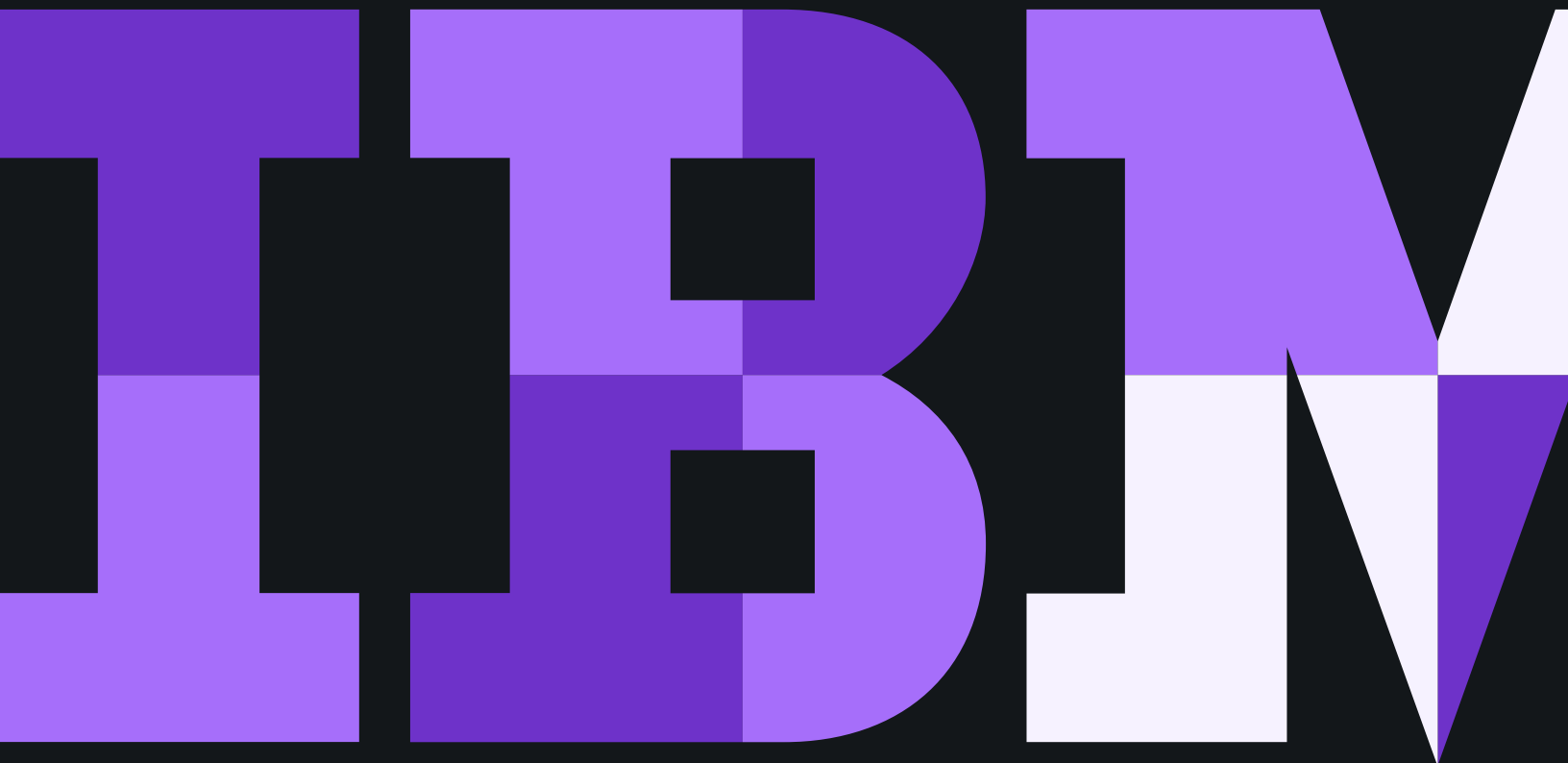


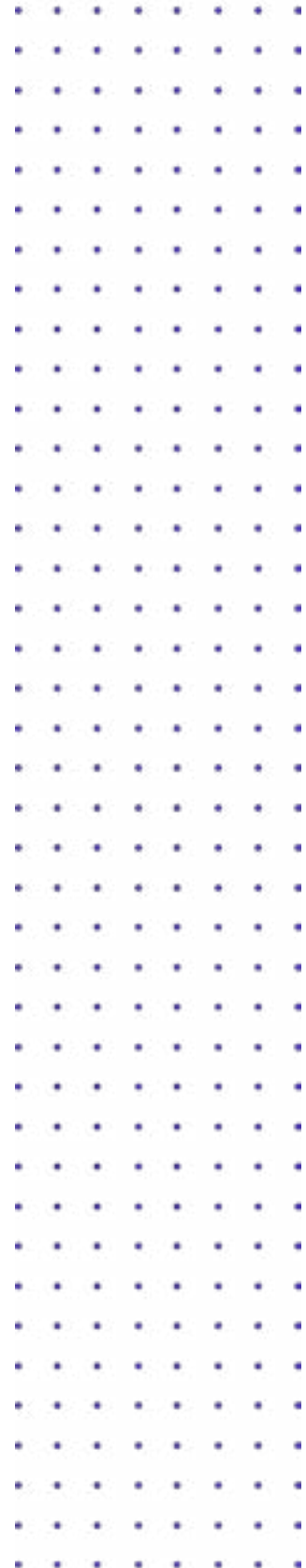
Drive to protection

Accelerating threat management performance



Contents

- 3 Is your security environment built to win?
- 3 Eliminate blind spots with a 360° view of security
- 4 Protect yourself with AAA: Automation, AI and Apps
- 4 Assemble the right team and empower them
- 5 Accelerate your threat responses
- 6 IBM Security Threat Management Solutions: Built to win



Is your security environment built to win?

In car racing, a lot of work goes into winning before the race even starts. Racing teams look for the best engine, the best tires, the best team and all the intelligence they can get to give them an advantage on the track. Security teams operate in much the same way. They bring together the best products, people and practices to ensure their handling performance is top-notch when the race to stop threats is on.

So, the question is, what's driving your security performance? Maybe you've built your own security engine from dozens of different parts, but are they tuned and integrated to perform at optimal capacity and efficiency? Can you view performance metrics and conditions from a single dashboard to troubleshoot problems effectively, isolate issues and respond in real-time to emergencies? Is your pit crew prepared for ransomware or the next big threat? If you're not on track to confidently handle threats at every turn, even your best security efforts could stall.



Today's complex SOC environments feature hundreds of different tools. What's driving your security success?



In 2019, it still takes 206 days for security teams to find their most advanced threats — and another 73 days to remove those threats from the network

Eliminate blind spots with a 360° view of security

Every car has a blind spot — an area where visibility is compromised. Security solutions have blind spots too. Maybe your blind spot prevents you from seeing hard-to-find threats or detecting compliance issues down the road. Wherever they exist, blind spots compromise your security team's ability to identify, protect against and respond to threats in a timely manner.

If you want 360-degree visibility around security, you need the right telemetry — that is, a single dashboard where security information is collected and reported.

Most security teams face information fragmentation. They may have one tool that reports on network attacks, another that scans for compliance and a third that detects access privilege escalations. And so, instead of a single, holistic view of security data, security teams spend too much time and effort trying to piece together the big picture from a mosaic of different monitors and moving parts.

IBM Security Threat Management gives security teams the visibility they need to succeed. By unifying security data, security teams can navigate with confidence — identifying not just data at risk, but vulnerabilities across networks, on thousands of endpoints and between clouds. IBM Security's unified approach helps security teams spot suspicious activities and anomalies that often get lost in the "noise" of day-to-day security operations. IBM Security also provides the threat intelligence security teams need to strengthen their security posture and avoid risks.

Protect yourself with AAA: Automation, AI and Apps

Threat management, like car racing, combines human intelligence with machinery. Security analysts and threat hunters are the drivers, racing against time and avoiding danger. **Artificial intelligence and machine learning accelerates their efforts by automating security tasks and responses.** With IBM Security Threat Management solutions, you benefit from experienced people who bring a wealth of expertise to the table, and advanced technology that automates the right tasks to speed your response to time-sensitive threats.

Most organizations are inundated with security data from different applications. They may have a security incident and event management (SIEM) tool from one vendor, a user behavior analytics (UBA) solution from another, malware detection from a third, and so on. All this security data, if left unfiltered, can make it harder to find real threats, from ransomware nested in your network to compromised credentials holding the keys to valuable data. IBM Security Threat Management can filter out this noise automatically, exposing the real threats in real time.

Assemble the right team and empower them

A security team is like a pit crew in the moment of crisis. You don't want to equip them with a complex system of security tools, screens, dashboards and databases — all of which can compromise their agility and insight. You want to empower them with the right tools and technology to quickly and deeply investigate Indicators of Compromise (IoCs), multichain attacks and other threat signals.

IBM Security Threat Management delivers the tools you need to investigate threats intelligently — from SOAR (security orchestration, automation and response) to SIEM, advanced analytics to artificial intelligence — and connects them with third-party security apps and IT operations under a single dashboard. The result is an integrated, orchestrated security environment that dramatically improves threat response times, detects hidden threats and turns security analysts into master hunters. On top of that, we support your team with our team — the world-class security experts of IBM X-Force — to provide timely threat intelligence and real-world training that gives you an inside advantage against cyber threats.



65%

of organizations say volume and severity of attacks is increasing



77%

of organizations have difficulty hiring and retaining IT security professionals


Accelerate your threat response

Security tools from multiple vendors aren't the only source of fragmentation. Many security teams are spread out across different geographies, making it difficult to respond to threats consistently and effectively. As threats move across your security landscape, do you present a united front, or is it every security analyst for himself? **If you don't have a strategic plan in place that includes automated incident response, a single view of security data and real-time communications during remediation, your biggest threat may be your own divided defenses.**

IBM Security Threat Management helps you respond to threats consistently and quickly across your entire organization. Using dynamic playbooks and automated security tools, IBM Security Threat Management delivers an orchestrated, real-time threat response that links people and processes together seamlessly for truly unified security. A holistic view of security data and threat management tasks ensures that your security analysts can coordinate their response like a single team, even if they're deployed in different parts of the field.

When threat management defenses unite, business moves faster

Unified threat management helps businesses navigate around security threats with speed and agility so they can keep moving forward.

[Watch video](#) 

Using dynamic playbooks and automated security tools, IBM Security Threat Management delivers an orchestrated, real-time threat response



IBM Security Threat Management Solutions: Built to win

You can build your own threat management solution, or you can choose a precision-engineered solution built by experts. At IBM Security, our track record speaks for itself, from industry recognition to customers that represent the world's leading companies. Our security threat management solutions feature advanced products and exceptional people that work together in perfect alignment, including:

IBM Security QRadar: An advanced, intelligent SIEM solution that helps security teams visualize, detect and automatically respond to threats — up to 50X faster than the competition.

IBM Security Resilient: An industry-leading SOAR solution that protects against threats and accelerates incident response across your organization through dynamic, automated playbooks.

IBM Security i2: A threat intelligence platform that helps threat hunters stay sharp and effective with expert-curated intelligence from the national security and defense field, law enforcement, industry fraud teams and more.

IBM Security X-Force Threat Management Services: Your personal pit crew for threat management, IBM X-Force provides security expertise when you need it most, from testing your security defenses to fighting in the front lines against cyberattacks.

IBM Security Intelligence & Operations Consulting Services: Security professionals who assess, design, build and optimize your security environment for superior performance.

IBM Security X-Force Incident Response and Intelligence Services (IRIS): An elite team of IBM X-Force experts who deliver deep security intelligence and tested incident response plans to help your security team bolster defenses, battle attackers and regain balance after an attack.





© Copyright IBM Corporation 2020

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2020
All Rights Reserved

IBM, the IBM logo and ibm.com 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 and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.



Please Recycle