

Helping to secure critical healthcare infrastructure from internal and external IT threats, ensuring business continuity and supporting compliance requirements.



**Preemptive security solutions
for healthcare**



Preemptive security solutions for healthcare

Secure healthcare infrastructure cost-effectively

Properly securing information technology (IT) infrastructure has never been more critical for organizations in the healthcare industry. Healthcare institutions, plan providers and life sciences organizations alike need to safeguard confidential corporate and patient data from internal and external threats, not only as a best practice, but also to meet ever-evolving regulatory compliance requirements such as the Health Insurance and Portability and Accountability Act (HIPAA) and PCI Data Security Standard (DSS). A breach of protected health information (PHI) could result in enormous financial and legal ramifications, not to mention the potential negative impact on an organization's reputation.

At the same time, in order to provide prompt, personalized service and improve operational efficiencies, healthcare organizations must make critical business data easily accessible to employees, enable secure information sharing and allow remote network access. The transition from paper records to electronic files, combined with organizations conducting business around the globe and the introduction of new medical technologies and treatments, make it critical that healthcare

IT systems accelerate and support business processes, while addressing security in a holistic and cost-effective manner.

However, some healthcare organizations are hesitant to adopt preemptive security solutions due to concerns around cost, integration with legacy IT systems, hefty management requirements and limited visibility into existing security vulnerabilities. Not to mention the fact it can be difficult to instigate IT changes, even when such changes are made to improve and support business operations.

The reality is that healthcare organizations cannot afford take a reactive approach to IT security; there is simply too much at stake. Operating on the belief that conventional, password-protected security systems provide sufficient infrastructure protection or that today's Internet threats are simply unavoidable, can potentially result in corporate liabilities, network downtime and lost employee productivity. The most successful and protected organizations in the healthcare sector will focus on cost-effective, preemptive security solutions that help to ensure business continuity, protect the security and privacy of patient information and support compliance requirements.



Best practices to help meet healthcare security requirements

With a proven track record of serving healthcare institutions, plan providers and life sciences organizations, IBM recognizes the following best-practice IT security strategies and tactics as the building blocks needed to help protect valuable IT assets and data, and support compliance efforts in a cost-effective manner.

Assess the security and compliance posture

To transform existing IT security investments into an integrated, effective model that meets regulatory requirements and internal controls, organizations must first understand their current environment. Organizations in the healthcare industry are particularly vulnerable to security threats due to the increasingly large volumes of confidential patient data being stored electronically, combined with a historical lack of use of IT technology to protect corporate assets.

Establishing a baseline for security remains a critical first step in building a strong IT security foundation. To gain a better understanding of security and compliance postures, IBM recommends:

- *Performing vulnerability assessments and penetration testing, allowing organizations to review a detailed analysis of existing weaknesses and potential inlets for malicious activities.*
- *Leveraging security assessments of applications, IT controls and regulatory mandates, to better determine the level of protection against potential threats.*

Assessments are designed to make organizations aware of problems in advance and help establish a roadmap to address and prioritize discovered security vulnerabilities.

Improve and harden security across networks and applications

After a baseline for security has been established and any weaknesses have been identified for remediation, a logical next step is to improve and harden network and application design by:

- *Designing security-rich access zones.*
- *Applying “good guys in/bad guys out” security solutions and advanced techniques to help protect the network and information assets from theft and misuse.*
- *Using advanced security technologies, such as powerful intrusion prevention and behavioral anomaly detection, to help mitigate threats.*

Enhance identity and access management

With the need to protect increasing volumes of confidential corporate and customer data – and HIPAA, PCI and other compliance requirements a major concern – identity and access management form critical components of a holistic security strategy for organizations in the healthcare sector. The recommended approach involves:

- *Managing user rights and identities throughout their entire lifecycles.*
- *Using strong authentication to help ensure that only authorized individuals can access certain resources.*
- *Evaluating user activity to support optimal threat management and demonstrate due diligence with compliance standards.*

Properly securing information technology (IT) infrastructure has never been more critical for organizations in the healthcare industry

Preemptive security solutions for healthcare



Increasing data security helps healthcare organizations meet compliance requirements and ensure that confidential patient data is properly protected

By enhancing identity and access management, healthcare organizations can help reduce the risk of information theft while enabling connectivity for employees, patients, customers and trusted third parties. In addition, organizations can more proactively identify and address inappropriate network activity and document the effectiveness of security policies and identity-related controls.

Increase data security

Increasing data security helps healthcare organizations meet compliance requirements and ensure that confidential patient data is properly protected. To achieve a truly secure data environment, organizations must first establish a core data security architecture by:

- *Setting information asset profiles to determine where critical data resides, who can access it and how well it is protected.*
- *Applying and managing a comprehensive encryption strategy to help keep PHI confidential and meet compliance mandates.*

- *Implementing enterprise key management for encryption and data protection across the enterprise, from storage on local, removable devices through servers and hosts to long-term backup and storage on tape.*
- *Managing the disposal of data-bearing media – whether it is paper, magnetic media or optical media – to help protect the organization’s confidentiality, and that of their customers and patients, for the long term.*

Address physical security requirements

Physical security threats are a harsh reality. To help offset the risks, healthcare organizations can create an enterprise-wide, universal identification (ID) solution by:

- *Integrating identity management systems with physical security systems.*
- *Deploying a digital video surveillance strategy and architecture to help reduce physical threats and mitigate the inefficiencies of analog video technology.*
- *Engaging in contingency planning to help enhance the ability to deal with critical infrastructure threats.*

Monitor risk and compliance

Continuous monitoring of risk and compliance with regulations such as 21 CFR Part II, HIPPA, PCI DSS, and more is essential to driving effective IT security and brings health care institutions full circle to the first step of establishing a security baseline. Considering the dynamic nature of modern IT networks, continuous monitoring enables organizations to:

- *Work from a risk and privacy strategy to make improvements and then measure those improvements and report the results.*
- *Use automated tools to create reports that not only demonstrate effective threat mitigation but also help simplify various components of compliance testing and reporting.*

Innovative solutions to address security needs

Security solutions from IBM help healthcare organizations remain ahead of the onslaught of IT threats. IBM provides security solutions that help healthcare institutions, plan providers and life sciences organizations protect their valuable network and data assets and reduce overall threats while streamlining costs. Following a well-established framework for helping to secure healthcare networks, IBM works directly with clients to prioritize IT security projects and build an implementation roadmap.

IBM offers a comprehensive approach to creating a security-rich IT environment. Depending on each organization's unique needs, IBM's security solutions can help:

- *Assess security posture from a people, process, technology, risk and compliance perspective.*
- *Protect valuable network and information assets – preemptively.*
- *Defend the IT environment against threats.*
- *Monitor the IT landscape for security changes.*
- *Control risk within the organization as it relates to technology and overall compliance.*

Security solutions from IBM include hardware, software, consulting and managed services delivered through a comprehensive portfolio that covers the following areas.

Security governance solutions

Security governance solutions from IBM go beyond the technical perspective to evaluate existing security practices in light of current requirements and future objectives. This helps organizations address security in a holistic and cost-effective manner while potentially accelerating the return on investment.

The knowledge gained from security governance solutions can help organizations allocate funds and resources to manage information security threats more effectively. With IBM's regulatory and standards compliance services, organizations can assess and develop operational models

and processes that help them establish, manage, monitor and maintain effective IT security. These capabilities help organizations streamline compliance with regulations such as HIPAA and PCI DSS.

Security governance solutions from IBM encompass security risk management, program design and management, regulatory compliance services, privacy services and security education and training services designed to drive an effective, integrated security program that meets operational and IT needs.

Threat mitigation solutions

Threat mitigation solutions from IBM can help maximize existing security investments while reducing cost and complexity. Encompassing the IBM Internet Security Systems™ (ISS) suite of products and services, these threat mitigation solutions include network protection, endpoint protection and enhanced application integrity as well as security and vulnerability management.

Fueled by in-depth security intelligence gathered by the IBM Internet Security Systems X-Force® research and development team – a world authority on global Internet threats and vulnerabilities – IBM ISS solutions are designed to offer proven protection at a lower total cost of ownership.

Threat mitigation solutions help healthcare organizations to better understand current security posture and develop strategies that can enhance future security investments. Plus, threat mitigation solutions from IBM are designed to anticipate and guard against attacks on the network every hour of every day throughout the year – before they can adversely affect the IT environment. More important, advanced threat prevention technologies from IBM are designed to automatically protect the network from data loss and attack – for example, a hacker who is attempting to gain access to confidential patient records – without requiring significant management or expertise from internal IT staff.

Preemptive security solutions for healthcare

Identity and access management solutions

Identity and access management solutions from IBM help healthcare organizations quickly realize return on investment by bringing users, systems and applications online fast. In addition, these solutions can help organizations manage users, access rights and privacy preferences throughout the identity lifecycle in a more effective manner and in a security-rich environment. IBM can help healthcare organizations design, implement, deploy and maintain a seamless and integrated identity management system that is designed to reduce the costs of supporting multiple systems and identities. IBM's identity management solutions help protect valuable data and resources while enhancing the user experience through single sign-on and automated password reset capabilities. In addition, IBM solutions facilitate the sharing of identities between healthcare organizations, which can enhance growth initiatives. Services in this area leverage industry-leading IBM Tivoli® software to help organizations define and maintain access policies and user rights, and monitor and report actual user activity, in order to facilitate compliance initiatives.

Identity and access management solutions from IBM provide assessment, strategy, proofing, information lifecycle management (ILM) and authentication services to facilitate regulatory compliance while providing security-rich access to the people who need it.

Data security solutions

Whether data is in transit between endpoints or resting at an endpoint, data security solutions from IBM can enable widespread electronic collaboration while helping to protect sensitive data from existing and emerging threats. IBM's holistic approach establishes a core data security architecture that integrates with best-in-class components from IBM and other vendors to help protect key data assets and online transactions from external threats inbound from the Internet, as well from threats within the organization. Built on world-class research and development, IBM's data security solutions can enable organizations to take a proactive security posture, rather than reacting to security events as they happen.

Integrated data security solutions include high-performance, transparent encryption services to help protect data from unauthorized physical access and inadvertent data exposure when media is lost or stolen or when systems are decommissioned from service.

The following are also part of the data security solution portfolio provided by IBM:

- *Activity compliance monitoring and enforcement.*
- *Content protection.*
- *Enterprise management solutions for public key infrastructures.*
- *Mobile endpoint protection.*
- *Intrusion prevention capabilities.*

Physical security solutions

IBM integrates best-in-class digital video surveillance technology from marketplace leaders with advanced video analytics developed by IBM to create a powerful physical security solution. Older, analog surveillance solutions can be labor intensive, difficult to maintain and expand, and limited in their capability to provide alerts and post event analysis. With the digital video surveillance solution from IBM, healthcare organizations can gain a more cost-effective, scalable and integrated way to capture, store, retrieve and manage digital video content. Plus, organizations can take advantage of automated, intelligent analysis to help improve realtime or post-event decisions and actions.

Healthcare organizations can benefit from the ability to:

- *Respond more effectively to threats in the physical environment.*
- *Enhance the security of main and remote sites.*
- *Increase operational efficiency.*
- *Find new ways to extract useful information from video surveillance data.*



As an established technology adviser to the healthcare sector, IBM understands organizations' strategic and IT requirements.

IBM – the trusted security adviser to healthcare organizations

As an established technology adviser to the healthcare sector, IBM understands organizations' strategic and IT requirements. An industry-leading IT integrator and trusted resource to global organizations, IBM brings high-quality security tools to the healthcare industry using a defense-in-depth approach.

IBM takes threats seriously – and it has the research to prove it. The X-Force team, a world authority in threat and vulnerability discovery and analysis, regularly conducts primary security research. IBM monitors the Internet threat landscape and actively participates in setting the daily Internet threat level with the U.S. Department of Homeland Security. IBM security experts also conduct global threat monitoring every day, year-round, from five security operations centers (SOCs) located around the globe, and manage tens of thousands of security sensors for clients worldwide. With IBM solutions, organizations gain a comprehensive security knowledge base created and maintained by IT security experts.

When healthcare organizations are looking for a trusted technology adviser that can assume security management on an outsourced or out-tasked basis, IBM is well suited to help establish and maintain a security program, virtually regardless of the model deployed. IBM also provides direct access to expert security consultants who understand attack design, underlying vulnerabilities, security policies and compliance mandates. To help address an organization's needs from physical and data security to identity management and compliance audits, IBM provides skilled consultants to complement the efforts of internal staff or to provide comprehensive managed security services.

Security solutions from IBM are designed to enhance an organization's security posture at the level it requires. Rather than delivering only hardware or software, the IBM security portfolio spans people, process and technology – just as any effective IT initiative would. No matter where an organization falls along the security continuum, IBM solutions can help reduce risk and alleviate the pains associated with security.

For more information

To learn more about how security solutions from IBM can help protect organizations more effectively and efficiently – and to find the appropriate IBM security entry point – please contact an IBM representative or IBM Business Partner. You may also call 1 800 776-2362 or visit:

ibm.com/services/us/iss



© Copyright IBM Corporation 2007

IBM Global Services

Route 100

Somers, NY 10589

U.S.A.

Produced in the United States of America

1-08

All Rights Reserved

IBM, the IBM logo, Internet Security Systems, Tivoli and X-Force are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.