An integrated, intelligent approach to security

Security for today’s world: The IBM® Security immune system

Today’s cyber security challenges are complicated. And they rarely fit into the categories defined to run your business. Disconnected point products and services don’t provide the comprehensive solutions you need, when you need them. What’s more, those solutions tend to be expensive and hard to manage, leaving you with empty pockets and big headaches. That’s why, in a field flooded with 1,200+ point product vendors, IBM is helping clients develop an integrated and intelligent security immune system.

IBM’s expertise in integration enables full collaboration across third-party vendors, technology providers and IBM Business Partners to enhance security while lowering costs and complexity. Backed by analytics, real-time defenses and proven experts, the IBM Security immune system provides a fully integrated approach that allows solutions to grow, adapt and work together within your infrastructure to improve effectiveness. The result: intelligence, visibility and actionable insights across your entire environment.

A three-pronged approach to security

The IBM Security immune system delivers a full range of planning, response and readiness solutions to address your specific needs across three key areas:

- **Security Transformation Services** help transform your security program.
- **Security Operations and Response** helps you build a cognitive SOC.
- **Information Risk and Protection** helps you take control of digital risk.
Next-level security: Driving innovation with cognitive, cloud and collaboration

Today’s security systems need to go beyond blocking threats. That’s why the IBM Security immune system is built around a core of analytics. Using techniques that can recognize and understand threats, the immune system can help you outthink threats by incorporating the very latest in cognitive, cloud and collaboration technologies.

Cognitive

Cognitive systems like Watson™ for Cyber Security shine a light into data that’s been dark to organizational defenses until now. With the ability to interpret huge volumes of structured and unstructured data, they’re revealing brand new insights, patterns and security context. Using data mining, machine learning, natural language processing and human-computer interaction, cognitive systems provide evidence-based recommendations to help you act with confidence, at speed and scale.

Cloud

Cloud data security is a top priority, whether your cloud is on-premises, off-premises or a hybrid. The dynamic nature of cloud means you need a more automated, agile and elastic approach than traditional security measures. IBM Security can help you plan, deploy and manage security as you move workloads and data to the cloud, and as you consume security from the cloud. As a result, you can lower costs, increase flexibility and gain critical visibility.

Collaboration

IBM X-Force® Exchange lets you research global security threats, aggregate actionable intelligence and collaborate on solutions. With over 800 terabytes of threat intelligence data and 36,000 members, it’s a key resource for closing gaps in your organization’s security. And with IBM Security App Exchange, you can find, develop and share applications and best practices, while its collaborative platform helps facilitate faster, more effective incident response and resolution.

See the big picture

To learn more about the IBM Security immune system and its integrated approach to protecting your organization, download our interactive brochure at: ibm.biz/immunesystem

© Copyright IBM Corporation 2017

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
July 2017

IBM, the IBM logo, ibm.com, Watson and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

SSF03018-USEN-01