Highlights

- Mitigate vulnerabilities with personalized threat protection
- Minimize false positives that waste time and resources
- Use natural language processing and business insight to eliminate language and cultural barriers
- Improve team collaboration, speed response coordination
- Employ assessments, reporting and benchmarking to better convey risk status to executives
- Get support powered by IBM® Watson® for Cyber Security

Personalized protection with IBM Managed Security Services

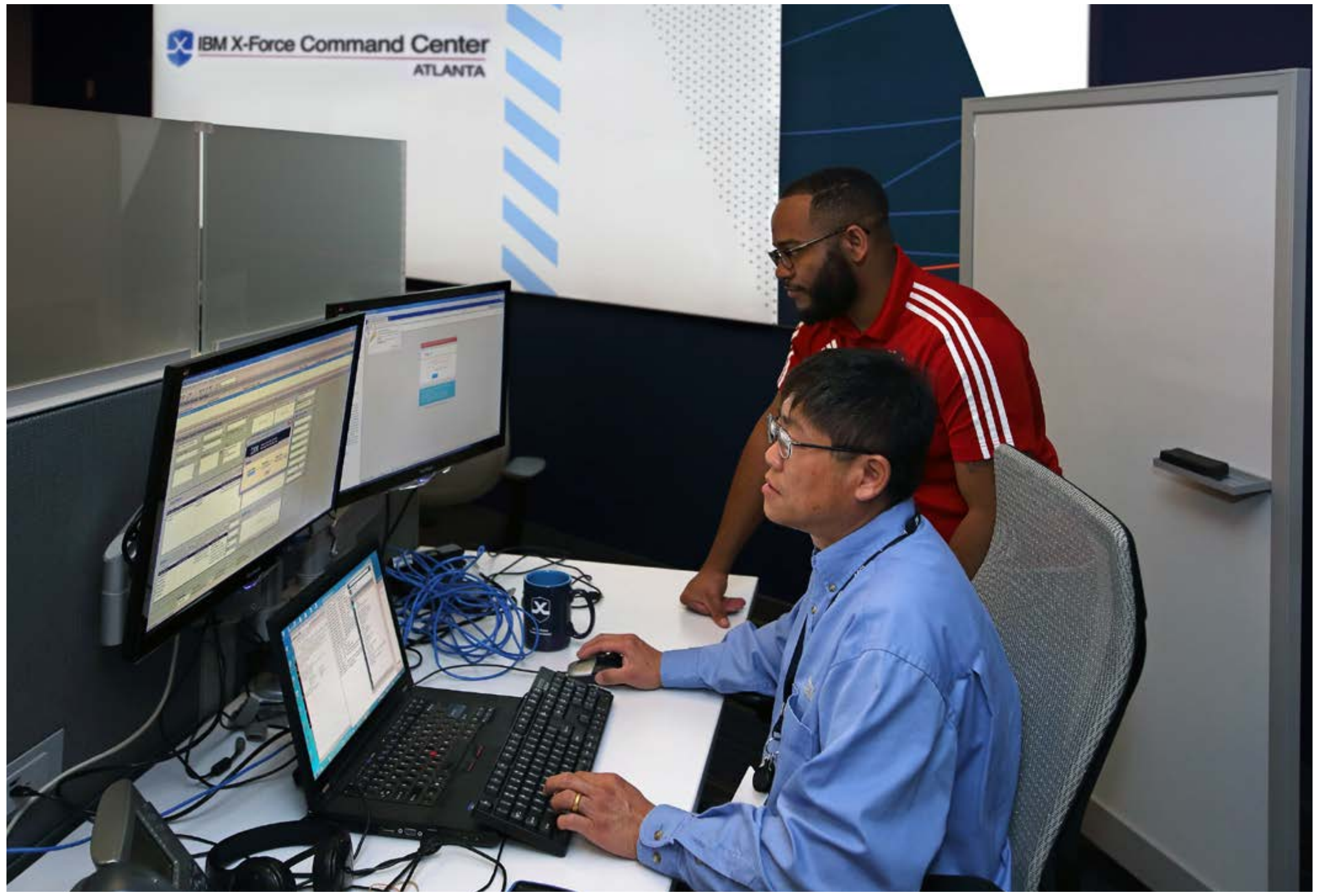
Now powered by IBM Watson for Cyber Security and delivered from IBM X-Force Command Centers

Today's organizations live under the unrelenting threat of a cyber attack, whether it comes in the form of a service interruption, the theft of business and customer data or some other costly or embarrassing security breach. To prevent the unthinkable on an ongoing basis, security teams need more power to protect company assets, more insights into their security posture and more expertise to stay on top of a constantly evolving security landscape.

Many IT organizations are turning to managed security services to provide these and other capabilities, helping to manage security risk while reducing security costs. But to be effective, today's enterprise security needs more than just an outsourced vendor who points out problems and then hurries on to the next customer. Effective security requires a partner who can leverage every available resource, including cognitive capabilities, while serving as a valuable and integral part of the security team.

A powerful partner trusted by thousands

IBM is a powerful cybersecurity partner who can provide a high level of personalized protection from attacks, including in the cloud. IBM has differentiated itself from other managed security services providers by making significant investments to provide clients with services built on industry-leading security intelligence, cutting-edge cognitive technology and proven security methods delivered by global security experts—and all delivered from the global array of IBM X-Force® Command Centers. With IBM Managed Security Services, IBM serves as a natural extension of your security team, providing the highest quality of service while addressing your unique security requirements.



We know more

Thanks to X-Force threat research and intelligence, as well as IBM Watson for Cyber Security, IBM has access to huge volumes and a wide range of threat intelligence and real-world insights that can be used to create personalized protection from security threats. IBM monitors and manages 270 million endpoints, and scans 100 million websites and images for security issues every day, resulting in the receipt and processing in the X-Force Command Centers of more than 35 billion security events per day. Among the capabilities for intelligence and insight IBM provides are:

- **Continuous learning and prediction:** Machine learning and data mining capabilities provided by IBM Watson for Cyber Security combine knowledge of current and past security events to enable highly accurate predictions.
- **Industry-leading threat hunting:** One of the most recognized security research teams in the world, the X-Force Threat Research team provides threat intelligence to help organizations reduce security risk.
- **Retrospective analysis:** IBM Managed Security Services can perform pattern and threat analysis on a massive trove of threat data, learning from past threats to help protect organizations from future ones.

We take action

Other managed security vendors simply monitor for problems, then throw those problems "over the wall" for the customer to handle. IBM leverages its massive security resources to not only sort through the threat data but also isolate what requires action. IBM then works hand-in-hand with your security team to identify or take the necessary action. IBM capabilities that make this action work for you include:

- **Real-time actionable insights:** IBM provides real-time actionable insights and recommended courses of action for both proactive defense against potential threats and active response against existing threats.
- **Reduced false positives:** False positives can be a huge waste of valuable time and security resources. Of the more than 35 billion security events IBM captures daily, only about 450 are legitimate threats. IBM has committed to minimizing false positives in order to keep the focus on actual events requiring a response.
- **Automated Tier 1 support:** Rather than waiting for a security analyst to look up information manually, organizations can take advantage of automated Tier 1 support—via phone or virtual chat—powered by IBM Watson for Cyber Security.

We understand how to work together

IBM provides the ability to communicate in a number of written languages via the IBM Managed Security Services portal, effectively translating both words and intent. These capabilities, along with the deployment of a number of new video communication technologies, enable stronger collaboration among teams and faster coordination of responses, no matter where the teams are located. IBM capabilities for improving collaboration and cooperative work include:

- **More effective teaming:** IBM is focused on serving as a security partner and extension of your security team, rather than simply as an outsourced vendor.
- **Customer knowledge:** IBM is able to leverage visibility into your organization as well as knowledge of the threat landscape in specific geographies and specific industries to provide insights that are uniquely relevant to you.

We tell you how you are doing

With visibility into thousands of security implementations, IBM can provide insights into a specific organization's security posture and requirements, delivering industry-specific risk assessments, security information on specific cloud vendors you may be considering and reporting that helps communicate your risk status to executive team members. These insights are made possible by capabilities that include:

- **Customized risk benchmarking:** IBM insights allow you to compare how you are performing on specific variables against peers in your industry and geographic region.
- **Industry-specific understanding of threat actors:** Cybercriminals pose different threats in different industries, but IBM can identify industry threats based on context and initiate proactive remediation.
- **Cloud platform security profiles:** By monitoring and managing thousands of cloud implementations, IBM can recommend specific cloud vendors based on your specific security requirements.

Why IBM?

IBM Managed Security Services include network security management services such as firewall management, vulnerability management, intrusion detection and prevention system management, unified threat management, secure gateway management, and email and web security management. IBM also provides managed security information event management (SIEM), security event and log management and secure software-defined wide area network (SD-WAN) services.

IBM Managed Security Services are delivered from global X-Force Command Centers, which combine best-in-class tools and highly experienced security experts supported by IBM cognitive technology to deliver state-of-the-art threat monitoring and intelligence. The 24x7 IBM watch floor provides around-the-clock coverage, with monitoring and assessment capabilities that enable organizations to quickly and efficiently mitigate vulnerabilities, helping you stay ahead of the most advanced threats.

Additionally, the IBM Security Right to Use program allows clients to bundle the expense of security hardware from a wide number of technology vendors into their IBM Managed Security Services solution. This allows hardware expenses to be included in the monthly operational expense bill, rather than listed as a capital expense.

For more information

To learn more about IBM Managed Security Services, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/services/managed-security-services/

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products 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 15 billion security events per day 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

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2017

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.