Solution Brochure

Protect, Detect, Correct

Security Connected for Healthcare Providers

McAfee is now part of Intel Security.

With Security Connected, healthcare providers can reduce risk and response time and lower overhead and operational staff costs.

Some 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). Intel Security provides specific solutions for healthcare providers that improve protection, detection, and correction.

The high black-market value of healthcare data and personally identifiable information (PII) has led to attackers targeting vulnerable healthcare infrastructures, including ubiquitous mobile devices. Patients are also more educated and adamant about asserting their privacy rights, even as they demand more convenient access via mobile apps, wearable devices, and patient portals.

Under pressure from regulators and the public, healthcare IT teams want to react faster to detect and mitigate risks and know where to implement next-generation controls to ease the security and compliance burden. As the healthcare industry becomes more competitive, IT teams also are expected to enable new patient-facing services, from Wi-Fi throughout the hospital environment to advanced digital medical systems.

Protect Confidentiality and Availability.

Organizations are discovering the visibility and efficiency of broader information security controls united by event correlation, contextual analytics, and compliance audit and enforcement. Enabling this optimized environment, the open Security Connected platform from Intel Security offers a unified, adaptive architecture to help reduce risk and response time and lower overhead and operational staff costs. Products, services, and partners use a common management platform and share context-specific data in real time. They act as a team to keep patient health information confidential and ensure that hospital and IT networks remain available.

The same security issues resonate with virtually all healthcare providers:

- Securing sensitive data against loss and attack.
- Protecting mission-critical systems.
- Defending online web portals and mobile apps.
- Managing the explosion in digital devices and the Internet of Things (IoT).
- Proactively managing incidents.
- Continuous compliance.

Start With a Checkup.

Just like a patient, a healthy healthcare infrastructure requires regular checkups, and every outcome is a bit different. McAfee® Foundstone® Professional Services can help with strategic and technical consulting services, such as risk assessments, penetration testing, data loss prevention (DLP) assessments, compliance checks, and evaluation of your incident response program. Based on your situation, we can then prescribe, prioritize, and help you achieve the people, process, and technology changes appropriate to strengthen your security posture.

Defend Your Data.

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 medical and 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.

Prevent misuse and data loss.

McAfee, a part of Intel Security, provides security solutions for maintaining data integrity and control over sensitive information. Centrally managed, integrated host- and network-based DLP helps reduce data breaches and monitor how users are interacting with data. DLP filtering on email and web gateways can block exfiltration of PHI, as well as other regulated data, such as credit card and employee information.

Block phishing and malware.

Determined data thieves will use customized software to penetrate your network and attack your data. Many attacks start with phishing of healthcare workers—one wrong click, and attackers can download files that steal credentials. Attackers are then free to navigate your applications and databases. By using advanced malware engines on your gateways, you can block phishing links and malware downloads.

Encrypt your valuable data.

We offer a number of encryption solutions to help protect data at rest, in use, and in motion.[1] Flexible and extensible controls secure sensitive data—from PHI and employee records to the information specified under HIPAA, HITECH, Red Flags, and various state and government regulations. These encryption solutions protect a wide variety of endpoints such as laptops, tablets, and smartphones, as well as removable media.

Monitor access.

We also provide database activity monitoring for detailed analysis of interactions with structured data contained in back-end databases. You can view 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 Enterprise Security Manager, our modular security information and event management (SIEM) platform, you can improve visibility across these and other systems, upgrading your understanding of risks as well as your ability to detect and respond to advanced attacks. For example, you can analyze data about who has accessed key clinical application information correlated with where users are in the building and the normal baselines for users and applications. Watchlists can look back in time, backtrace interactions around key data events, and monitor for future activity to match your monitoring preferences.

“My advice to anyone looking at security solutions is to focus on integration. Now that we’re using McAfee, we can go to McAfee ePO software and pull mountains of data or use the SIEM solutions from McAfee to quickly and efficiently find the root cause of an issue. The time-to-value is almost instant—and that is beyond beneficial.”

—Andrew Howard, Security Officer, Texas Tech University Health Sciences Center

Detect and Deflect Before Damage Is Done.

Intel Security products leverage integrated global threat intelligence to provide the broadest threat data, deepest data correlation, and most complete product integration in the market. This gives Intel Security products unique visibility into online dangers such as botnets, worms, DNS attacks, and even advanced persistent threats (APTs).

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. Open and integrated security allows these systems to share data securely, while supporting your requirements for actionable intelligence, ubiquitous monitoring, and continuous compliance.

Layer in effective protection.
Intel Security offers integrated endpoint security solutions that unify key protections against malware, hackers, phishing, and malicious websites. Managed at your site or through the cloud, Intel Security endpoint security provides layers of controls to detect and fend off emerging threats. Blacklists are based on signatures, and heuristics are applied 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.

Fight zero-day and unknown malware.
Endpoint suites can work with the McAfee Threat Intelligence Exchange and network and content security products to detect, analyze, convict, and immunize your systems against emerging advanced malware. When endpoints encounter new and suspicious files, they can ask the exchange for a risk assessment. While traditional advanced forensics require specialized tools and training and a great deal of manual effort, McAfee Threat Intelligence Exchange turns intelligence into automated protection driven by IT’s rules.

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. Whitelisting, which is available in suites or as a standalone technology, 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 use virtual servers for efficiency and virtual desktops as a more effective way to deliver IT services to endpoints. Our malware protection solutions maximize virtual resource efficiency while integrating with McAfee Global Threat Intelligence (McAfee GTI) for the latest threat information. You can embrace virtualization without additional risk.

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.

Intel Security 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, we recommend 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. Intel Security 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. These solutions correlate data from McAfee GTI, vulnerability scans, application behavior, and system behavior to identify network attacks and automatically prevent malicious activity.

Solving the Device Dilemma.

From initially blocking mobile device use in hospitals, many healthcare environments now promote mobile devices, but must still contend with the diversity of personal smartphones, tablets, and laptops used to access networks, applications, and data, as well as many types of specialized medical devices and wearable sensors. Thoughtful controls can protect assets while facilitating personal device preferences and new digital-enhanced services.

Manage the mobile reality.

Management of consumer devices involves managing access, managing and securing devices, and controlling where sensitive data resides. Our controls can allow or disallow devices to operate on the network, regardless of whether they are laptops, smartphones, or tablets. Intel Security 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 you can greatly mitigate risks to sensitive data, including its persistence on personal devices. Across multiple products and vendors, we offer 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.

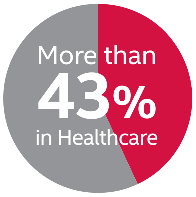
Enable access.

Network access control solutions from the Intel Security Innovation Alliance partners 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 is part of our endpoint security suites. It 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.

Correct and Comply.



According to Identity Theft Resource Center's 2013 annual list of security breaches, the healthcare sector accounted for more than 43% of all the breaches listed.[2]

Minimize Management Pain.

Restricted budgets and a shortage of staffing create havoc when incidents require fast response and remediation. Integrated management and workflows support better and more efficient risk management with measurable benefits, such as situational awareness across the organization and minimized response time. With Security Connected, diverse network- and data-centric controls, event correlation, and analysis provide insights into mitigating risk: where new or next-generation controls are needed and where you can leverage or optimize existing controls.

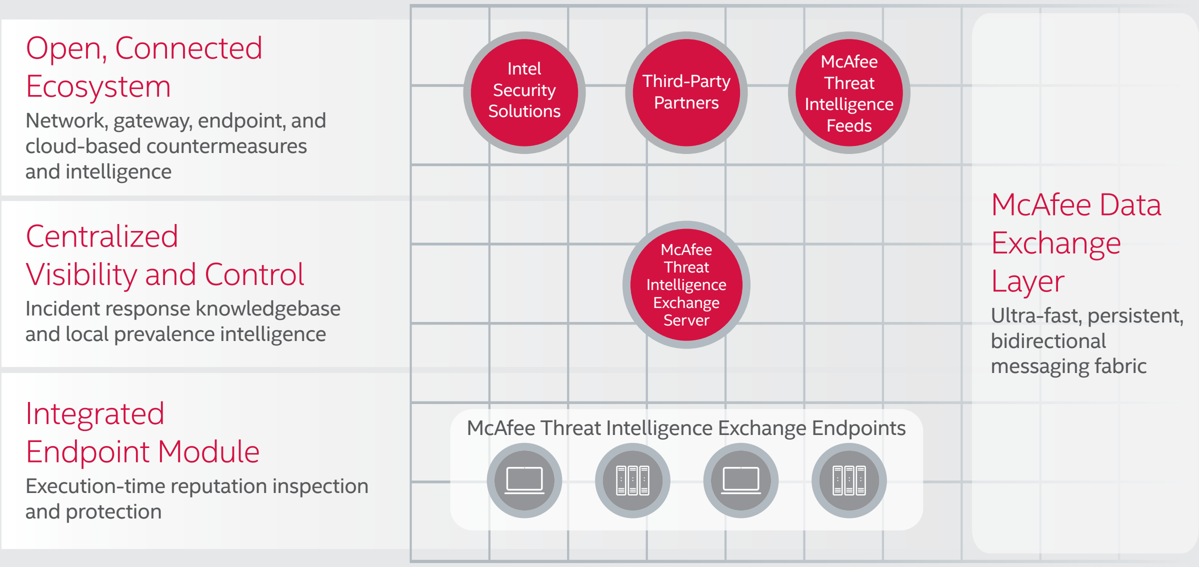
Manage events in context.

McAfee Enterprise Security Manager (SIEM) collects data from many sources and then uses correlation rules to help you prioritize events that need investigation. 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. With high performance and scale, analysts and administrators can access the data they need, when they need it, and then use automated workflows for prompt action. Using content awareness, McAfee Enterprise Security Manager 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.

Within McAfee Enterprise Security Manager, risk-based dashboards can alert you to relevant events. A risk score unifies vulnerability status, asset criticality, and any countermeasure protection available for the threat to gauge the severity and risk of a threat. This assessment will help security and IT operations teams prioritize threats and patching efforts according to the asset's risk value.

McAfee Threat Intelligence Exchange Solution Overview



Open, Connected Ecosystem

Network, gateway, endpoint, and cloud-based countermeasures and intelligence

Centralized Visibility and Control

Incident response knowledgebase and local prevalence intelligence

Integrated Endpoint Module

Execution-time reputation inspection and protection

Intel Security Solutions

Third-Party Partners

McAfee Threat Intelligence Feeds

McAfee Threat Intelligence Exchange Server

McAfee Threat Intelligence Exchange Endpoints

McAfee Data Exchange Layer

Ultra-fast, persistent, bidirectional messaging fabric

Figure 1. McAfee Threat Intelligence Exchange provides breakthrough endpoint protection by extending McAfee VirusScan® Enterprise to make local, contextual file execution decisions. It can also send files for analysis by the McAfee Advanced Threat Defense, feed SIEM watchlists, and notify gateways about changing risk reputations.

Connect everything.
McAfee® ePolicy Orchestrator® (McAfee ePO™) software works with McAfee Enterprise Security Manager to extend visibility and control across the entire security and compliance management environment, including Intel Security Innovation Alliance partner products. Integration with our 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. Integrations using the McAfee Data Exchange Layer are replacing point-to-point integrations for real-time data sharing and adaptive protection.

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.

Ease remote management.
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, reset passwords, and remediate problems, easing the burden for on-site technicians. McAfee ePO Deep Command works on Ethernet LAN and secured Wi-Fi and also has the ability to find the Intel vPro systems in your corporate network.

Continuously comply.
McAfee Foundstone consultants can also assess gaps in your organization's regulatory and compliance status and make recommendations for next steps.

More than 30 Million Compromised

The Washington Post reports that more than 30 million patients have had their PHI compromised in a breach.[3]

Take Charge.

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

- Secure sensitive data against loss and breaches with integrated controls that adapt to your systems.
- Employ security controls that work in and across healthcare network zones and covered entities and support mission-critical 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.

Intel Security can help you extract more value from security investments, while enabling data protection, a stronger risk posture, and cost-effective security—all of which are central to a successful, secure healthcare environment. Learn more at mcafee.com/securityconnected.

Learn More.
Networked medical devices have bridged the human-machine interface, delivering the most personal of benefits. They literally embed the Internet into people's lives, improving medical outcomes, offering better quality of life, and lowering healthcare costs. They also potentially introduce security flaws along with thosebenefits.[4] *The Healthcare Internet of Things—Rewards and Risks* Report.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com.**

[1] Healthcare-Friendly Security, http://www.mcafee.com/resources/white-papers/wp-healthcare-friendly-security.pdf
[2] http://www.nuemd.com/news/2014/10/08/report-healthcare-sector-accounts-more-43-percent-data-breaches
[3] http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/
[4] http://www.mcafee.com/us/resources/reports/rp-healthcare-iot-rewards-risks.pdf

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com