

Advanced threats 3 steps to safety

Visualize threats

Uncover patterns

Stop attacks

*Today's **advanced threats** can be hard to prevent. Automation and intelligence are your keys to closing the gap between threat detection and remediation.*

It's not IF you will be attacked, but WHEN.

Threats to your data can come from anywhere. From a cybercriminal on the other side of the globe. Or the employee down the hall. Either way, they're harder to prevent than ever before.



ADVANCED THREATS

250%

Increase in ransomware during 2017¹



INSIDER THREATS

4x

Increase in spam emails in 2016, expanding the chief cause of accidental data loss by insiders²

AS THREATS GROW IN NUMBER, THEY ALSO GROW UP

Securing data, applications and networks from today's onslaught of advanced threats means moving a step beyond looking for the usual malware and obvious points of entry. As threats evolve in scale and sophistication, you need to:

- **CLEARLY VISUALIZE** threats looming over the horizon, attacks at the gate and malicious behavior that already made it through your defenses
- **INTELLIGENTLY ANALYZE AND CORRELATE** events to focus your limited resources toward advanced threats that are real risks rather than wasting valuable time listening to white noise
- **SEAMLESSLY STOP** attacks with a tightly orchestrated flow of information and actions between tools

Attackers are holding data for ransom because they know you can't do business without it. They're establishing a beachhead on the Internet of Things (IoT) because it's everywhere. They're weaponizing artificial intelligence (AI) because they intend to outsmart defenses.

Today, in fact, even the most innocent-appearing action—like clicking on a web link or an email attachment—might open the door to a malicious actor. With malware and phishing schemes on a steeply rising, rocket-like trajectory, valid credentials are falling into the hands of cybercriminals in record numbers, paving an easy path to data beaches.

Why is it SO HARD to protect against advanced and insider threats?

*What's stopping you from keeping the **dyrewolves at bay**? What's missing in security strategies, leaving organizations to pick up the pieces over hijacked and lost data?*

ADVANCED THREATS

62%

Security experts who expect hackers will use AI within a year³

INSIDER THREATS

82%

Insider and privilege misuse breaches that took months, or even years, to be discovered⁴

FUZZY VISION

Most security information and event management (SIEM) solutions simply aren't seeing or presenting the full picture of your security posture.

Gone are the days of simply scouring security system log files and intrusion prevention systems.

As the enterprise has moved out in the world, your SIEM needs to follow suit. Also, your SIEM can no longer act alone. With more and more advanced persistent threats making it past the firewall, your SIEM needs to see more information inside the enterprise.

DISCONNECTED DOTS

Attackers no longer rely simply on the obvious frontal assault. They are smart, patient and sneaky. They infiltrate through the most seemingly benign places, then lie in wait for days or months before they strike.

You must be smarter to ferret them out. But you also need help in discerning between real threats and white noise. **Only Pac-Man earns points for chasing ghosts.**

You not only need to see what the threats are, you also need ways to discover who's attacking, what they're attacking, attack severity and what you can do to triage.

TOOLS TALK, BUT CAN'T ACT

Data—even when integrated across the environment, so you know who's doing what and where they're doing it—can't automatically stop attacks.

Your threat defense needs **SIEM to see what's happening, AI to help identify the connection points of suspicious activity, and automated systems to shut down the threat.**

You also need to align your people, processes and technology to properly orchestrate incident response. Of course, all this needs to start happening in a more rapid fashion. Months, weeks, even days are simply too long to be exposed to an advanced attack.

How SERIOUS are these attacks, really?

Many organizations find it difficult to **protect** themselves from attack, **preserve** their brand value, **avoid** erosion of customer trust and **prevent** financial loss.

WHERE ARE THE GREATEST RISKS?



58%

Financial services organizations suffer more cyberattacks than any other industry²



71%

Healthcare faces highest proportion of insider attacks²



90%

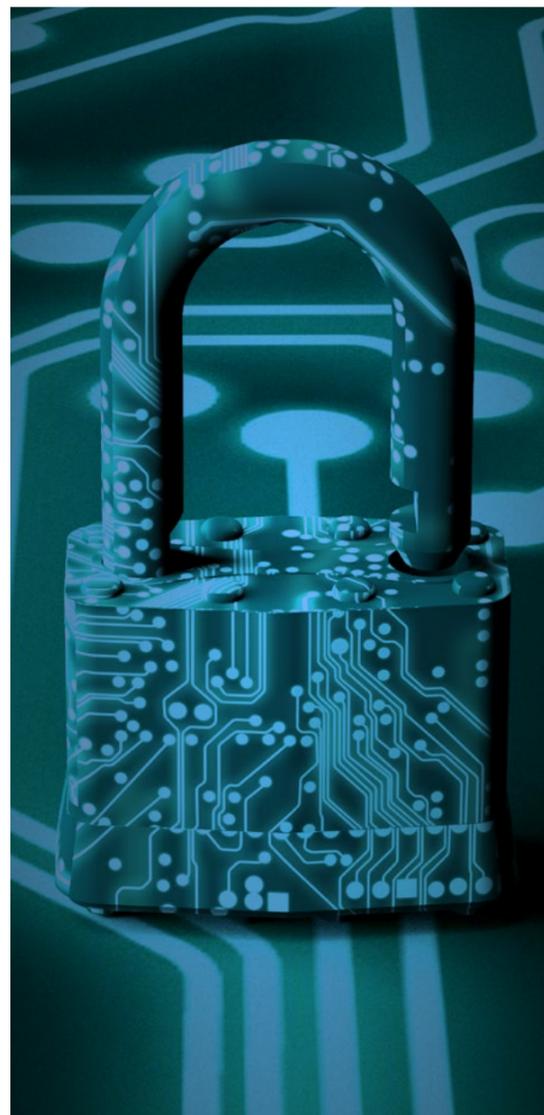
In communications, retail and manufacturing, most attacks come from the outside²

IN THE REAL WORLD

- The **WannaCry ransomware attack** used open ports to cripple 100,000 companies in 150 countries.⁵
- An average of **858 new malware signatures** were created each *hour* in 2017.⁶
- A single, successful phishing campaign kicked off an **organization-wide attack**.⁷
- A firm lost network connectivity when a **disgruntled employee** sabotaged passwords.⁸
- A terminated employee used another employee's credentials to **transmit codes and commands** that impair the availability of data, programs and systems.⁹
- Employees were paid by a cybercriminal to install malware on systems that allowed the **unlocking of codes to hundreds of thousands of mobile phones**.¹⁰

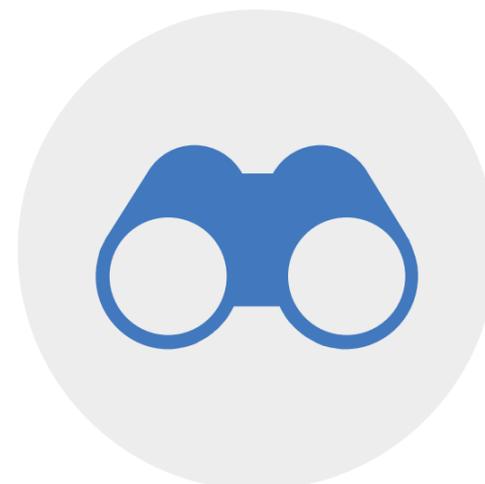
3 key security STEPS you need to take—and the benefits of each

*Ideally, the goal of security is to **quickly and accurately detect and stop threats**. But effective security isn't an instant, one-step process. It's a journey requiring the right tools and skills for the next destination in your business growth.*



CLEARLY VISUALIZE

- **Reduce** time to detect potential offenses and suspicious behavior
- **Receive** precise analysis of the threat landscape to reduce false positives
- **See** a comprehensive picture of risky activities to proactively address potential threats
- **Employ** automated rules and sophisticated algorithms without lengthy and complex SIEM setup



INTELLIGENTLY UNCOVER

- **Radically increase** the speed of analysis and insight generation
- **Address** any lack of resources for analysis and investigations
- **Add** to the capabilities of security analysts to address skills gaps
- **Ingest** internal and external data, structured or unstructured, with AI to rapidly reason through and identify likely threats



SEAMLESSLY STOP

- **Reduce the impact** on employee productivity, brand value and customer trust as you protect against interruptions and financial loss
- **Shorten the dwell time** of cybercriminals' activity on your systems
- **Truncate the time** it takes to respond to security incidents
- **Lessen the impact** of advanced threats with a layered security approach to critical data protection

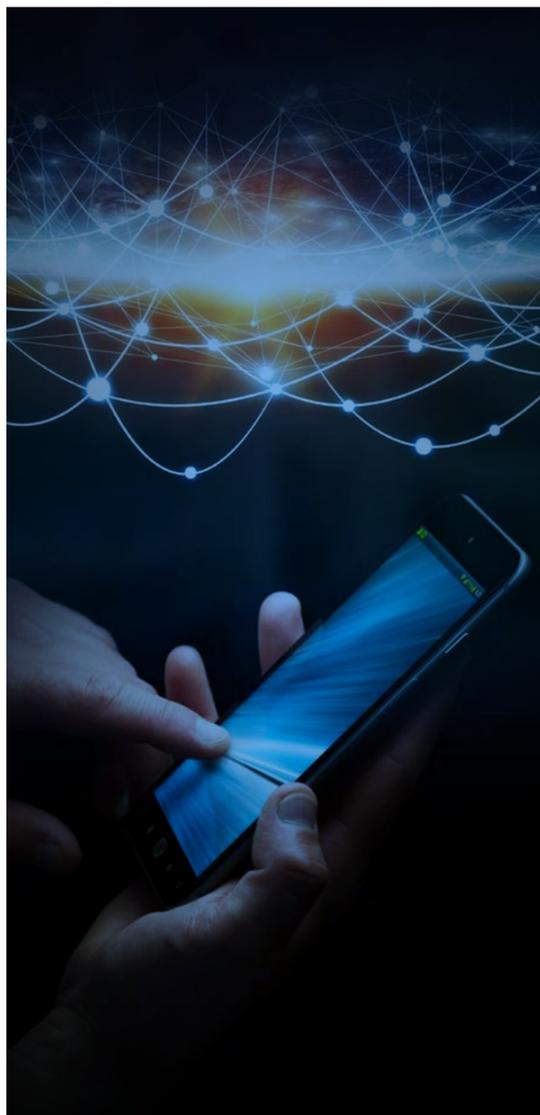


[Learn more](#) in this IBM solution brief about protecting your enterprise from advanced threats.

CLEARLY VISUALIZE

Gather and filter information so you can SEE what's really going on

Clearly visualize threats from **one window in less time with more accuracy using integrated systems.**



WHAT YOU WANT TO DO

- **Start seeing threats in faster cycles** with integrated systems displayed from a single window
- **Cut through the noise** created by false positives amid huge volumes of network activity

WHAT STANDS IN YOUR WAY

- **Lack of visibility** into the activities of rogue users or cybercriminals who have gained access to your environment
- **Inability to identify** the information, data and events that must be collected to detect threats
- **Disparate systems** that are unable to share security-related information or communicate with each other

WHAT YOU NEED TO GET THERE

- **Big-picture views** of your environment's overall health and risk posture, along with trends in users' activities and behavior patterns
- **Event chaining** that enables spotting threats quickly, with the ability to escalate automatically and triage based on criticality and risk
- **Data- and threat-agnostic solutions** that can connect with your existing systems
- **A single command console** that catalogs users by name, their anomalous activities, the severity of events and risk scores, along with other data and incident information that is contextually relevant
- The ability to **create a one-click watchlist** of the riskiest users and potential exploits, with drill-down views into underlying log and flow data, and the ability to create your own notes for follow up
- **Security expertise**, systems deployment and managed services designed to quickly increase your visibility into threats
- **Consulting services to modernize your security operations** across people, processes and technology



INTELLIGENTLY UNCOVER

Use advanced technologies to UNDERSTAND the threats you face

*Intelligently uncover suspicious activity by **transforming data into intelligence using AI, machine learning and advanced rules engines**—so you can focus on the real threats to your organization and stop chasing ghosts.*



WHAT YOU WANT TO DO

- **Turn data and information into intelligence**
- **Detect and analyze advanced threats** using artificial intelligence and machine learning

WHAT STANDS IN YOUR WAY

- **Inability to effectively process high volumes of data** to uncover threat-related activities
- **The need to minimize network noise** to avoid wasting time and security resources with chasing false positives
- **Lack of resources or skills** to quickly and effectively research and analyze threats

WHAT YOU NEED TO GET THERE

- **Incident investigation capabilities that use AI** for automated threat analysis and threat hunting to aid security analysts
- **Unstructured threat data analysis and correlation** based on local security incidents across security bulletins, blogs, research papers and more
- **Greater speed in analysts' investigations** (an increase of as much as 60 times is possible¹¹) using AI
- **Advanced analytics and machine-learning algorithms** to quickly identify high-risk activities, prioritize the riskiest users, uncover compromised credentials and deliver alerts about serious incidents
- **Alerts that let you know when users alter normal application practices**, deviate from the normal practices of their peers, perform invalid operational sequences or conduct data exfiltration
- **Abilities beyond traditional analyst capabilities** to pinpoint risky users and suspicious incidents in a vast volume of threat data
- **Services to help** with system deployment, integration and automation that deliver best-in-class attack detection, threat intelligence and analysis

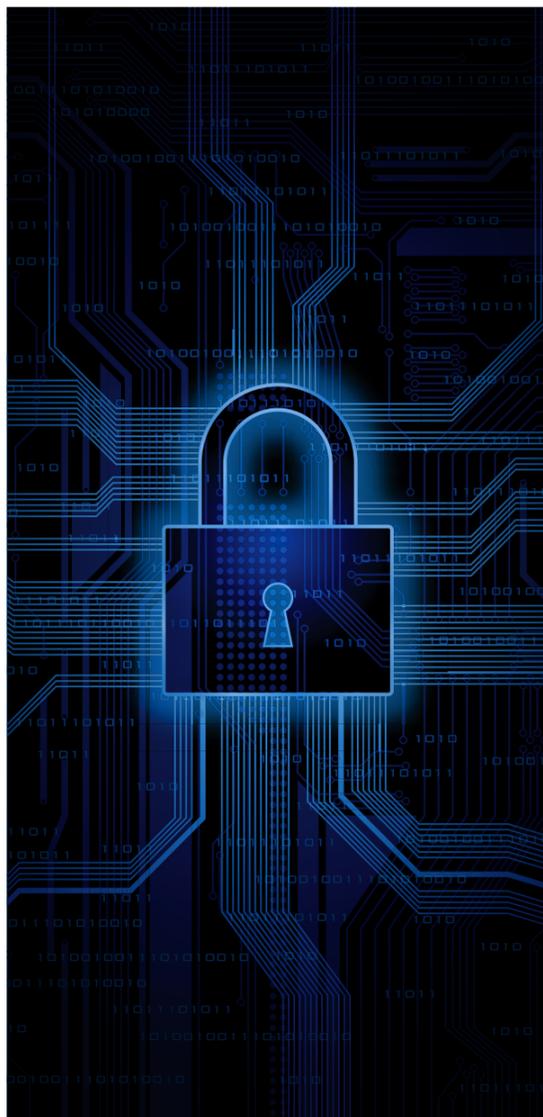


Watch to see how malicious activity can be [spotted and stopped](#) with a combination of user behavior analytics and strong access controls.

SEAMLESSLY STOP

Take action quickly to HALT threats and minimize damage

*Seamlessly stop threats and reduce their impact with the **orchestration of people, processes and systems automation.***



WHAT YOU WANT TO DO

- **Block threats** using dynamic systems orchestration and automation
- **Reduce false positives** so that real users, true customers and valid partners can continue to access the resources they need

WHAT STANDS IN YOUR WAY

- **Disparate systems** that don't work in concert to act on threats
- **Inability to reduce the dwell time** an attacker remains active on your systems and network
- **Can't respond quickly** to potential attacks without disrupting business

WHAT YOU NEED TO GET THERE

- **Proactively contain insider threats** by automatically suspending high-risk users' accounts
- **Customizable identity and access policies** ranging from complete shutdown of malicious users' access to layered step-up or multi-factor authentication
- **Dynamic policies** to change risky users' access across applications or databases
- **Integration with incident response solutions** to automatically initiate remediation processes
- **Threat blocking measures** for your endpoints, including mobile devices
- **Security expertise** as well as system deployment and managed services designed to respond quickly to threats
- **Consulting services** to determine and help establish your strategy for incident response across people, processes and technology



[Learn more](#) in this infographic about the risks of advanced threats and how to stop them.

COMBATING today's threats with IBM

Partner with IBM and you can get clear visibility coupled with the ability to respond dynamically to help **protect against both insider and advanced threats.**

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

Integrated IBM solutions deliver advanced capabilities for automation, AI and machine learning, along with strong user and systems management capabilities, for end-to-end security—all supplemented with a full range of security consulting and managed services.

Security solutions from IBM identify who is doing what—as well as when and where they're doing it—on your systems and networks. Additional integrations with IBM solutions for analytics, management, and monitoring for individuals, systems and data give you superior insight into and control over threats and security-related activities. **The result? You can shorten your response time and reduce the risk of data loss due to threats stemming from unintentional user errors or malicious theft and sabotage.**

[Learn](#) how IBM solutions can help meet the advanced threats your enterprise faces.

FOR MORE INFORMATION

To learn more about IBM Security, visit:

ibm.co/apt

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

© Copyright IBM Corporation 2018

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
April 2018

IBM, the IBM logo, ibm.com, QRadar, 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.

FOOTNOTES

- 1 Anthony Cuthbertson, "[Ransomware attacks rise 250 percent in 2017, hitting U.S. hardest](#)," *Newsweek*, May 23, 2017.
- 2 IBM Security, "[2017 IBM X-Force Threat Intelligence Index](#)," *IBM Corp.*, March 2017.
- 3 "[Black Hat Attendees See AI as Double-Edged Sword](#)," *Cylance*, August 1, 2017.
- 4 "[2017 Data Breach Investigations Report: 10th Edition](#)," *Verizon*, 2017.
- 5 "[Ransomware Attack Hits 200,000 In At Least 150 Countries: Europol](#)," *Newsweek*, May 14, 2017.
- 6 Ralf Benzmüller, "[Malware trends 2017](#)," *G DATA*, April 10, 2017.
- 7 Rachel Abrams, "[Target Puts Data Breach Costs at \\$148 Million, and Forecasts Profit Drop](#)," *The New York Times*, August 5, 2014.
- 8 Jaikumar Vijayan, "[Ex-IT Admin Found Guilty in San Francisco](#)," *PCWorld Magazine*, April 28, 2010.
- 9 "[Former Employee of Silicon Valley Company Pleads Guilty To Damaging Ex-Employer's Computers](#)," *United States Department of Justice Attorney's Office Press Release*, June 8, 2016.
- 10 Jon Brodtkin, "[AT&T sues former employees, alleging massive phone unlocking scheme](#)," *Ars Technica*, September 18, 2015.
- 11 "[Wimbledon 2017: Protecting the oldest brand in tennis with the latest in cognitive security](#)," *IBM*, 2017.