Buyer’s guide for Managed Security Services Providers

Grow your managed security operations center (SOC) business with IBM Security

IBM **Security**

Contents

01

Security monitoring, threat detection and response
Address your security needs and grow your business.

02

Partner with us to drive revenue
Meet your customers' needs effectively and profitably.

03

Taking threat detection and response to the next level
Leverage advanced analytics and threat intelligence to speed up investigation time.

04

Intelligent analytics for actionable insights into the most critical threats
Respond to cyberthreats with confidence and automate with intelligence.

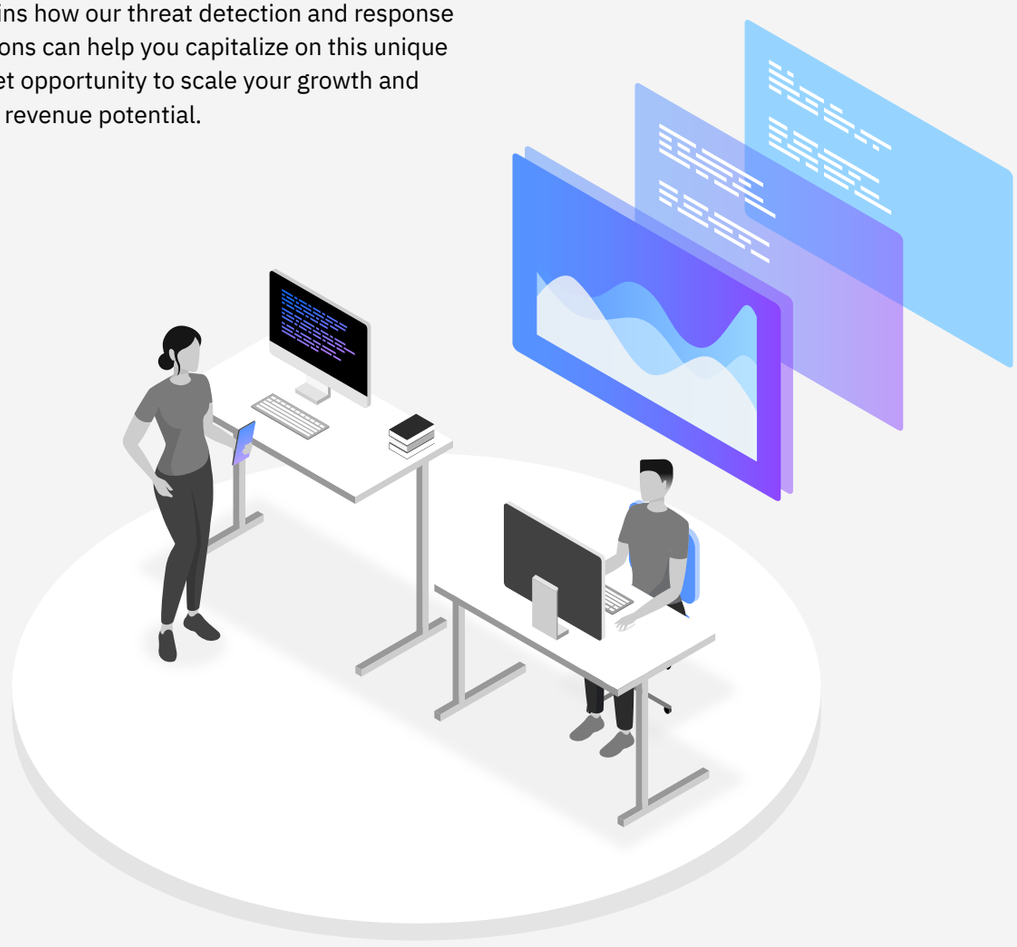
01
Security monitoring, threat detection and response

The shift towards digital transformation and the adoption of hybrid cloud infrastructure are changing the way industries do business. This change offers customers new digital experiences while enabling a global and disparate workforce. Recent events have only accelerated this digital transformation as organizations suddenly have thousands of individuals connecting from home computers outside an IT department's control. Users, data and resources are now spread widely across the globe, making it challenging to connect them quickly and securely. Without a traditional on-premises infrastructure for protection, employees' home environments are vulnerable to compromise, putting the entire business at risk. In turn, organizations are looking for a zero trust approach to address the security needs of this data-driven hybrid cloud environment.

However, a surge in data breaches, an ongoing cybersecurity skills gap, and an increase in global regulations mean many organizations simply can't continue on their journey alone.

As a Managed Security Service Provider (MSSP), you can capitalize on this opportunity. Though, like your customers, you can't do it alone. Zero trust requires a broad portfolio of security capabilities and expertise.

You need security partners that offer differentiated, best in class capabilities, and act as trusted advisors to help you effectively grow your business. This ebook outlines the MSSP Partner Program by IBM Security® and explains how our threat detection and response solutions can help you capitalize on this unique market opportunity to scale your growth and boost revenue potential.



02

Partner with us to drive revenue

As an MSSP, you will face an increase in market demand over the next few years, and you need to be prepared. To win and retain business, you'll need to demonstrate the ability to deliver security services more competently and less expensively than what clients can achieve on their own. You need an integrated platform that can deliver advanced security intelligence with rapid time to value, while providing the scalability and functionality needed to meet requirements quickly and easily from old and new customers alike.

By pairing the right vendor partner with the right partner program, you can stay ahead of the technology curve, provide differentiated value-added services, and boost revenue. When selecting a security vendor partner, you need someone who can help you:

- Collaborate on sales engagements through training and field support
- Expand your business by providing marketing collateral and support
- Deploy and implement effective security solutions easily
- Manage enterprise products across multiple customers
- Enable your internal security team on best practices
- Protect your customers' data and assets
- Achieve recurring services revenue

The MSSP partner program by IBM Security empowers partners by providing access to security technologies with flexible business models, enabling you to meet your customers' needs effectively and pro itably. To help you acquire and serve customers much better, we have enhanced this program with numerous investments including:

- Marketing growth funds to help drive your managed security business and win new clients
- Technical and transformational consulting options built for MSSPs
- Flexible licensing options (perpetual, term, monthly and SaaS)
- Opportunities to leverage our managed security offerings
- No-cost training options for technical and sales staff
- IBM Seller compensation

As a member of this program, you can take advantage of the entire IBM Security ecosystem and optionally leverage IBM Consulting or Product Professional Services team to build your suite of offerings.

Explore how →

“With other security intelligence systems, it can take months or require more money to realize benefits. With QRadar, we can deliver value to a new client within four weeks, which is quite unusual in our market. We are growing rapidly because we can provide value rapidly.”

Christophe Bianco
Managing Partner and Chief Technology Officer,
Excellium Services

ibm.com/case-studies/excellium-services

03
Taking threat detection and response to the next level

We understand that when it comes to your customers, one size does not fit all. While some organizations are just getting started with enterprise security monitoring, others are ready for a fully managed, 24x7 security operations center (SOC). IBM's threat detection and response solutions are fully integrated, and can offer detection and response services either as a stand-alone offering or as part of a comprehensive solution based on your customers' unique needs.

A modular and integrated suite of threat detection and response capabilities that runs on an open security platform

To guard against complex threats and enable your customers to navigate digital transformation, extended detection and response (XDR) capabilities are critical—such as deeper visibility, automation and contextual insights across endpoints—while working with your existing tools.

An evolution of the security intelligence portfolio, IBM QRadar® XDR is a suite of security software that spans the core foundational capabilities of threat detection, investigation and response.

Designed to be deployed by MSSPs, QRadar XDR is an open, connected approach to XDR and is:

- Built on our open, cloud-native security platform IBM Cloud Pak® for Security
- Committed to open security and the Open Cybersecurity Alliance (OCA)
- Allied and integrated with more than 200 cloud and security vendors

The QRadar XDR suite includes IBM native security technologies that customers can leverage for:

- Security Orchestration, Automation and Response (SOAR)
- Security Information and Event Management (SIEM)
- Network Detection and Response (NDR)
- QRadar XDR Connect

With the addition of ReaQta, the QRadar XDR suite will include an option for endpoint detection and response (EDR). This will allow IBM to provide native capabilities for all core XDR functions, while also providing the option to leverage existing investments and third-party tools across IBM's broad partner ecosystem.

Key benefits:

- Leverage automated, advanced analytics and threat intelligence to speed up investigation time
- Gain complete visibility into security data from a single pane
- Scale rapidly with out-of-the-box use cases and integrations
- Reduce events into a prioritized list of important alerts
- Drive compliance and manage regulatory risks

04

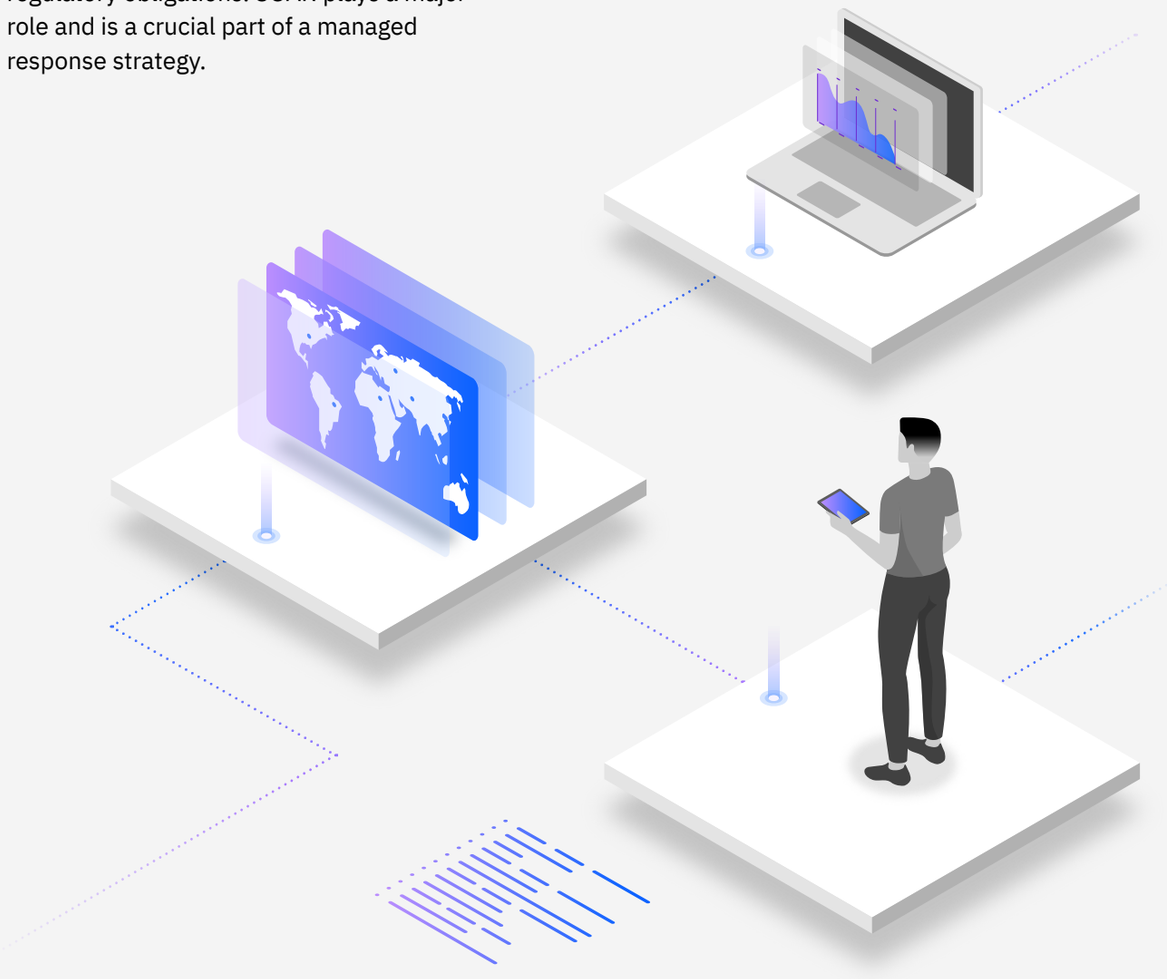
Intelligent analytics for actionable insights into the most critical threats

Whether you have a security team of 10 or 100, your goal is to ensure that your customers' business thrives. That means protecting your customers' systems and data to stop threats, stay ahead of cybercrime, and maintain compliance. However, the pressures facing the modern SOCs can make it difficult for you to achieve your goals. With the surge in unaddressed threats, insights overload, lack of cybersecurity skills and longer dwell times, the stakes are higher than ever before.

IBM QRadar SIEM helps security teams to detect, prioritize and respond to threats across an organization. It helps reduce dwell time in your customers' environments and boosts analysts' efficiency, thereby driving greater customer satisfaction, reduced overhead costs and increased margins for your business.

Orchestrate and automate incident response
In the current cyberthreat landscape, it's no longer a question of "if" an organization might get compromised, but rather "when".

When an incident does occur, it can take hours—if not days—to respond to complex, sophisticated cyberattacks and sort through the multitude of constantly shifting global regulatory obligations. SOAR plays a major role and is a crucial part of a managed response strategy.



04
Intelligent analytics for actionable insights into the most critical threats

By integrating IBM QRadar SOAR, you can accelerate your incident response processes while reducing operational overhead. It is specifically designed to help your team respond to cyberthreats with confidence, automate with intelligence, and collaborate with consistency. It guides your team in resolving incidents by codifying established incident response processes into dynamic playbooks. The open and agnostic platform helps accelerate and orchestrate responses by automating actions with intelligence and integrating with other security tools.

By deploying SOAR, MSSPs can ensure that analysts are focused on investigating and remediating the most critical security incidents that could impact their customers.

Empower your security team to:
- Automate compliance reporting tasks with prebuilt content for major compliance regulations (such as PCI, GDPR, HIPAA and more)
- Gain insights from information spanning across your customer footprint
- Streamline incident response and scale managed service operations
- Drive consistency in service delivery

Network visibility and advanced analytics
Networks—the foundation of today's connected world—are a prime target of attackers seeking to cause uncertainty and disruption, and cyberattacks across enterprises are becoming all too common. Detection of known indicators of compromise is no longer enough. Security teams require tools that detect abnormal behavior and send out alerts on advanced attacks before it's too late.

IBM QRadar NDR helps analyze network activity in real time. It combines depth and breadth of visibility with high-quality data and analytics to fuel actionable insights and response.
Enable and empower your security team to:
- Profile assets continuously based on attributes and behavior to uncover threats and compromised devices
- Gain visibility into unusual activity indicative of malicious lateral movement in real time
- Shift from reactive to proactive by querying historical network activity
- Reduce dwell time with quick detection

Connect your tools. Automate your SOC. Free up time for what matters most.
Different tools deliver a variety of insights which are critical to detecting advanced threats. However, having too many tools and too many alerts can cause visibility issues and alert fatigue. Open XDR can connect critical insights across siloed tools to deliver a single workflow—infused with automation—designed to accelerate detection, investigation and response, all while leaving your data where it is.

04

Intelligent analytics for actionable insights into the most critical threats

QRadar XDR Connect is a cloud-native open XDR solution that saves you time by connecting tools, workflows, insights and people. It brings together a set of capabilities to help enhance, automate and simplify extended detection and response. It enables SOC teams to:

Gain enhanced insights while improving threat detection.
QRadar XDR Connect helps teams cut through the noise of too many alerts from disparate tools. By connecting additional telemetry with your data using an open security platform, QRadar XDR Connect correlates and prioritizes related alerts so your team can detect without alert fatigue.

Act faster. Automate threat investigation. Accelerate threat hunting.
QRadar XDR Connect uses artificial intelligence (AI) to automate case investigation and correlate data, thereby enabling analyst efficiency and allowing more time for strategic analysis and threat hunting. A threat timeline, MITRE ATT&CK mapping and contextual threat intelligence can help improve prioritization, root-cause analysis and response.

Leverage your existing security tools.
There is absolutely no need to get rid of all your existing tools and replace it with new ones. Delivered on an open security platform, QRadar XDR Connect enables you to use the security tools of your choice. Let your security team leverage the existing solutions. Provide them with the opportunity and ability to connect a range of tools, data and intel feeds to modernize your SOC and address the specific needs of your team.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
April 2022

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.

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.

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.