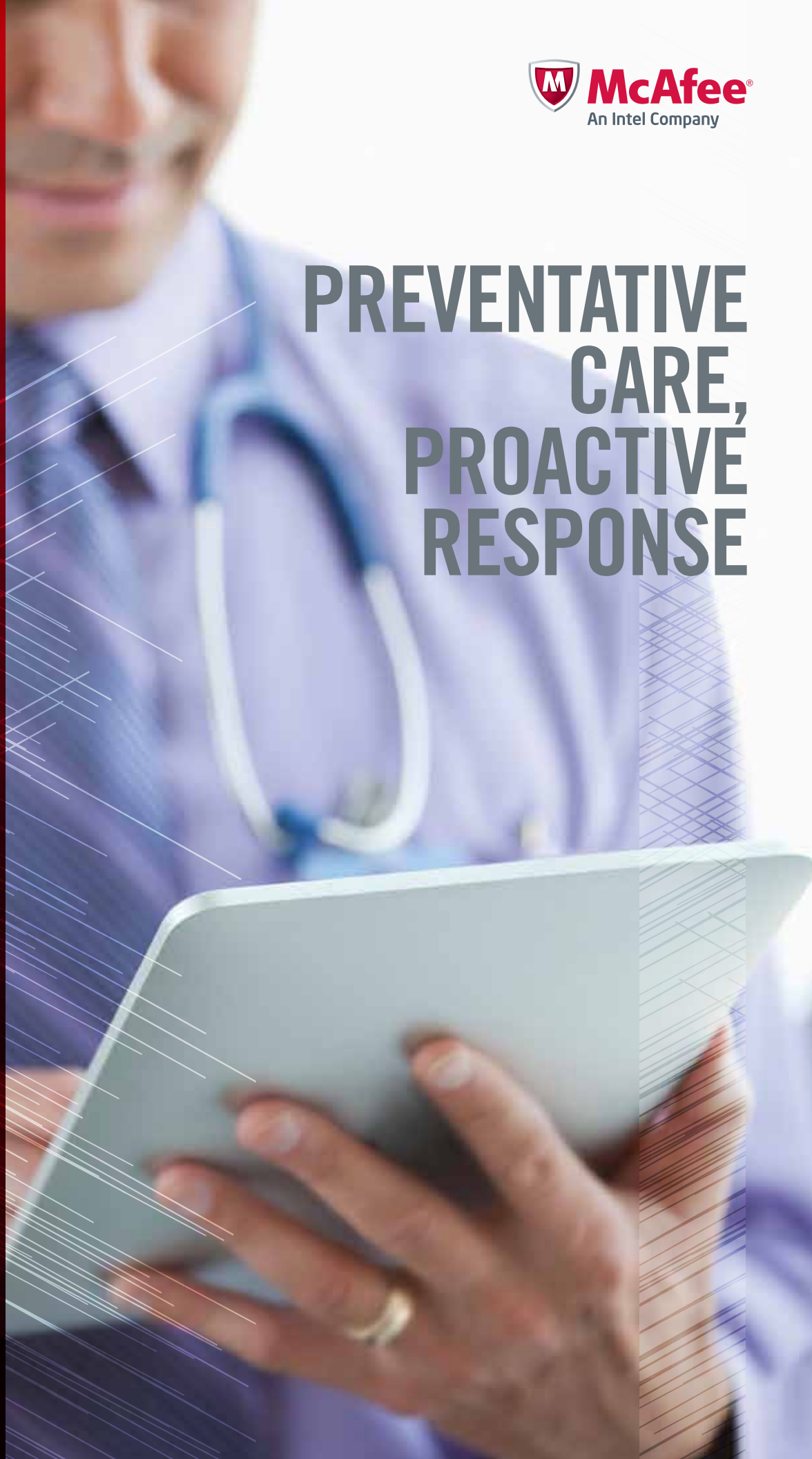


Security Connected for
Healthcare Providers

PREVENTATIVE CARE, PROACTIVE RESPONSE





Protect Confidentiality and Availability

Many security companies treat all organizations that fall within the healthcare ecosystem the same. The fact is, the security issues facing healthcare providers, such as hospitals and clinics, are very different from issues facing healthcare payers (insurance companies) and research organizations (pharmaceuticals). McAfee formulates specific solutions for healthcare providers that improve prevention, detection, and response.

Healthcare breaches increased 32 percent from 2010 to 2011, according to a Ponemon Institute study.¹ Several factors have contributed to this jump. Regulatory reforms have pushed healthcare organizations to embrace electronic health records and exchange health information, straining their security systems. Instead of hospital-provided units, physicians and nurses now carry personal devices, which introduce new risks to sensitive patient data. IT teams want to react faster to mitigate risks and know where to implement next-generation controls to ease the security burden. As the risks rise, organizations see the value of broader information security controls with event correlation and compliance support.

Security Connected from McAfee is a framework for the integration of products, services, and partnerships to provide centralized, efficient, and effective risk mitigation for the issues that matter most to healthcare providers. For more than two decades, McAfee has helped healthcare providers of all sizes enhance their security postures.

The same security issues resonate with virtually all healthcare providers:

- Securing sensitive data
- Protecting mission-critical systems
- Defending online web portals
- Managing the influx of personal devices
- Proactively managing incidents
- Continuous compliance

Defend Your Data

The healthcare industry is more connected than ever. As a result of the electronic patient data and claim handling promoted by the ARRA-HITECH Act of 2009, protected health information (PHI) has gone viral. It can be found everywhere, from mainframes to mobile devices. While designed to enhance efficiencies, electronic data and claim handling also increase risk as sensitive PHI flows from hospital departments to other organizations. Traditional network-centric solutions simply do not provide sufficient controls to protect PHI and other sensitive data from abuse.

Prevent misuse

McAfee provides security solutions for maintaining data integrity and control over sensitive information. Centrally managed, integrated host- and network-based data loss prevention from McAfee helps reduce data loss and monitor how users are interacting with data.

Encrypt your valuables

McAfee incorporates a number of encryption solutions as well as digital rights management to help protect data at rest, in use, and in motion. These controls provide a flexible and extensible solution for protecting sensitive data—from PHI and employee records to sensitive information as specified under HIPAA, HITECH, Red Flags, and various state and government regulations.

Monitor access

McAfee also provides database activity monitoring for detailed analysis of interactions with structured data contained in back-end databases. You can see the direct access by database administration tools frequently used by privileged users, as well as the indirect access via front-end applications that serve the majority of end users.

Mine for insights

Through McAfee® security information and event management, you improve visibility across these and other systems. You can analyze data about who has accessed key clinical application information correlated with where users are in the building. This sort of integration provides a broad view across the organization, showing your network as well as key data sources.

Get Systematic about Security

Healthcare providers leverage a wide range of commercial, proprietary, and legacy systems. Your networks connect fluid user communities and partners. This heterogeneous operating environment is further complicated by the fact that you have fewer IT and security resources than organizations in other business verticals.

Layer in effective protection

McAfee offers integrated endpoint security solutions that unify key protections against malware, hackers, and malicious websites. Managed at your site or through the cloud, McAfee endpoint security provides layers of controls to detect and fend off emerging threats. McAfee blacklists based on signatures and also applies heuristics to detect suspicious behavior within each host. We keep endpoint protection up to date with threat intelligence gleaned in real time from sensors around the world.

When McAfee security senses something suspicious, it consults with the McAfee Global Threat Intelligence™ (McAfee GTI™) network for the latest risk assessment. We constantly collect, analyze, and update McAfee solutions with protection against known malicious IPs, domains, URLs, emails, files, and more. McAfee Deep Defender adds a layer of defense beyond the operating system to detect and remove rootkits that might shield destructive and data-stealing malware.

Preserve integrity with whitelisting

Healthcare providers often have systems with limited operating resources, no or low network connectivity, or no way to maintain frequent signature updates—kiosks, processing terminals, and carts on wheels. McAfee whitelisting helps you ensure the integrity of these systems and minimize maintenance. With dynamic whitelisting, you allow only approved applications. This prevents the installation of malicious code, untested patches, and other unwanted software. We also minimize user-initiated changes to systems meant to have limited and specialized use, preventing disruption to operations.

Optimize for virtualization

Many healthcare organizations utilize virtual servers for efficiency and virtual desktops as a more effective way to deliver IT services to endpoints. McAfee malware protection solutions maximize virtual resource efficiency while integrating with McAfee GTI for the latest threat information. You can embrace virtualization without additional risk.

The Security Connected framework helps you achieve optimized security each day, improving situational awareness and reducing risk while driving compliance and operational efficiencies.

“The average economic impact of a data breach [to healthcare organizations] was \$2.2 million, up 10 percent from last year. In addition, most respondents believe their organization has suffered from time and productivity loss (81 percent) followed by brand or reputation diminishment (78 percent) and loss of patient goodwill (75 percent). The potential result is patient churn; the average lifetime value of one lost patient (customer) is \$113,400, an increase from \$107,580 in last year's study.”

—Ponemon Institute December 2011 Second Annual Benchmark Study on Patient Privacy and Data Security

McAfee Global Threat Intelligence™ delivers the industry's most comprehensive, real-time threat protection, providing McAfee products with deep visibility into current and emerging online dangers to activate deployment of countermeasures ahead of threats. It leverages millions of sensors and more than 350 researchers across more than 30 countries to predict, discover, research, and remediate threats across network, endpoint, and information solutions.



Open Your Online Doors Safely

Never before has so much information been so easily accessible by so many. For healthcare providers, this trend manifests as B2B and customer self-service web portals. Business partners, physicians, and patients alike want to access health information such as lab results, billing information, and prescriptions through interactive web portals. While these portals offer incredible convenience, they are also gateways to sensitive patient data. Both websites and the databases behind them are prime targets for attackers.

Defend web portals

McAfee has a wide range of products, partnerships, and services that protect web portals within your environment. Since you cannot place endpoint controls on all the systems visiting your portal, McAfee recommends robust network-based security controls to combat traditional network-centric attacks, including denial-of-service, as well as attacks that exploit web and application vulnerabilities.

Apply protection network-wide

The first line of defense for portals should be firewalls and intrusion prevention systems (IPS) that inspect network traffic. McAfee offers next-generation solutions that are application- and context-aware for precise protection. These solutions allow you to manage web-based access to your applications based on user role, such as physician, partner, or billing provider. Our network security solutions also monitor both standard and encrypted web traffic for malicious behavior and attacks, such as SQL injection. McAfee correlates data from McAfee GTI, vulnerability scans, application behavior, and system behavior to identify network attacks and automatically prevent malicious activity.

Scan for weak spots

McAfee vulnerability scanning services can also monitor your consumer-facing websites to detect vulnerabilities, misconfigurations, and malicious code that could jeopardize patient access and patient data. To help you demonstrate PCI compliance, our McAfee PCI Certification Service provides guidance, real-time analysis of your compliance status, and quarterly automated scanning of your site. This service provides dynamic port scanning, port-level network services vulnerability testing, and web application vulnerability testing to protect against exploits like SQL injection, cross-site scripting, clickjacking, and business logic attacks specifically aimed at exploiting the way applications are written.



Bring Your Own Device

Healthcare environments are exposed to the wide-scale use of personal smartphones, tablets, and laptops to access networks, applications, and data. The division between IT systems and consumer electronics devices has become blurred. Healthcare providers—historically slow to adopt new trends—need to protect their assets while facilitating this personal device revolution.

Manage the mobile revolution

Management of consumer devices involves managing access, managing and securing devices, and controlling where sensitive data resides. McAfee controls allow or disallow devices to operate on the network, regardless of whether they are laptops, smartphones, or tablets. McAfee solutions monitor and report on devices currently connected to the network and what those devices are doing. A combination of data security controls and consumer device controls means that McAfee can greatly mitigate risks to sensitive data, including its persistence on personal devices. Across multiple products and vendors, McAfee offers the ability to provision, set policies, control device capabilities, locate missing devices, and erase data on these devices. By leveraging these controls, employees can take advantage of consumer IT innovations while healthcare providers protect their businesses.

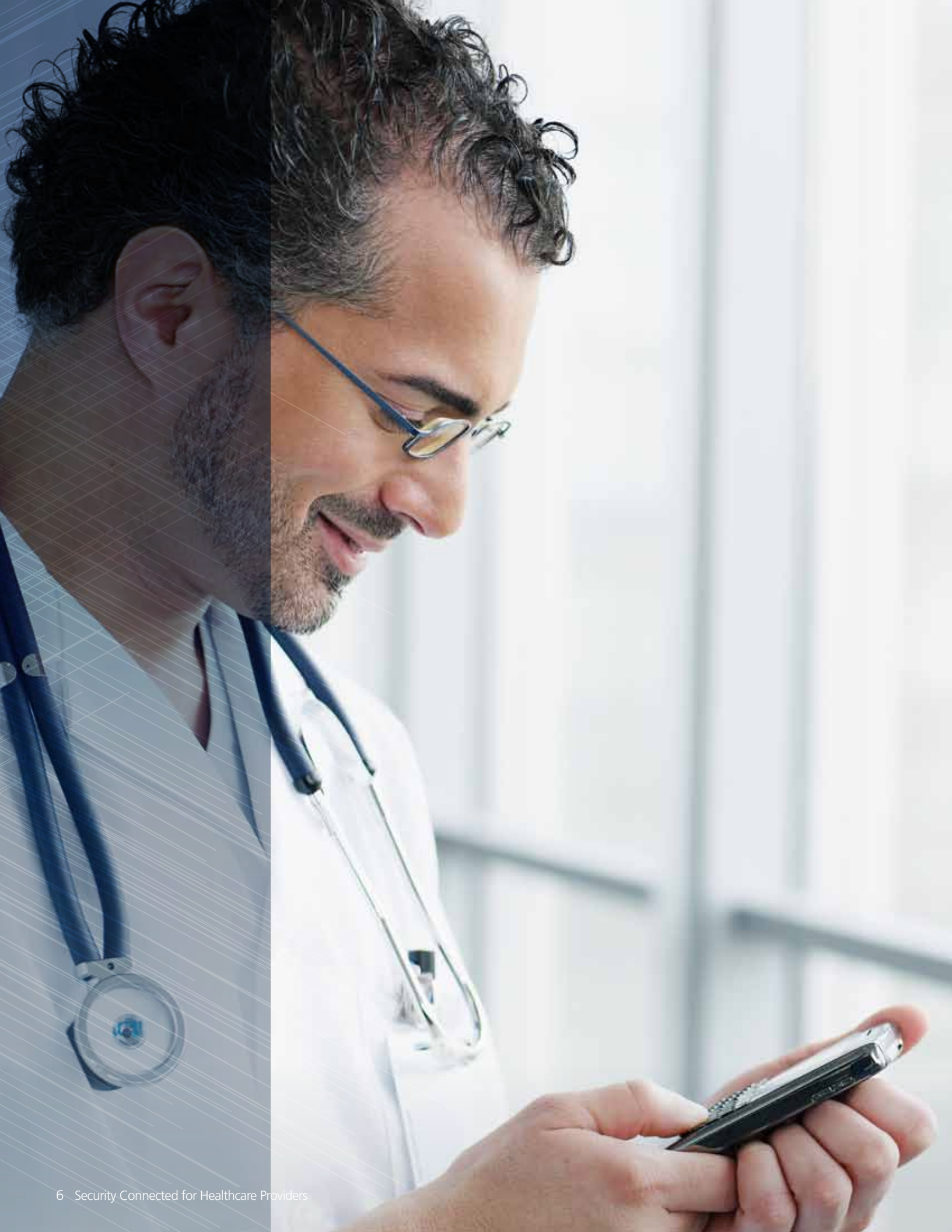
Enable access

Network access control solutions help you enforce compliance with policies before allowing laptop connections to your networks. Our mobile device security solutions properly configure smartphones and tablets to match corporate security policies and enforce compliance prior to network access.

Reduce risk

Our mobility management also automates the configuration and connectivity of VPN, Wi-Fi, PKI, and native email sync. Personalization features equip the device with a user's unique credentials to allow access to user-specific application services and enforcement of role-based policies. Mobile anti-malware and secure container options can help you keep sensitive data separate (and safe) from malicious and personal content on mobile devices.

*"Ninety-six percent of healthcare providers have had at least one breach in the last two years ... 49 percent have involved lost or stolen laptops or systems."
—Ponemon Institute December 2011 Second Annual Benchmark Study on Patient Privacy and Data Security*



Minimize Management Pain

Restricted budgets and a shortage of staffing create havoc when events require fast response and remediation. Prevention and better risk management provide measurable benefits, such as situational awareness across the organization and minimized response time. Diverse network and data-centric controls, event correlation and analysis provide insights into mitigating risk: where higher level of controls are needed and where you can leverage or optimize existing controls.

Manage events in context

McAfee Enterprise Security Manager (McAfee ESM) provides fast log and event correlation to help you manage events. It also wraps event data with additional contextual data for a rapid assessment of your security posture. Our solutions connect a real-time understanding of the world outside—threat data, reputation data, vulnerability news—with a real-time understanding of the systems, data, users, and activities inside your network. Using content awareness, McAfee ESM provides a comprehensive monitoring and reporting solution to protect patient privacy, meet HIPAA and PCI security mandates, enable safe exchange of patient health records, and meet FTC Red Flag Rules and 21CFR Part 11 requirements.

Manage assets based on risk

Integration with McAfee GTI and McAfee Risk Advisor lets you synthesize internal asset value and countermeasures and external risk factors into one risk value that you can use for analysis, threat detection, and appropriate, automatic blocking. When a new threat breaks, you'll know which systems are at risk and which systems have controls to mitigate the risk, so you can provide your staff with actionable direction. Optimizing and planning for the next security action based on the risk means more efficient and effective security.

Connect everything

McAfee® ePolicy Orchestrator® (McAfee ePO™) software works with McAfee ESM to extend visibility and control across the entire security and compliance management environment, including McAfee Security Innovation Alliance partner products. Integration with McAfee network and endpoint solutions delivers one-of-a-kind information integration, correlation, analysis, and reporting value to healthcare providers searching for a strategic platform partner, not a point product vendor.

Maintain your standards

The McAfee Security Management platform helps monitor events and create, automate, verify, and report on consistent policies to enhance and prove compliance with HIPAA, regional privacy laws, and more. To enforce compliance of endpoints distributed around healthcare facilities—large hospitals, clinics, and satellite sites—McAfee ePO Deep Command enables remote management of systems equipped with Intel AMT. A central administrator can wake up each system on demand or at a scheduled time that won't impinge on healthcare duties. This control lets you run scans remotely, apply security updates, and remediate problems, easing the burden for on-site technicians. McAfee Foundstone® consultants can also assess gaps in your organization's regulatory and compliance status and make recommendations for next steps.

Take Charge

Use the Security Connected framework to protect data confidentiality, improve availability, reduce risk, achieve compliance, and optimize operations.

- Secure sensitive data with integrated controls that integrate with your systems and processes
- Employ security controls that work in and across healthcare network zones and covered entities and support mission-critical, proprietary, and legacy systems
- Embrace web portals, web services, and mobile devices—and ensure the right controls are in place for confidentiality and compliance
- Leverage situational awareness across network and endpoint controls to proactively manage incidents based on risk
- Take advantage of solutions that are purpose-built for healthcare providers with native device and protocol support and automation for regulatory controls and reporting

McAfee can help you extract more value from security investments while enabling the improved risk postures and cost-effective security that are central to an optimized Security Connected approach.

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.

