Diverse_Security

IBM provides thousands of security experts and integrated portfolio of security solutions to help you detect and prevent advanced threats.

TOP SECURITY CONCERNS FOR MIDSIZE BUSINESSES The “security” umbrella covers a lot of territory. Threats come from malicious hackers and innocent employees— even hardware itself (for example, a crashed hard drive can destroy data every bit as much as a planned attack).

The list of threats includes:

1. Data loss or leakage: Damage can be caused by hackers who find increasingly creative ways to infiltrate systems to steal proprietary data or disrupt operations. But many (in fact, most) security breaches arise from sources that are closer to home. An employee loses a laptop computer. Discarded PCs are sent to a recycling firm without wiping the hard drive. A disgruntled employee siphons off data to offer to a competitor. Midsize businesses must protect their data from malicious outsiders as well as from well-meaning insiders.

2. Cyber-attacks: This broad category of malicious malware and data theft is large, dangerous, and eating into our economy. The latest IBM X-Force Trend and Risk Report notes that hacking has long since moved from the realm of bored teenagers to sophisticated criminal rings who are making lots of money. Most recently, concerns have centered on “Advanced Persistent Threats” perpetrated by well-organized, often states sponsored, groups that focus on industrial or national espionage. The new hackers are creative, sophisticated, and well-funded. Midsize businesses can be impacted by a broad based attack that may take the form of malicious code hidden in common file formats (e.g., PDF or JavaScript). They can also be affected when their partners—for example, their email providers—are attacked.

3. Unauthorized access to proprietary data – Nearly half of all data breaches are tied to misuse of access privileges, according to security experts; and the number is increasing by double-digits. The fault lies with a combination of lax security technology and poor policy implementation or enforcement. Too often companies rely on simple authentication schemes that are easy for unauthorized users to guess or find (for example, employees tape their passwords under their keyboards or choose passwords like “12345”). Or, a disconnect between HR and IT means that former employees, contractors, or partners retain access to company networks long after they have left the company, through IDs that aren’t invalidated. Midsize businesses must look for identity authentication solutions that are strong enough to prevent unauthorized access, but simple enough for employees to use without frustration.

4. Inaccessible or unusable data. Data protection isn’t just about thwarting crime. It’s also about making sure the data is available and usable as needed. Midsize businesses need to protect themselves from critical hardware or software failures by building a resilient infrastructure with appropriate backup processes. They also need to identify acceptable durations of downtime and develop appropriate recovery processes.

5. Compliance. Industry standards, such as those issued by the Payment Card Industry (PCI), and laws designed to protect consumers, corporations, and employees specify how certain data must be handled—both in active state and in stored or archived state. Regulations may be issued by any number of governing bodies (for example, federal, state, and even local governments), and they often change. For midsize businesses, the challenge is to continually keep up with regulations that may apply, as well as to prepare and file reports that certify compliance.

IBM Security Solutions for Midsize Businesses

IBM developed its “Security Roadmap for Midsize Businesses” to remove the complexity of security decisions for midsize businesses. As shown in Figure 1 below, the Security Roadmap identifies three categories where businesses need protection. IBM solutions in each category span security, compliance, and resiliency. These solutions are often available for on-site or cloud/hosted deployments.

IBM Security AppScan

IBM® Security AppScan® Standard helps organizations decrease the likelihood of web application attacks and costly data breaches by automating application security vulnerability testing. IBM Security AppScan Standard can be used to reduce risk by permitting you to test applications prior to deployment and for ongoing risk assessment in production environments.

IBM Security AppScan Standard supports:

- Broad coverage to scan and test for a wide range of application security vulnerabilities.
- Accurate scanning and advanced testing that delivers high levels of accuracy.
- Quick remediation with prioritized results and fix recommendations.
- Enhanced insight and compliance that helps manage compliance and provides awareness of key issues.

Why IBM?

▪ Expertise: Fueling IBM’s security expertise is a research team that rivals any in the world—the formidably named IBM X-Force. This team is devoted to compiling, analyzing, and mitigating the growing number of Internet threats, and has developed one of the world’s most comprehensive databases of threats. Staying one (or more) steps ahead of increasingly creative and well-funded hackers, the X-Force tracks software vulnerabilities (up 36 percent in the past year), identifies sources of threats, and builds countermeasures. While X-Force knowledge is used to develop the pre-emptive security capabilities in IBM products and technologies, the team’s work is considered too important to be kept in-house. Instead, part of the X-Force mission is to educate the market about the nature of threats. To that end, the X-Force publishes its Trend and Risk report twice yearly, and its Threat Insight Report quarterly.

▪ Expertise: Fueling IBM’s security expertise is a research team that rivals any in the world—the formidably named IBM X-Force. This team is devoted to compiling, analyzing, and mitigating the growing number of Internet threats, and has developed one of the world’s most comprehensive databases of threats. Staying one (or more) steps ahead of increasingly creative and well-funded hackers, the X-Force tracks software vulnerabilities (up 36 percent in the past year), identifies sources of threats, and builds countermeasures. While X-Force knowledge is used to develop the pre-emptive security capabilities in IBM products and technologies, the team’s work is considered too important to be kept in-house. Instead, part of the X-Force mission is to educate the market about the nature of threats. To that end, the X-Force publishes its Trend and Risk report twice yearly, and its Threat Insight Report quarterly.

- Scope: In a fragmented industry, IBM offers the scope and breadth to build a business-wide security plan for customers. The company’s comprehensive security portfolio— comprising services, software, and hardware—covers a range of security solutions addressing user identity authentication, data and applications, and infrastructure protection. The breadth of portfolio and expertise enables IBM to build integrated end-to-end security solutions for every size business, based on their needs.
- Service Level Agreements: IBM stands behind its claims with robust service level agreements—including the industry’s first results-based money-back assurances for many solutions.
- Partner Network: Most midsize businesses work with one or more local partners who act as an extension of their IT team. IBM’s extensive network of certified IBM Business Partners makes it easy to find a partner in your area to help you implement and maintain your solution.