a medium-sized business takes as a result of a security failure. This type of business is far less likely to have a contingency plan or risk fund. An attack can easily cause a midsize business to grind to a complete halt, particularly if a threat disrupts the relationship between the midsize company and larger organizations doing business with them. The larger organizations can withhold payment for services rendered, or threaten them with legal action. A single breach in this environment can put a smaller company out of business—period.

Analysis of Threats and Responces

The research indicates that the number of attacks on organizations varies greatly from country to country, as does the impact of the attacks and the time and money spent on security. Better than half of all companies are seeing more incidents this year than last, with the biggest spikes in the United States, Canada, India and China. It is unclear whether the threats that midsize organizations face come from other countries; however, McAfee's 2008 *Virtual Criminology Report* pointed to growing evidence that countries around the world are turning to cyberespionage, often with the purpose of stealing company secrets.

Threat Increase from 2008 to 2009



China has been affected the most from an increased volume of inbound threats and costs. Nearly 40 percent of businesses in China had an incident that cost an average of $85,000. In the last year, one in five midsize organizations around the world has had a single incident that cost an average $41,000 loss of revenue—losses they can ill afford to absorb during this economic crisis.

There is also a correlation between the countries that spend the most time and money on security and those that experienced the most security incidents: the United States and India. Companies in the United States spend the most time on security of any country we surveyed—four or more hours a week. And more Indian companies increased their 2009 budgets than froze them.

Unfortunately, that is not a uniform finding; and in fact, in two of the countries where threats have spiked the highest, companies decreased their budgets the most. What's more, three out of four midsize organizations did not increase their IT budgets this year, and one in five actually cut back.

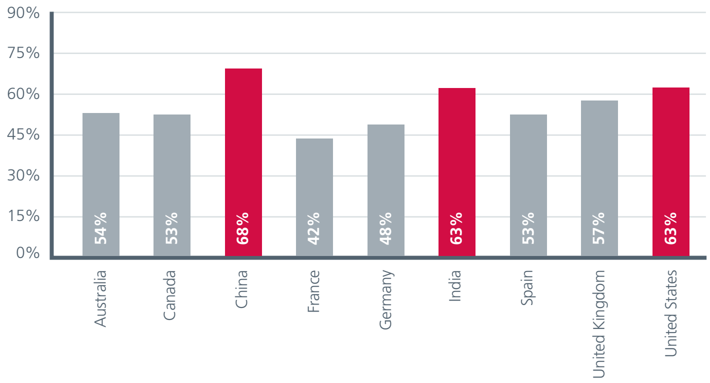
Trend data shows that most midsize organizations globally are spending the same amount of time on proactive security in 2009 as they did in 2008. Threats are increasing—but the time spent preventing attacks is not.

The numbers speak for themselves: it is more costly to remediate a successful attack than to prevent one in the first place. In the United States in 2008, midsize organizations spent a total of $17.2 billion fixing IT security incidents. What's more, according to McAfee's 2009 Unsecured Economies report, corporations lost $1 trillion worldwide as a result of data loss, both malicious and accidental.

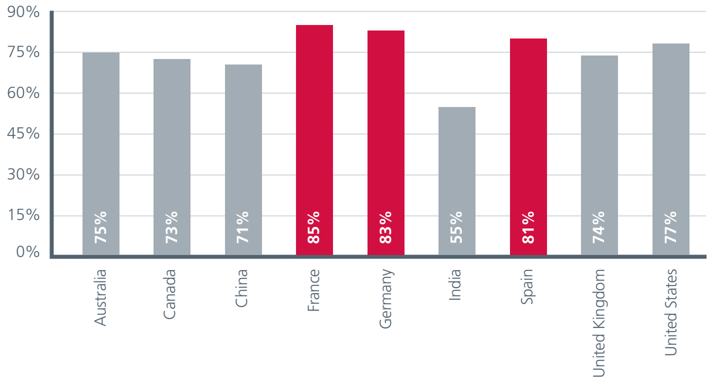
The countries where companies invest the least time on prevention suffer the greatest financial losses and downtime from cybercrime when it happens. In Canada, where 32 percent of companies spend an hour or less on prevention, just over half of the companies surveyed took a week or longer to recover from their most recent cyberattack. Similarly, in France more than half of midsize organizations spend an hour or less on proactive security each week, with the result that 45 percent took several days to recover when an incident occurred. Contrast that with the United Kingdom, where 53 percent of companies spend 2-5 hours a week on prevention. An impressive 54 percent of British companies take less than a day to get back on track after a breach. And in the United States, nearly 60 percent of companies spend four or more hours a week on proactive security; and 40 percent of midsize organizations in the United States take less than a day to recover from an incident.

Threat Versus Budget

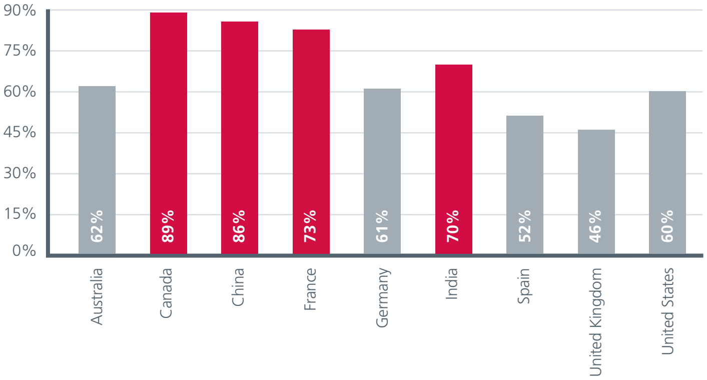
Percentage of Midsize Organizations That Have Seen an Increase in Threats in 2009



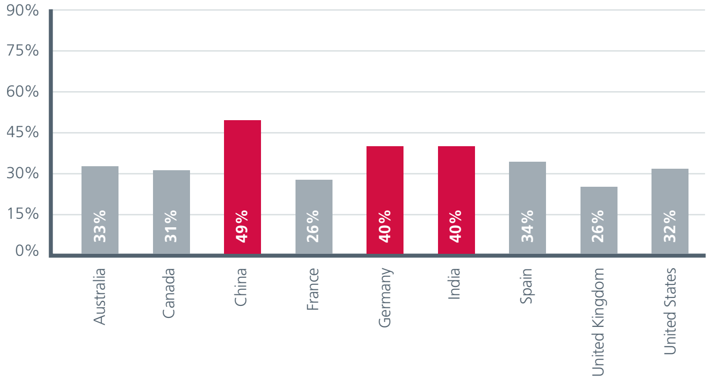
Percentage of Midsize Organizations That Froze or Cut Their IT Security Budgets in 2009



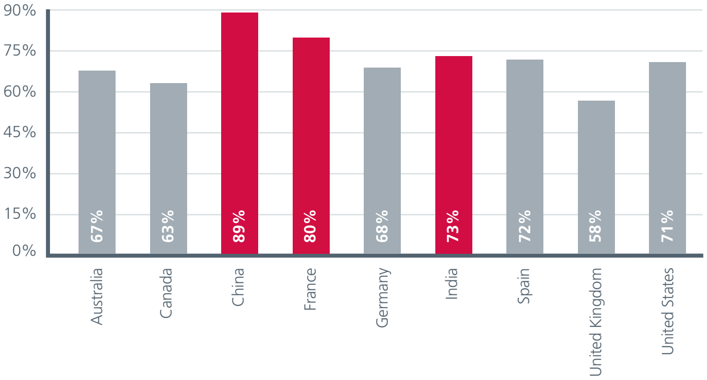
Percentage of Midsize Organizations That Took More than One Day to Recover From Their Most Recent Cyberattack



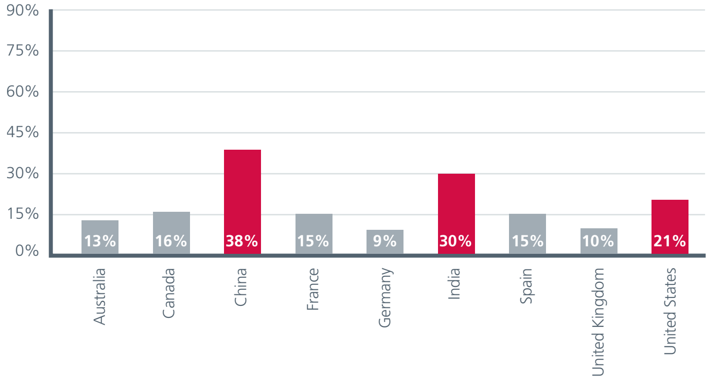
Percentage of Midsize Organizations That Suffered At Least One Data Breach Last Year



Percentage of Organizations That Think a Serious Breach Has Some Chance of Putting Them Out of Business



Percentage of Midsize Organizations That Suffered an IT Security Incident That Caused Them To Lose Revenue Last Year



The Changing Face of Threats

As we saw in 2001 and 2002, cybercrime not only increases during a recession, it takes new forms. Hackers become more industrious and more sophisticated, finding new ways to prey on overtaxed employees whose defenses fall when their workloads and worries increase. McAfee Labs is seeing an increase in password-stealing Trojans and botnets on social networking sites. The greater interactivity and richer content offered by advanced Internet technologies like Web 2.0 only makes a hacker's job easier, opening the door to socially engineered threats on popular Web sites that seem to be safe.

Stressed employees, in fear of being laid off, spend more time than ever on networking sites like LinkedIn to stay in touch with business contacts and keep on top of employment opportunities. Marketing teams who still have to get leads but have no budgets use Facebook, and sales representatives who can't travel have to use video conferencing to stay in touch with customers. Once there, cybercrooks lure them to malicious sites that steal identities, capture credit card information, or infect their company laptops with malware.

Spam may not be an especially new or exotic threat, but don't underestimate its cost to companies and their employees. Spam volumes grow by more than 117 billion e-mails every day, currently comprising some 92 percent of all e-mail. And while everyone knows the dangers of fraudulent email, phishing is still a highly profitable business: the average loss per victim is $866.

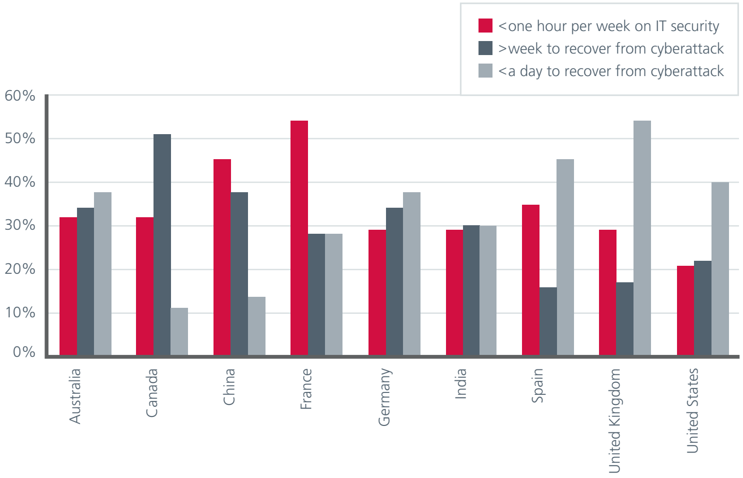
The one change (year over year) is that breaches are more quickly realized. Last year 15 percent of midsize organizations in the United States didn't even know whether they'd suffered an incident, whereas this year the number has fallen to five percent. These are very encouraging numbers, because understanding your adversaries and their methods is the first step to defeating them. We see more organizations investing in vulnerability management software to combat these threats.

To achieve the highest possible protection levels and the lowest possible risk and cost, organizations must consider an approach that incorporates these elements:

- Integrated defense across systems and networks to deliver layered protection
- Real-time threat intelligence and reputational analysis, backed by a dedicated team of security research experts
- An open security management platform that provides a singular management console and integration with multi-vendor environments

Moving from Reactive to Proactive

Time Spent on IT Security Versus Time to Recover from The Most Recent Cyberattack



The Best Defense in a Downturn

Business best practices are the same no matter what the economy or what an organization is investing in, whether it is labor or inventory or security: allocate resources where they will generate the greatest return. The equation is especially favorable when it comes to IT security, where just a few hours a week can prevent costly, if not catastrophic, outcomes.

A cost-cutting environment provides an opportunity for companies to make their IT security solutions more streamlined and effective. The result of this approach is fewer security breaches, less downtime and revenue loss, and less risk in one of the toughest economies in decades. But how exactly does a company achieve this goal?

Combining consolidated protection with centralized management is a security best practice, according to leading analysts. This combination is critical for proactively identifying potential risks and stemming loss of time and revenue. It also gives companies the greatest visibility into compliance status while lowering costs as much as 50 percent compared to a point-product approach.

- Integration—Consolidate security vendors who offer integrated suites rather than siloed products
- Centralized management—Gain greater visibility and increased control via a single management console
- Lower costs—Integrated solutions are more economical, resulting in savings in license and support costs and more efficient administration and management

This approach should extend to all five threat vectors—email, Web, networks, systems, and data —and should incorporate auto-updating to ensure that the protection is current. The solution companies choose must cover every security element: system protection beyond antivirus, Web and email security, network defense with firewalls, host intrusion prevention, network access control and data protection on every device.

With an integrated set of security offerings, centrally managed, an IT administrator at a midsize company can still dedicate the same number of hours per week while gaining a more proactive and comprehensive security coverage. McAfee's "Secure in 15" approach provides the daily practices needed to do that—in as little as 15 minutes per day.

We think that's the way security needs to be—comprehensive but easy to maintain and at reasonable cost. That way, midsize organizations can focus their efforts on what really matters: building their core business and fulfilling their mission.

For more information please contact:

United States
Tracy Ross
Director, Public Relations
McAfee, Inc.
408 346 5965
tracy_ross@mcafee.com

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.

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