Enabling the Retail enterprise with innovative security solutions

Opening systems for business while protecting against system and data compromise
Protecting the storefront to the back room and demonstrating compliance

Retailers around the world are striving to improve the customer experience as a primary means of competitive differentiation. Reducing check-out times, introducing more self-service options and offering customer loyalty programs are common retail initiatives supported by information technology (IT).

The modern consumer demands product availability, shopping convenience, competitive prices and multiple order channels. With customer demands at an all-time high, retailers must maintain the availability of point-of-sale and back-end systems around the clock. To support dynamic growth, many retailers are migrating to open Linux or Windows environments for faster deployment times, reduced costs and flexibility. With all the improvements technology affords, some of these advancements also open retailers to additional security risks. The distributed nature of retail networks with multiple storefronts means there is more to protect from Internet threats and insider abuse.

Many consumers now view information security as a differentiator and will change shopping habits based on a “secure shopping environment.” The service-oriented architectures that support modern supply chain networks also require a defense-in-depth security strategy. While IT security can enhance revenue-generating operations such as point-of-sale systems and supply chain networks, it’s also needed to prevent losses caused by trusted insiders. Compliance with the Payment Card Industry Data Security Standard (PCI DSS) also weighs heavily on any retailers that process credit card data, increasing the need to centrally manage, monitor and report on the entire security operation.

Retail executives, chief information security officers and IT staff understand the high stakes of security, but often lack the real-time metrics and operational reporting to support security at the same level as other IT initiatives. Despite such challenges, successful and protected retailers will focus on secure IT efforts and security solutions that protect the network and customer data, help meet PCI compliance requirements, and support revenue generation.

Retailers around the world are striving to improve the customer experience as a primary means of competitive differentiation.
Using the right approach to IT security for retail

With a long history of serving retail companies, IBM recognizes the following best-practice IT security strategies and tactics as the building blocks needed to protect valuable IT assets and data, and support compliance efforts and business initiatives.

Assess your security and compliance posture
To transform existing IT security investments into an integrated, effective model that meets regulatory requirements and internal controls, you must first understand your current environment. Establishing a baseline for security remains a critical first step in building a strong IT security foundation. To gain a greater understanding of your security and compliance posture, IBM recommends:

• Performing vulnerability assessments and penetration testing, allowing you to review a detailed analysis of existing weaknesses and potential inlets for malicious individuals
• Leveraging security assessments of your applications, point-of-sale systems, governance and IT controls enables you to determine your level of protection against potential threats. Assessments make you aware of problems before auditors do, and help establish a roadmap to address any discovered security vulnerabilities.
**Improve and harden enterprise security across networks and applications**

Once you’ve established a baseline for security and identified weaknesses for remediation, a logical next step is to improve and harden your network and application design by:

- Designing security-rich access zones and applying whitelisting, blacklisting and other advanced techniques to protect your network and information assets from theft and misuse
- Using advanced security technologies such as intrusion prevention and anomaly detection to help mitigate threats.

**Enhance your identity and access management**

With insider threats on the rise and compliance requirements a major concern, identity and access management form critical components of a holistic security strategy. The recommended approach involves:

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

By enhancing your identity and access management, you can help reduce the risk of information theft, while enabling connectivity for customers, employees, supply chain partners and other trusted third parties. In addition, you can more proactively identify and address inappropriate behavior and document the effectiveness of security policies and identity-related controls.

**Increase data security**

In order to protect information assets and increase data security, you 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’s protected
- Applying and managing a comprehensive encryption strategy to help keep private information 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’s paper, magnetic media or optical media, to help protect your and your customers’ confidentiality for the long term.

**Address physical security requirements**

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

- Integrating identity management systems with physical security systems
- Deploying a digital video surveillance solution to help reduce physical threats and mitigate the inefficiencies of analog video technology
- Protecting critical digital video surveillance infrastructure and stored data
- Engaging in contingency planning to help enhance your ability to deal with critical infrastructure and homeland security crises.

**Monitor risk and compliance**

Continuous monitoring of your risk and compliance is essential to driving effective IT security and brings retailers full circle to the first step of establishing a security baseline. Continuous monitoring enables you 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.
Address your security needs – from the storefront to the back room – with innovative solutions from IBM

IBM’s security solutions help retailers remain ahead of the onslaught of IT threats. IBM provides security solutions that help retail companies protect their valuable network, data and point-of-sale assets, reduce overall threats, and enhance revenue opportunities. Following a well-established framework for securing retail and supply chain networks, IBM works directly with clients to prioritize IT security projects and build a roadmap for implementation.

IBM offers a comprehensive approach to securing the IT environment. Depending on your unique needs, our security solutions can help you:

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

Security solutions from IBM include hardware, software, consulting and managed services delivered through a full range of offerings that cover 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 business requirements and future objectives. This helps you address security in a holistic and cost-effective manner while potentially accelerating your return on investment. The knowledge gained from the IBM security governance solutions can help you allocate funds and resources to manage information security threats more effectively. With our PCI compliance services, you can assess and develop operational business models and processes that help you establish, manage, monitor and maintain effective enterprise IT security on an ongoing basis.

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 your business and IT needs.

Threat mitigation solutions
Threat mitigation solutions from IBM can help you maximize existing security investments while reducing cost and complexity. Encompassing the IBM Internet Security Systems™ (ISS) suite of products and services, these threat mitigation offerings include network protection, endpoint protection for point-of-sale systems, 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 offer proven protection for your valuable business data.

IBM’s threat mitigation solutions are packaged to suit retail network environments, with convenient multi-function appliances that include layered threat protection. 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 your business. More importantly, advanced threat prevention technologies from IBM are designed to automatically protect your network from data loss and attack without requiring significant management or expertise from your internal IT staff.
Identity and access management solutions
IBM identity management solutions help organizations quickly realize return on investment by bringing users, systems and applications online fast. In addition, you will be able to effectively and securely manage users, access rights and privacy preferences throughout the identity lifecycle. IBM can help you 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 across the enterprise and the supply chain. Our identity management solutions 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 partners, which can streamline security for the supply chain network. Offerings in this space leverage industry-leading IBM Tivoli® software to help you define and maintain access policies and user rights, and monitor and report actual user activity to facilitate PCI compliance.

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

Data security solutions
Whether data is in transit between stores or resting at within a central database, data security solutions from IBM can enable widespread electronic collaboration while helping to protect sensitive data from existing and emerging threats. Strong data security helps increase customer confidence. IBM’s holistic approach establishes a core data security architecture that integrates with best-of-breed components from IBM and other vendors to protect key data assets and business transactions. Built on world-leading research and development, our data security solutions can enable you to take a more a proactive security posture, rather than reacting to security events that can cause irreparable damage to your brand.

IBM’s integrated data security solutions include high-performance, transparent encryption offerings 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
- Enterprise content protection
- Enterprise key management solutions for public key infrastructures
- Mobile endpoint protection

Physical security solutions
IBM integrates the best-of-breed digital video surveillance technology from market 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, you can gain a more cost-effective, scalable and integrated way to capture, store, retrieve and manage digital video content. Plus, you can take advantage of automated, intelligent analysis to help improve real-time or post-event decisions and actions. IBM can also secure the infrastructure around a video surveillance deployment, improving uptime and reducing risk from insider and Internet-based threats. Your enterprise can benefit from the ability to:

- Respond more effectively to threats in the physical environment
- Enhance the security of headquarters and retail locations
- Increase operational efficiency
- Find new ways to extract useful business information from video surveillance data
- Boost customer satisfaction by alerting store management to long checkout lines
- Provide analyses of customer responses to marketing displays
- Identify employees or high-wealth customers using facial recognition technology.
IBM – your trusted security advisor

As an established technology adviser to retail companies, IBM understands your business and IT requirements. As an industry-leading IT integrator and partner to global organizations, IBM is able to bring superior security tools to retailers.

IBM is ideally suited to help you establish and maintain a security program, regardless of the model you choose to deploy. With a solutions focus, IBM does not merely offer one-off security products that contribute to management headaches. Instead, our security solutions work together to deliver comprehensive protection for retail and supply chain networks, point-of-sale systems, and back-end operations.

IBM also provides direct access to expert security consultants who understand attack design, underlying vulnerabilities, security policies and compliance mandates. Addressing your needs from physical and data security to identity management and PCI compliance audits, IBM provides skilled consultants to complement the efforts of your internal staff or to provide comprehensive managed security services. Many retailers outsource security management to IBM in order to streamline costs and conserve valuable IT resources.

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 United States Department of Homeland Security. Plus, IBM security experts 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.

IBM security offerings are designed to keep retail networks up and running at optimal performance levels. 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 your organization falls along the security continuum, IBM’s scalable and affordable solutions can help you reduce risk and alleviate the pains associated with security.

For more information
To learn more about how security solutions from IBM can help protect your organization more effectively and efficiently – and to find the IBM security entry point that is right for your organization – contact your IBM representative or IBM Business Partner, or visit:

ibm.com/security/index.shtml