

# Visualize, uncover and stop advanced threats

Comprehensive approach

IBM Security solutions

Clearly visualize

Intelligently uncover

Seamlessly stop

More information

## HIGHLIGHTS

- **Clearly visualize** threats from one window in less time with more accuracy using integrated systems
- **Intelligently uncover** suspicious activity by transforming data into intelligence using artificial intelligence (AI), machine learning and advanced rules engines—so you can focus on the real threats to your business and stop chasing ghosts
- **Seamlessly stop** threats and reduce their impact with the orchestration of people, processes and technology automation

Cyber attacks continue to advance in scale and complexity. At the same time, IT budgets are thin, and security talent is simply outstripped by demand. The modern security operations center (SOC), whether on-site or virtual, needs to deploy a combination of technologies and people to close the gap between attacks and remediation.

When you partner with IBM Security, you can get clear visibility into enterprise-wide infrastructure activities, coupled with the ability to respond dynamically to help protect against advanced, persistent and opportunistic threats, whether they come from outside or inside the organization.



-01-

**Threats have advanced in volume and complexity. With IBM Security solutions, you can detect and respond quickly to reduce risk.**

Comprehensive approach

**IBM Security solutions**

Clearly visualize

Intelligently uncover

Seamlessly stop

More information




# Detecting and stopping threats with IBM Security

IBM Security is the only partner that can deliver clear visibility, thorough analysis and rapid response to advanced persistent threats, insider threats and more with integrated solutions.

Integrated IBM Security solutions enable advanced capabilities for automation, AI and machine learning, along with strong user and systems management capabilities, for end-to-end security. All of this is supplemented with specific security consulting and managed services.

The result? You can dramatically shorten your response time while reducing the risk of data loss due to threats stemming from unintentional user errors or malicious theft and sabotage.

## IBM Security solutions for detecting and stopping threats

 <b>CLEARLY VISUALIZE</b>	 <b>INTELLIGENTLY UNCOVER</b>	 <b>SEAMLESSLY STOP</b>
<b>IBM QRadar Security Intelligence Platform</b>	<b>IBM QRadar Advisor with Watson</b>	<b>IBM X-Force Incident Response Intelligence Service (X-Force IRIS)</b>
<b>IBM Security Intelligence Operations and Consulting Services</b>	<b>IBM QRadar User Behavior Analytics</b>	<b>IBM Security Access Manager</b>
<b>IBM Managed Security Information and Event Management (SIEM)</b>	<b>IBM Managed Detection and Response</b>	<b>IBM Security Identity Governance and Intelligence</b>

## CLEARLY VISUALIZE

# Gather more, then smartly filter, to see true threats in less time

Comprehensive approach

IBM Security solutions

**Clearly visualize**

Intelligently uncover

Seamlessly stop

More information

### IBM Security can help you see the danger in threats

Using security solutions from IBM, you can start seeing threats in faster cycles with integrated systems displayed from a single window. And you can cut through the noise created by false positives amid huge volumes of network activity. Using IBM Security solutions, you now can:

- Reduce time to detect potential incidents and suspicious behavior
- Receive precise analysis of threat data to reduce false positives
- See a comprehensive picture of risky activities to proactively address potential threats
- Employ automated rules and algorithms without lengthy and complex security information and event management (SIEM) setup

### IBM QRadar Security Intelligence Platform

[IBM® QRadar®](#) is a sophisticated security analytics platform for uncovering hard-to-find advanced threats, detecting anomalies and removing false positives. It consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout your network. Its advanced analytics engine reveals the event and the footprints left behind. With a full application marketplace, you can extend the QRadar field of vision and analytics to new threats in the wild to help protect your organization from future infiltration. The integration of QRadar with your incident response system helps stop threats—from detection to analysis to remediation.

### IBM Security Intelligence Operations and Consulting Services

[These services](#) include assessment of security intelligence and operations, consultation on building a security operations center, and capabilities for improving security intelligence, streamlining threat analysis and speeding adoption of new use cases and rules.

### IBM Managed Security Information and Event Management Services

Backed by IBM global security operations centers, [Managed SIEM Services](#) offer around-the-clock security monitoring and reporting using IBM X-Force® research capabilities along with data intelligence to improve identification of and response to threats.



## INTELLIGENTLY UNCOVER

# Use advanced technologies and services for full threat forensics

Comprehensive approach

IBM Security solutions

Clearly visualize

**Intelligently uncover**

Seamlessly stop

More information

### IBM Security can show you what risks and threats mean

With IBM Security, you can turn data and information into intelligence by detecting and analyzing advanced threats using AI and machine learning to:

- Radically increase the speed of analysis and insights
- Address resource shortfalls for analysis and investigations
- Power boost the capabilities of security analysts to easily fill skills gaps
- Broaden investigations into advanced threats by using unstructured data with data from analytics

### IBM QRadar Advisor with Watson

[IBM QRadar Advisor with Watson™](#) draws on structured and unstructured data to give security teams exponentially more actionable insights to uncover threats. Delivered through software-as-a-service, the solution gives you fast deployment with powerful capabilities that address the challenges of skills shortages, alert overloads, incident response delays and outdated security information.

### IBM QRadar User Behavior Analytics

[IBM QRadar User Behavior Analytics](#), a fully integrated component of QRadar Security Intelligence Platform, uses machine learning to understand normal user behavior, predict expected behavior and detect deviations that could indicate an insider threat. Security can easily see the user context of threats as well as identify the highest-risk users in the organization. When integrated with [IBM Security Identity Governance and Intelligence](#), QRadar automates layered step-up or multi-factor authentication policies or shuts down access.

### IBM Managed Detection and Response Services

Delivered from the global network of IBM X-Force Command Centers, [these services](#) provide continuous monitoring of enterprise laptops, desktops and mobile devices, supporting policy configuration and maintenance, and enabling comprehensive threat-hunting investigations.



## SEAMLESSLY STOP

# Take action quickly to halt threats and minimize damage

Comprehensive approach

IBM Security solutions

Clearly visualize

Intelligently uncover

Seamlessly stop

More information

### IBM Security can help you stop a threat in its tracks

IBM Security solutions help you block threats using dynamic systems orchestration and automation. At the same time, you can reduce false positives so that real users, true customers and valid partners can continue to access the resources they need. Using IBM Security solutions, you now can:

- Reduce the impact of threats on employee productivity, brand value and customer trust as you protect against interruptions and financial loss
- Shorten the amount of time cybercriminals spend on your systems
- Rapidly respond to security incidents
- Lessen the impact of advanced threats on critical data with a layered approach to security

### IBM X-Force Incident Response and Intelligence Services (X-Force IRIS)

Skilled IBM professionals provide a comprehensive [approach to security](#) that delivers critical insights into threats, assistance in preparing for and responding to threats and incidents, and help in developing processes that can be executed in the event of an incident.

### IBM Security Access Manager

[IBM Security Access Manager](#) is a modular, integrated access management solution for securing access points by defining and enforcing who and what can access what resources. When malicious user behavior is detected and flagged in your SIEM, the solution can automatically shut down access to specific systems to protect your data. Highly scalable and configurable, IBM Security Access Manager is offered both as a physical appliance and as a virtual appliance image.

### IBM Security Identity Governance and Intelligence

[IBM Security Identity Governance and Intelligence](#) delivers a business-centric approach designed to significantly simplify user access provisioning and the certifying and reviewing of policies. It also provides analytics and reporting to help you make more informed decisions on access, with capabilities covering enterprise user lifecycle management; access risk assessment; and mitigation, certification and password management. With this offering and its integration with your SIEM, an insider threat can be stopped with customizable identity and access policies from complete shutdown of malicious users' access to layered step-up or multi-factor authentication.



Watch how IBM behavioral analytics and identity access tools work together to [spot and react to malicious activity](#).

Comprehensive approach
IBM Security solutions
Clearly visualize
Intelligently uncover
Seamlessly stop
<b>More information</b>

# Why IBM Security?

IBM Security closes the gaps between capabilities for advanced threat detection, analyzing and distinguishing the true threats from the white noise, and stopping threats as much as 60 times faster than other solutions.<sup>1</sup>

Through integrations between the security analytics, threat intelligence, user-behavior analytics, and automated identity and access controls, as well as access to comprehensive security consulting and managed services, IBM Security solutions can help you shorten your response time to advanced threats while reducing the risk of data loss in an attack.

## For more information

To learn more about protecting your organization from insider threats, please contact your IBM representative or IBM Business Partner, or visit: [ibm.co/apt](http://ibm.co/apt)

## About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security software and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors more than one trillion security events per month in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: [ibm.com/financing](http://ibm.com/financing)

© Copyright IBM Corporation 2018

IBM Security  
New Orchard Road  
Armonk, NY 10504

Produced in the United States of America  
April 2018

IBM, the IBM logo, ibm.com, QRadar, X-Force, and Watson 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](http://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.

<sup>1</sup> Based on IBM customer experience.

