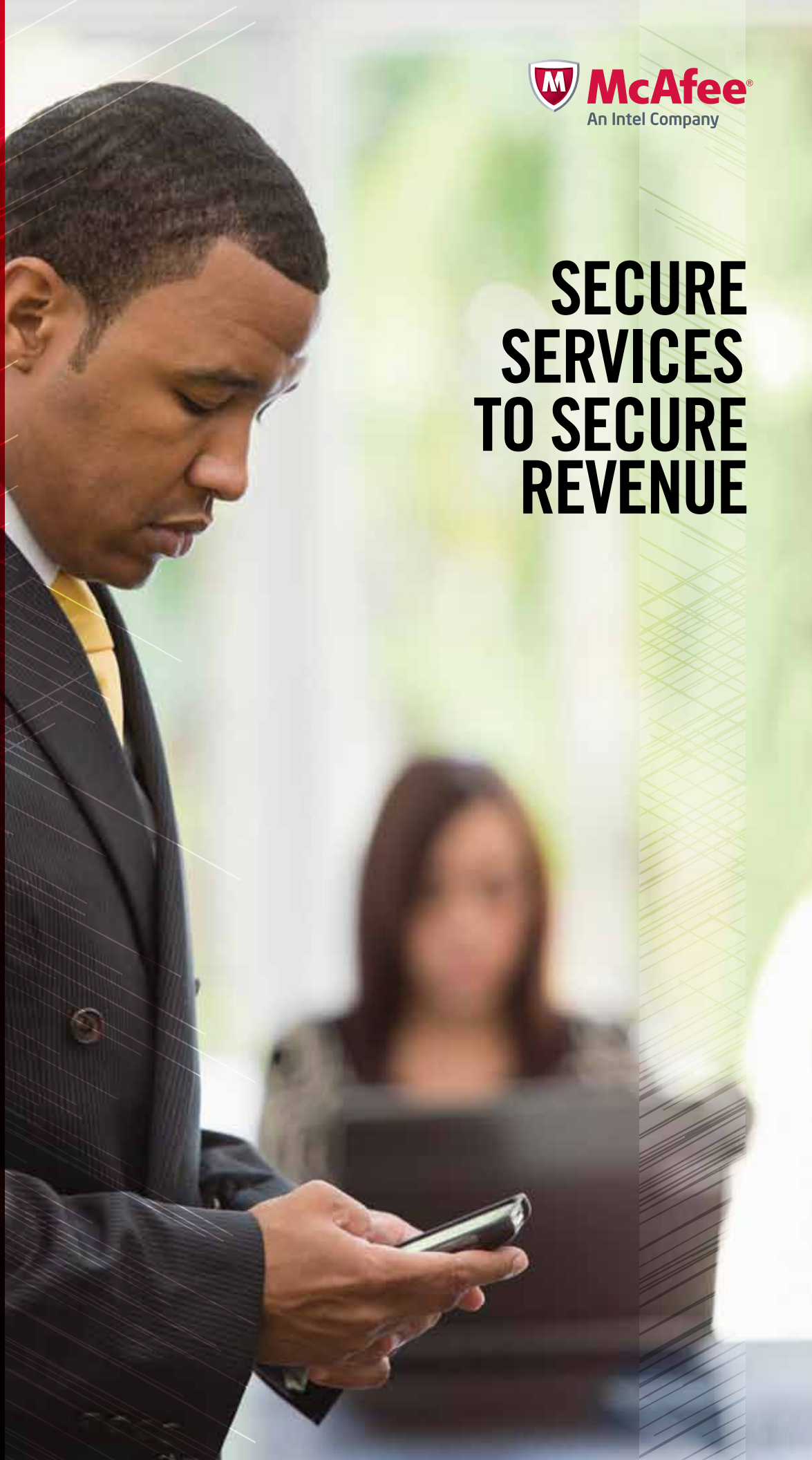
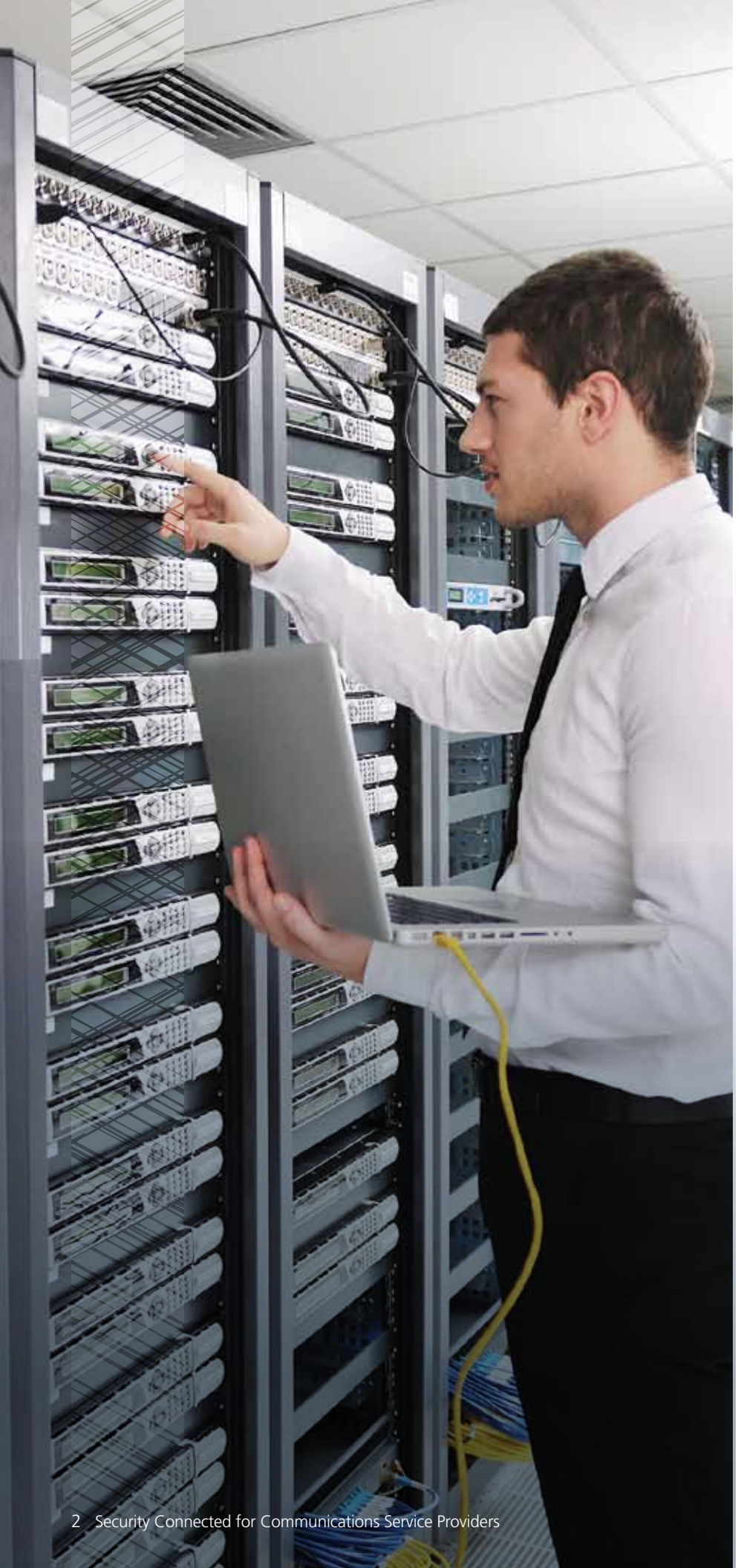
Solutions Brochure

McAfee
An Intel Company

SECURE SERVICES TO SECURE REVENUE

Security Connected for Communications Service Providers





Changing Landscape

As a Communications Service Provider (CSP), you face increasing pressure to become more agile and innovative, lower costs, and deliver revenue-generating, value-added services. Building trust with secure services and security-oriented services helps you to differentiate, create operational efficiencies, and maintain or drive up revenues in mature and emerging markets.

Being seen and performing as an industry leader is paramount. Faced with new devices, network options, and service plans, consumers and business buyers are getting savvier and more selective, placing heavy demands on telcos, carriers, and service providers to be agile, innovative, and secure.

Security Connected from McAfee can help you meet these demands through integration of products, services, and partnerships. It provides centralized, efficient, and effective risk mitigation for the issues that matter most to CSPs like you—and your valuable customers.

Partnering with McAfee will help you evolve from commodity vendor to trusted resource. You can build trust with customers and employees, be a trusted advisor to enterprises, and be the trusted provider that introduces small and mid-sized businesses (SMBs) and consumers to compelling branded security services.

For more than two decades, McAfee has helped CSPs navigate this changing landscape. We have worked with CSPs to enhance their internal security postures and have helped them position themselves as security thought leaders in their communities as they enable strong security postures for their customers.

While protecting internal assets, cost structures, and availability, CSPs can also meet revenue expectations by serving the increasing security and privacy concerns of their customer bases. Trust McAfee to help you:

- Secure your infrastructure
- Protect customers
- Generate revenue

The Secret to Attracting Customers? Trust.

Be trustworthy

Customers have choices in CSPs. Letting you sell them even the most basic access requires proof—often measured in media coverage—that you maintain a secure infrastructure for efficient, safe, and compliant processing of sensitive customer information to prevent fraud and identity theft. Since switching is simple in many markets, customer retention demands you prevent network or application downtime.

Be a trusted advisor

Enterprises partner with CSP leaders to cut costs without taking on extra risk. This means taking the security posture you have established within your own infrastructure and using it to offer strong and flexible security for your enterprise customers. Being a thought leader in security, offering the right advice, and supporting the right products means building adaptability, visibility, and intelligence into your systems so you can help businesses adapt safely to changing threats and technologies.

Be the trusted security provider

Winning in branded security services means building an infrastructure that can protect SMB and consumer customers today and easily adjust to future market opportunities and threat scenarios. You can offload the day-to-day worries of security when you are known as the trusted provider—always available, always on, never failing.

Secure Infrastructure: "Trustworthy" Starts with Secure Services

Since infrastructure change is disruptive and expensive, make sure the security you put in place for yourself is the best and most forward thinking. To do so, you need to understand the threats out there today, as well as the risks that are coming with new technologies like IPv6 and ever-evolving cyberattacks.

The stages can be seen as a lifecycle, from reactive to compliant to optimized. After surviving years of regulatory scrutiny, most CSPs are somewhere in the compliant/proactive phase. The motivation to optimize? To spend less on security while achieving a stronger security posture. Since the content below is not presented as bullets, we don't need this sentence.

We recommend looking at your infrastructure in security stages that layer security components effectively, closing coverage gaps and maintaining operational efficiency.

Basic protection

As fundamental components, do you have all the traditional security capabilities for perimeter and remote protection? Do you have secure compute stacks with optimization for cryptographic acceleration? Does your system support scalable remote access, leverage real-time threat intelligence, and provide intelligent security monitoring? These core systems offer visibility and proactive protection linked with email and web protection for comprehensive data loss prevention. These solutions are all available from McAfee and its partners as part of our Security Connected platform. We can also enhance your legacy systems through our open and extensible security management platform.

"By bringing McAfee's core security DNA within Intel, we can offer better solutions and products to the market."

—Renée J. James, executive vice president and general manager, Software and Services Group, Intel Corp.

Efficiency

Next, move on to optimizations that enable the cloud, drive down costs, and increase leverage from investments. Look for innovative tools such as hypervisor-based antivirus, soft intrusion prevention systems (soft IPS), secure virtualized storage, and remote access. For example, McAfee can employ soft IPS to look for illicit traffic that is moving through the switching fabric—not through the physical network. This system finds threats that propagate from cloud image to cloud image and may not become visible on the physical network for quite a while.

Compliance and technology enhancements

With core preventative and defensive controls in place and an efficient operational infrastructure, you are ready to support new regulations and technology options. How about adoption of IPv6 as dual stacks with IPv4 technology to support speed, volumes of users, and Internet of Things machine to machine (M2M)? Investigate hardware identification to permit reliable limits on data to comply with regulations or support multitenanting models that require your clients to prove compliance with regulations. The Security Connected platform has the extensibility and modularity necessary to plug in new technologies without forklift upgrades.

According to a GSMA study conducted by Machina Research,[1] "connected devices" might represent 24 billion devices in 2020, and $1.2 trillion in mobile service provider revenue.

Share the Security: Enhance Revenue as a Trusted Advisor

Enterprises looking to cut IT costs turn to CSPs as an outsourcing partner, enabler, and trusted advisor. They look to their CSP for guidance on services and assurance that their data is secure. The easiest way to sell security to an enterprise is to show it: display your internal security processes, results, dashboards, and reports. If you can show how you secure your own data center, for example, customers believe in your expertise. This means you have the opportunity to offer enterprises valuable new data center consolidation and cloud services.

The Managed Security Service Providers market is expected to grow at a CAGR of 17.5 percent over the period from 2010 to 2014.[2]

— *TechNavio*

As technology brings more devices into the enterprise, the reliability, availability, flexibility, cost savings, and security of the cloud will be essential in ensuring that all these services are trustworthy and operate properly. Enterprise customers are especially concerned with how to say "yes" to employees who want to bring their own devices into the network, while ensuring that data is secure. Your expertise and mobile device security infrastructure replace their concerns with confidence.

As the range of devices and implementations grows, the amount of data grows exponentially. Enterprises must manage this mountain of data while staying compliant. McAfee is helping many CSPs use McAfee® Security Information and Event Management (SIEM) technology to make sense of big security datai n billing, CRM, and ERP systems. By collecting, correlating, and sorting efficiently, they can prioritize security events from data sources as varied as M2M and IPS. Bringing this data together with dynamic risk and asset data creates a unified picture, the only way to monitor and protect what really matters. With this proven competency, you can offer these security services to your enterprise customers. Their big security data problems become your revenue opportunities.

Beyond big data, you can add value through your unique vantage point. Service providers have real-time insight into the network traffic being driven by a variety of applications and devices. You already use this knowledge to manage traffic to ensure quality of service. But, this is also a huge opportunity to pull in incremental revenue. Enterprises value data about network usage as "local intelligence" that helps them understand and perform forensics on security events. With Security Connected, local intelligence can be woven into the big security data fabric and made part of monitoring and reporting programs that help enterprises mitigate and manage risk.

Realize the Revenue: Be the Trusted Security Provider

The Security Connected platform and worldwide power of the McAfee brand can also be a launchpad for security features within your own branded and multitenant/co-hosted security offerings. You can serve as a trusted provider to businesses via multitenant Software as a Service (SaaS) platforms for small to medium business (SMB) or capture revenues from protection of consumers' full range of devices. Subscription-based security service offerings have the advantage of recurring revenue streams, since Internet-borne threats are an ongoing risk. Protection features and security signatures and behavioral rules must be updated to remain fully protected, so customers renew each year.

Mobile-only internet access is rising to 1 billion users by 2015
—Ovum

Both SMB and consumer buyers prefer to leave the security worries to someone else. They also prefer to buy McAfee. In a recent co-branding survey by Synovate, every prospect said they would prefer a McAfee-branded service to a generic or co-branded service in the service provider's name. For the specific carriers analyzed, the McAfee brand increased the likelihood to purchase by up to 16 percent.

Secure the SMB

Unlike bigger businesses that outsource security management but still like to keep products "in sight" on-premises and in managed data centers, SMB security buyers want to outsource everything. They want the same "set and forget," always-on reliability for security that they have for Internet and voice.

McAfee SaaS services are turnkey offerings for endpoint, web, and email protection designed to embed in your own branded packages. The brandable portal makes it simple for the customer to get started, and the McAfee Cloud Platform Provider program gives you a choice of managing the services yourself (OEM) or letting McAfee maintain day-to-day operations. We are committed to your success and your business model.

Court the consumer

More and more consumers are looking for core Internet security to be a seamless component of service. The service provider is their shield against hackers and viruses.

Services should support today's digital lifestyle. For example, as smartphone and tablet sales drive growth and spur your development of new networks, those devices need security and privacy features to protect users and their data. McAfee Mobile Security has been setting the pace for the consumer mobile market[3] with an expanding suite of integrated app, data, and device protections. McAfee Mobile Security has won awards and reviews from North America, Asia, and EMEA. It's a proven offering—McAfee has signed on 100 partners in the last year for McAfee Mobile Security, including Verizon Wireless, Vodafone, DoCoMo, Sprint, and Bell.

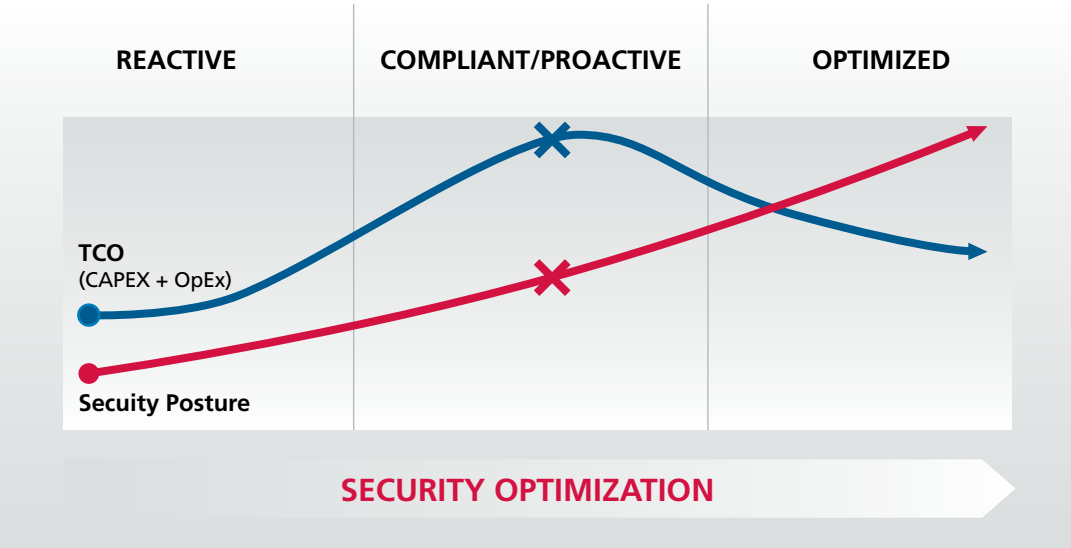
Mobile devices aren't replacing all traditional endpoints. PCs and Macs remain the biggest treasure trove of personal data for hackers. McAfee All Access includes convenient and real-time protection for consumer data and applications across the full range of Internet devices in homes: PCs, Apple Macs, Apple iPads, Google Android, and more. McAfee All Access can be the heart of your "whole home" security offering packaged with other services including broadband access, digital voice services, and content. Additionally, Intel and McAfee are building hardware-assisted security you can leverage for stronger mobile and endpoint security offerings.

SMB use of cloud resources to increase 30 percent in 2013 alone
—Telecommunication Industry Association

The Security Connected framework offers strategic recommendations for executives as well as a detailed reference architecture to guide practitioners through successful and efficient implementations. Through a focus on intelligent management, integrated solutions, and an open, partner-nurturing platform, Security Connected can help Communication Service Providers improve security postures, reduce costs, and increase agility.

"With the current paradigm shift in cloud technology and SaaS adoption, we believe that such an offering will offer tremendous value to both our partners and joint clients. We chose McAfee as our security technology partner to power our Security-as-a-Service platform because of their leadership in delivering proactive and proven security solutions."

—Kaiyang Cai
CEO, EGUARDIAN



Optimized organizations drive down cost while improving their risk management.

Connect with a Leader

McAfee understands your business and the thought leadership it requires to succeed. We have the resources to educate ourselves on your issues in technology and governance policy around services such as "clean pipes," forensics, and service contracts that enable global security. We apply this experience to refine the Security Connected approach for all three trust areas: trusted infrastructure, trusted advisor, and trusted provider.

- *Operational optimization*—We help you consolidate vendors, connect processes and data flows, leverage open interfaces, and increase real-time visibility with single pane of glass monitoring of big security data. These efficiencies: lower deployment, management, monitoring, and support costs. So you can prosper despite competitive pressures.
- *Agile*—This unique and open framework offers the capabilities, flexibility, and elasticity to help CSPs modernize legacy systems and embrace new technologies while navigating boldly through the changing business landscape and security pressures
- *Intelligent*—Take advantage of McAfee Global Threat Intelligence™—a real-time cloud-based service that helps protect our customers proactively against breaking threats. We collect billions of data points around the world, which we correlate and analyze through our advanced research systems to reveal emerging attacks and patterns across web, email, file, and network connections.
- *Modular*—CSPs who are upgrading and updating their networks can use McAfee solutions to build security into their systems and offerings over time to create the most cost-effective, manageable, and secure service delivery infrastructure. One Security Connected platform—endless uses.
- McAfee are investing in mobile security, identity, and other new initiatives like the Android Security framework and Trusted Guidance.

McAfee + Intel = Innovation

McAfee is teaming with Intel to build security into infrastructure. Through integration, we can decrease process and execution overhead and accelerate service performance. These investments help you leverage advanced security in your systems and service infrastructure without expensive consulting. We are enabling the future through ideas like hardware-assisted security and management for devices and systems and security and identity management built into core security processes and systems. The combination of Intel and McAfee is not about moving security into the hardware layer—it is about enabling security software with hardware and enabling hardware with software.

Security Connected Resources

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

Download the latest resources at mcafee.com/securityconnected.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, 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 is relentlessly focused on constantly finding new ways to keep our customers safe.

[1] http://connectedlife.gsma.com/wp-content/uploads/2012/02/Global_Impact_2012.pdf
[2] http://www.technavio.com/content/global-managed-security-service-providers-market-2010-2014
[3] http://www.businesswire.com/news/mcafee/20120402005480/en/McAfee-Mobile-Security-Recognized-Mobile-Security-App

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

56400br_telco_0313_wh