



Contents

- 2 Integrating the Secure by Design components
 - 2 Understanding threats and vulnerabilities on an ongoing basis
 - 3 Ensuring the security of the infrastructure
 - 3 Extending the Secure by Design vision to the enterprise
-

Secure by Design: Ongoing validation

The goals and motivations that drive companies to proficiency in IT security are different than for other IT initiatives, and so are the costs. While building systems that are slower than competitive solutions might lose a few clients, failing to protect data and information will alienate many more.

Some companies add security on an ad-hoc basis. However, piecemeal security is costly, inefficient, and typically fosters a reactive rather than proactive security posture. By not incorporating security into the foundational controls of the business, companies are forced to constantly add security controls to try to keep up with organizational, technology, and Internet landscape changes. Constantly implementing entirely new controls to safeguard information and assets as new technologies and new compliance regulations emerge puts businesses at risk, from both security and financial perspectives. Organizations must start thinking differently about the relationship between security and the rest of the IT infrastructure.

Built on the philosophy of Secure by Design, IBM Security Solutions are focused on the following three primary components of creating and maintaining a secure infrastructure:

- Knowledge of threats and vulnerabilities
- Structural elements
- Ongoing validation



The third in a three-part series, this executive summary white paper will focus on the ongoing validation of the secure infrastructure.

Integrating the Secure by Design components

Ongoing validation of IT security—the third Secure by Design component—is a fundamental aspect of security best practices. The first two elements of Secure by Design focus on understanding the threats and vulnerabilities present in the world today and the structural elements that comprise a secure infrastructure. The concept of ongoing validation is effectively incorporating those elements into the security posture on an ongoing basis. Security needs to be approached as process, not as a collection of products.

To be really successful at building an infrastructure capable of responding to the evolving threat landscape requires a proactive approach to security. Companies not only need to design their infrastructure with security in mind, they also need to be constantly evaluating their overall security posture. To do otherwise is to embrace a flawed approach of purely reactionary security. For these reactive companies, attempting to provide ongoing validation is not unlike changing the tires on a car that is already moving. As such, in order to run smoothly, and maintain business continuity day after day, companies need to proactively secure their infrastructure.

Understanding threats and vulnerabilities on an ongoing basis

The threat landscape continually evolves and changes, and for companies to remain competitive, they must stay ahead of potential threats. The IBM X-Force® research and development team can provide the foundation for a preemptive

approach to Internet security. One of the best-known commercial security research groups in the world, the team helps educate and protect companies on an *ongoing basis* from today's malicious threats, so organizations can eliminate any potential vulnerabilities. The X-Force team:

- Researches and tracks the evolution of threats through the IBM Global Operations Center
- Advises customers and the general public on how to respond to emerging and critical threats
- Develops assessment and countermeasure technology for IBM products, providing customers with information about how IBM products and services can protect against the threat
- Delivers the latest information on Internet threats and vulnerabilities through notifications, such as Protection Advisories and Alerts
- Produces reports, such as the Trend and Risk Report and the Threat Insight Report, throughout the year
- Maintains the world's most comprehensive threats and vulnerabilities database, the IBM X-Force database—the result of thousands of hours of research by the team, with much of its data used to power the proactive protection delivered by IBM products

IBM doesn't just help increase awareness of the threats and vulnerabilities that exist today. IBM helps companies better understand the context of the threat, such as specifically how it might be affecting midsize retailers across Europe. In this way, companies can make decisions based on a deeper understanding of the challenges they face. IBM helps clients not only understand the world that exists outside their four walls, but also delivers meaningful intelligence about how their business fits into that outside world.

Ensuring the security of the infrastructure

To sustain a solid security posture, even companies that design the infrastructure with adequate security controls will need to continue to invest in information security. Companies can, however, take a smart, cost-effective approach to continually building a more secure infrastructure.

Various events and developments can spur the need for new security controls, such as new technologies, the changing threat landscape, new compliance regulations, and even a successful attack. Some companies implement new controls with each new development that can impact the security of the infrastructure. Yet companies are at a disadvantage when the terms of their security are always being dictated to them, promoting a reactive security posture.

Compliance is a good example of how companies often approach security after the fact. Many companies wait until new regulations emerge, and then focus resources on establishing a methodology and identifying the security tools that can bring the organization into compliance. However, compliance is a response to the threats of yesterday. Changing security controls with every new compliance regulation means that companies are looking backward rather than forward. This approach to compliance also requires that companies dedicate unnecessary costs to their security processes.

IBM is dedicated to helping organizations create a proactive security posture that better secures the enterprise and more effectively meets compliance demands. Secure by Design

practices and solutions empower companies to often be in compliance before new compliance regulations arise. By taking advantage of IBM's Secure by Design philosophy, a company's IT decisions and purchases are not dictated by external events, but rather by a drive to enhance business operations and profitability.

Extending the Secure by Design vision to the enterprise

With a broad and deep awareness of today's information security landscape and challenges, IBM equips companies with the security they need today, while providing the tools and methodologies to validate the security infrastructure on an ongoing basis. From the security intelligence provided day after day by the IBM X-Force team, to the comprehensive portfolio of IBM Security Solutions, the Secure by Design philosophy permeates everything that IBM delivers to its customers, providing customers ongoing security benefits. Forrester Research sums up best how the IBM Secure by Design vision is establishing IBM as leader in information security:

“Security organizations that require global reach, a broad suite of security services, and good threat intelligence from a single vendor should look to IBM to deliver these services.”¹

For more information

To learn more about Secure by Design: Ongoing validation, please contact your IBM marketing representative or IBM Business Partner, or visit the following website:

ibm.com/security

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: ibm.com/financing



© Copyright IBM Corporation 2011

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
January 2011
All Rights Reserved

IBM, the IBM logo, ibm.com and X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

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

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 customer may need 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.

¹ Source: *The Forrester Wave™: Managed Security Services*, by Khalid Kark, Security & Risk Professionals, August 4, 2010.



Please Recycle
