

Security for today's world: integrated and intelligent

Protecting your organization with a security immune system

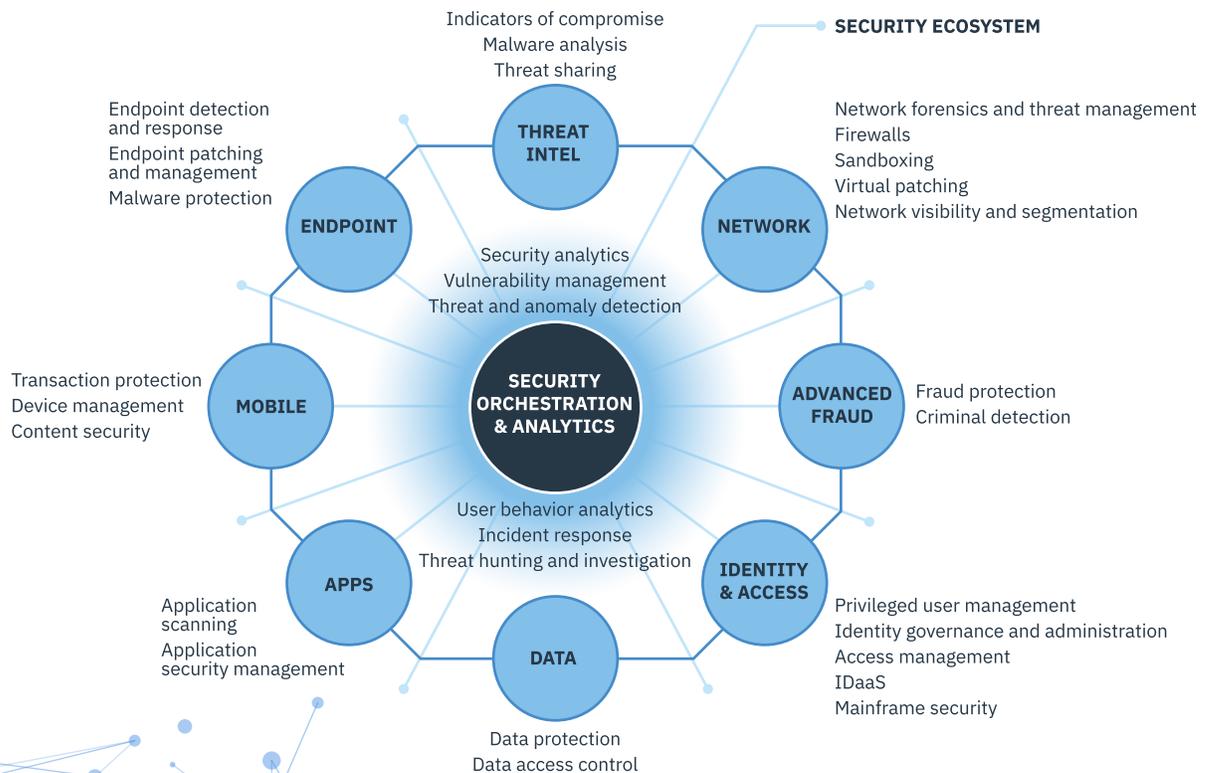
Today's cyber security challenges are complicated. And they rarely fit into the categories defined to run your business. Disconnected point products and services don't provide the comprehensive solutions you need, when you need them. What's more, those solutions tend to be expensive and hard to manage, potentially 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. This approach looks at a security portfolio in a more organized fashion—as an integrated framework of security capabilities that transmits and ingests vital security data to help you gain visibility, understand and prioritize

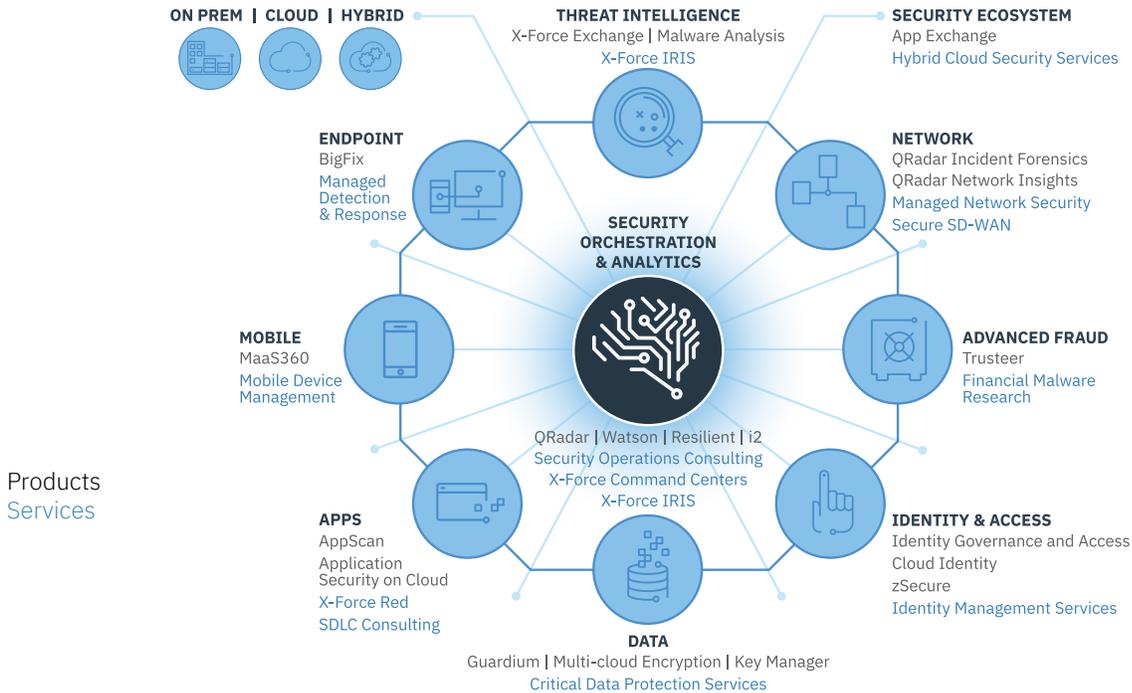
threats, and coordinate multiple layers of defense. As such, it functions much in the way that the human immune system does—assessing and identifying a virus, for example, and triggering an immune response.

The IBM® Security immune system is centered around a cognitive core of security orchestration and analytics which understands, reasons and learns the many risk variables across the entire ecosystem of connected capabilities. These capabilities also connect to an open partner security ecosystem of more than 200 “Ready for IBM Security Intelligence” partners; and IBM QRadar® includes over 500 out-of-the-box connectors to provide even more integration with other third-party tools.

An integrated and intelligent security immune system



IBM Security immune system



A three-pronged approach to security

The IBM Security immune system delivers a comprehensive range of planning, response and readiness solutions designed to help you address your organization's specific needs across three key areas.

Security Transformation

Services help you evolve your security strategy, creating a productive and mature security enterprise to help you:



- Build a solid security strategy that accelerates new IT trends, including BYOD, cloud, mobile, social and IoT
- Access the right skills — with experienced security advisors, responders, testers, analysts and engineers — available around the clock globally
- Gain visibility and defend against advanced threats with artificial intelligence that understands, reasons and learns to help analysts resolve incidents quickly
- Reduce complexity, increase productivity and consolidate fragmented solutions into an integrated solution utilizing analytics
- Address compliance with industry regulations, helping you set standards for your cybersecurity program based on risk assessments and controls

The Security Operations and Response

platform offers an integrated, end-to-end approach to building a cognitive security operations center (SOC) that can help enable you to:



- Prevent, detect and respond to threats in an intelligent, orchestrated and automated manner
- Continuously identify and remediate vulnerabilities
- Take advantage of IBM Watson® for Cyber Security to sense, discover and prioritize unknown threats
- Use deep threat intelligence provided by the IBM X-Force® Research team — and their massive threat databases — to hunt for indicators
- Orchestrate and automate incident response across people, processes and technology

Information Risk and Protection

solutions enable organizations take control of risk throughout their digital transformation journey by providing capabilities that can help:



- Streamline the process of moving to the cloud and support hybrid environments, with security-as-a-service solutions designed to identify users, secure access, and protect data
- Design applications from scratch with a “secure by design” best practice methodology
- Eliminate password and access hurdles and reduce fraud through simple sign-on and risk-based authentication for mobile and web experiences
- Enable secure collaboration for endpoint and mobile users across their applications, content, and data
- Protect data in motion and at rest and address compliance requirements such as GDPR, PCI, SOX, and more

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 approach is built around a core of analytics. Using techniques that can recognize and understand threats, IBM Security solutions can help you outthink threats by incorporating innovations in cognitive, cloud and collaboration technologies.

Cognitive

We believe that without cognitive security, organizations simply cannot keep up. There are just too many security events happening, too much information to digest and not enough people to do it all. The result? Security incidents can lose their urgency and the real threats can slip through.



IBM Watson for Cyber Security ingests enormous amounts of data—much of which is invisible to today's tools—making connections to pinpoint the greatest threats. You can change the game with these cognitive and machine learning-embedded solutions:

- **IBM QRadar Advisor with Watson** augments a security analyst's ability to identify and understand sophisticated threats. It combines the cognitive capabilities of Watson and the industry leading QRadar security analytics platform in a way that is designed to uncover hidden threats and automate insights.
- **IBM QRadar User Behavior Analytics** is designed to detect insider threats and identify the highest risk users. It uses machine learning to understand normal user behavior and quickly identify deviations from the norm that may indicate a threat.
- **IBM Security Guardium® Outlier Detection** applies machine learning towards protecting critical data and detecting threats and risks in data sources.

Cloud

Accelerate innovation and say "yes" confidently to digital transformation with the growing portfolio of IBM Security cloud-based solutions and services. Help protect your business with security solutions that act fast, scale up and down as necessary, and require minimal management.



We also offer managed cloud security services for organizations that want to take advantage of the flexibility and scalability of cloud but that do not have the skills in-house to manage cloud security.

IBM Security cloud-based solutions and services can help you:

- Manage identities and access with **IBM Cloud Identity Service** and **IBM Cloud Identity Connect**
- Protect data with **IBM Application Security on Cloud**, networks with **IBM Managed Cloud Network Security**, and endpoints with **IBM MaaS360®**
- Gain visibility with **IBM QRadar on Cloud** for network security intelligence and analytics
- Optimize security operations with **IBM Cloud Security Managed Services** and **IBM Security Intelligence and Operations Consulting Services**
- Fight digital identity fraud with **IBM Trusteer®**

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 over 40,000 members, it's a key resource for closing gaps in your organization's security. IBM X-Force Exchange helps analysts identify and streamline investigations about rapidly emerging attacks, enabling intelligence sharing that can help analysts contain and stop the spread of malicious and sophisticated campaigns.



With the **IBM Resilient® Incident Response Platform**, your organization can orchestrate your incident response (IR) function across people, process, and technology. The platform quickly and easily integrates with your existing security and IT tools, creating a central IR hub. This enables security teams to empower analysts with dynamic and automated workflows. As a result, organizations can drive down response times from hours or days to minutes.

With **IBM Security App Exchange**, you can find more than 120 apps that extend the capabilities of IBM Security solutions, helping you tailor your defenses to your requirements. What's more, this collaborative platform allows you—whether you are a customer, developer and business partner—to share applications, security app extensions and enhancements to IBM Security products to help fight the bad guys.

For more information

To learn more about the IBM Security solutions that make up the immune system and its integrated approach to helping you protect 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
December 2017

IBM, the IBM logo, ibm.com, Guardium, QRadar, MaaS360, Resilient, Trusteer, 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 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.

WGF12369-USEN-00