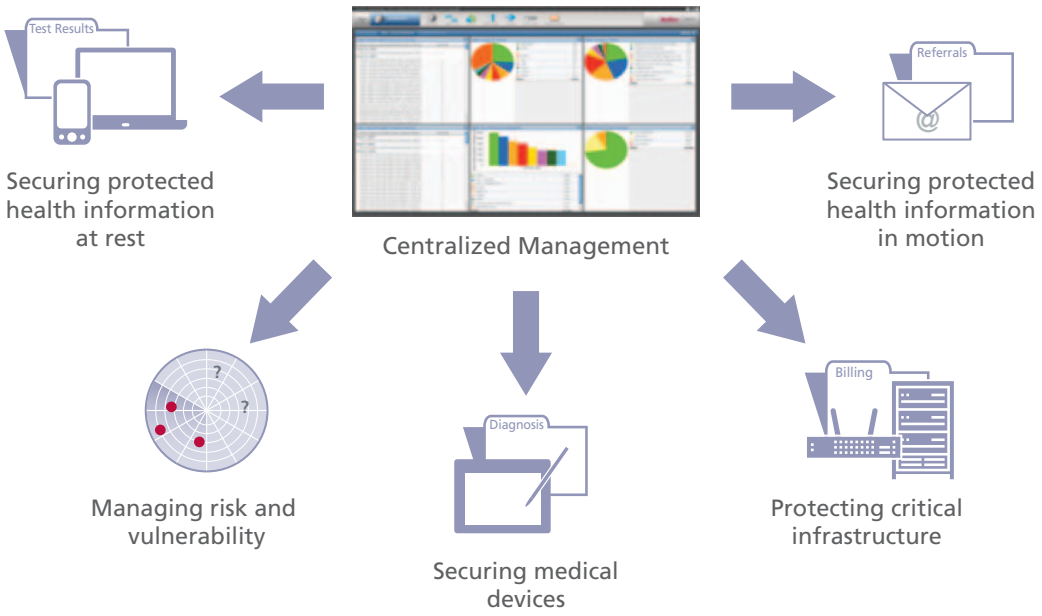
McAfee Solutions for Healthcare

Noninvasive protection for patient care

In the rapidly changing healthcare industry, doctors and other staff want greater flexibility to use new technology in the workplace. But increased flexibility also means increased risks, including data loss, vulnerability to malware, and violation of the HIPAA Privacy Rule. McAfee healthcare solutions address this need, enabling you to protect access to sensitive data, meet regulatory requirements such as HIPAA and PCI, and achieve the efficiencies necessary for success in a highly competitive industry.

Balancing flexibility and data protection has been a particularly difficult goal for the healthcare. On the one hand, the penalties for data breaches are increasing dramatically, while FDA regulations restrict changes to medical devices. On the other hand, doctors and other healthcare providers are eager for faster access to information, which helps them provide better care to patients. To achieve the promised benefits without increasing risk, McAfee recommends that healthcare organizations deploy an optimized security architecture.

McAfee's optimized security architecture provides protection against emerging threats while enabling healthcare providers to utilize the latest technologies. McAfee provides this protection while reducing the security footprint (or overhead), not only facilitating the free flow of secure information, but also reducing IT resources required to implement and maintain secure access. With McAfee, healthcare organizations reduce the cost of security and minimize their risks, and doctors gain efficiencies and improve their ability to deliver excellent care.



Security is an Important Part of Your Health Information Systems

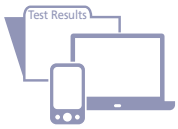
Electronic health information systems (HIS) promise to reduce operational expenses, increase productivity, and improve care quality. Security must be considered when implementing an HIS. Providers need be sure that their security matches their new electronic environment. It is no longer enough to install anti-virus and assume that health information and systems will remain secure.

Increasing Risks (and Penalties) for Healthcare Organizations

In February 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act increased penalties for North American healthcare providers guilty of data breach. It provided for:

- Stronger powers of enforcement by state Attorneys General
- Increased monetary penalties for breaches
- Mandatory disclosure requirements for data breaches
- Required compliance audit within 12 months

McAfee solutions for healthcare providers share a centralized security management platform to reduce the maintenance burden for security and regulatory compliance. The centralized security management platform enables data security, network security, policy management, monitoring, auditing, and the reporting required for PCI and HIPAA compliance.

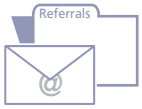


1. Securing Protected Health Information at Rest

Risk: The use of laptops and mobile devices increases the risk that protected health information (PHI) will be accessed by unauthorized individuals. A lost or stolen device with unencrypted data constitutes a breach if the device is secured with only simple password protection and contains any unsecured PHI.

McAfee solution: Protects devices with easy-to-manage, low-footprint encryption that meets HIPAA/HITECH encryption levels, minimizing the possibility of data loss and the subsequent need to send breach notifications.

- *Full-disk encryption*—Secures patient data on laptops and computers
- *Mobile device encryption*—Encrypts data (including classified mail) on mobile phones
- *File/folder encryption*—Automatically encrypts files copied from a server
- *Removable media encryption*—Automatically encrypts data copied to USB drives
- *Virtual disk encryption*—Supports virtual environments
- *Device control*—Limits which USB devices can be attached to a computer

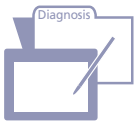


2. Securing Protected Health Information in Motion

Risk: Transmission of protected health information across a network through unprotected email or other electronic file transfers increases risk of data breach.

McAfee solution: Transparently encrypts data transmission and monitors patient information to prevent inadvertent or malicious transmission via email, instant messenger, printing, web, etc., whether by staff or malware.

- *Network data-loss prevention*—Transparently analyzes the network to prevent loss
- *Host data-loss prevention*—Blocks PHI data from being sent by a computer
- *Encryption of emails*—Ensures PHI information is always encrypted in transit
- *McAfee eBusiness Server*—Encrypts and compresses information between servers



3. Securing Medical Devices

Risk: Malware can disrupt not only computers but other healthcare devices. Because of their operating systems, MRI machines, heart rate monitors, and tablet computers are also susceptible to malware that spreads across a network.

McAfee solution: Protects medical devices such as medical tablet PCs and other thin client devices along with MRI-CAD scanners. Prevents attacks with low-footprint integrity checking and is incorporated into more and more vendors' premarket approved builds

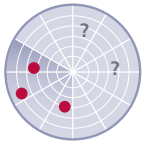
- *Application whitelisting*—Prevents installation of unwanted programs
- *Change control*—Manages software installation and upgrades and prevents unapproved changes
- *"Gold master" comparison*—Checks that devices have not been modified
- *Vulnerability scanning*—Identifies systems at risk and correlates threats to risks

4. Protecting Critical Infrastructure

Risk: Disruption to clinical services and billing can occur if poor protection allows external attacks to disrupt critical infrastructure or compromise PHI. Damage to reputation can also occur.

McAfee solution: Utilizes real-time global threat intelligence to stay ahead of changing threats, helping you avert system downtime and unauthorized access of PHI.

- *Anti-virus and anti-spyware*—Includes malware detection and removal
- *Host intrusion prevention*—Includes vulnerability protection and application blocking
- *Application whitelisting*—Allows only approved applications to run on a protected device
- *Change control*—Manages software installation and upgrades and prevents unapproved changes
- *Firewall*—Provides defense from network-based attacks
- *Network IPS*—Provides network-based malware protection
- *Email and web security*—Protects against spam and malware as well as outbound data loss
- *Vulnerability scanning*—Identifies systems at risk and correlates threats to risks



5. Risk and Vulnerability Management

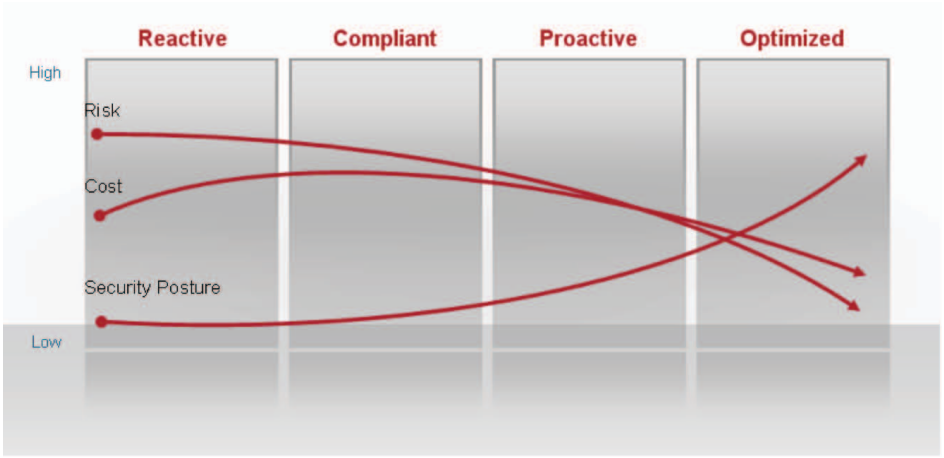
Risk: This difficulty of tracking vulnerable devices and the location of protected health information increases the potential of a data breach and possibility of willful infringement penalties.

McAfee solution: Provides data discovery and vulnerability management to identify, prioritize, and mitigate the risks associated with external and internal threats and data theft.

- *Data discovery*—Scans accessible devices for sensitive information such as PHI
- *Vulnerability scanning*—Identifies systems at risk and correlates threats to risks
- *McAfee Policy Auditor*—Automates processes for internal and external IT audits
- *McAfee Remediation Manager*—Automates remediation of policy noncompliance
- *McAfee Risk Advisor*—Proactively correlates threats, vulnerabilities, and countermeasures
- *Vulnerability and risk assessment services*—Provides expertise to help you assess your risks

Optimized Security Architecture—The Value We Offer Organizations Like Yours

No one is better positioned than McAfee to relentlessly tackle threats from every angle and help you safeguard your patients, users, networks, and billing systems. McAfee solutions, technologies, and award-winning global research team cover the full spectrum—the endpoint, the network, the gateway, the Internet, and all points in between.



McAfee enables you to move from reactive to optimized—and in the process, reduce risk and cost.

Multilayered security connects processes and intelligence across systems and networks. McAfee's integrated approach accomplishes more than any single element alone, enabling IT to fulfill business requirements more efficiently while responding to threats swiftly and effectively.

Compliance is integrated into your security process. With McAfee, compliance and the ability to prove compliance are built right into your everyday security processes, so that reporting and auditing is simply an output of the work your IT team already does.

McAfee Global Threat Intelligence offers a predictive approach to new threats. A better understanding of the threat horizon is critical to moving from reactive to proactive.

McAfee's centralized platform manages your entire security portfolio. To efficiently manage all security processes, the IT organization needs visibility across systems and networks, regardless of where those systems and networks are located.

Through our broad solutions, centralized management, integrated compliance, and Global Threat Intelligence, McAfee enables you to more effectively protect your patients, staff, systems, and data.

About McAfee

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. http://www.mcafee.com.

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

7192brf_sol-healthcare_1009_ETMG