

# Partner acceleration guide for IBM Security QRadar

April 2021

*Dear Business Partner,*

*Today's networks are more complex than ever before and protecting them from increasingly malicious and sophisticated attackers is a never-ending task. IBM QRadar Security can help organizations gain comprehensive insights to quickly detect, investigate and respond to potential threats.*

*To accelerate your sales and marketing efforts we have created the partner acceleration guide. This guide was expressly developed to help you to build a successful threat management business with QRadar.*

*This simple, easy-to-follow guide provides the full value proposition for our partners to add QRadar into their portfolio including market opportunity; solution description; client challenges and use cases; your investment required to build a practice; how to make money and key enablement resources.*

*Here's to great outcomes and explosive growth throughout the year! Please let us know if there is anything else, we can do to support your success.*

*We thank you for your partnership with IBM.*



**Mary O'Brien**  
*General Manager, IBM Security*



**David La Rose**  
*General Manager, IBM Partner Ecosystem*



# Table of contents

<a href="#"><u>Market landscape</u></a>	04
<a href="#"><u>Client challenges and solutions</u></a>	08
<a href="#"><u>What is IBM Security QRadar?</u></a>	11
<a href="#"><u>Differentiators</u></a>	13
<a href="#"><u>Free edition</u></a>	16
<a href="#"><u><b>Demand generation tactics</b></u></a>	<b>17</b>
<a href="#"><u>Your investment</u></a>	18
<a href="#"><u>ROI examples</u></a>	19
<a href="#"><u>Go-to-market resources</u></a>	21
<a href="#"><u>Demand generation tools</u></a>	22
<a href="#"><u>External client references</u></a>	23
<a href="#"><u>Contact us</u></a>	24

# Market landscape

## SIEM market is growing

USD 4.2B

2020

USD 5.5B

2025

Security Information and Event Management (SIEM) market size is expected to grow from USD 4.2 billion in 2020 to **USD 5.5 billion by 2025**, at a CAGR of 5.5% during the forecast period.<sup>1</sup>

<sup>1</sup> <https://www.marketsandmarkets.com/Market-Reports/security-information-event-management-market-183343191.html>

<sup>2</sup> <https://reprints2.forrester.com/#/assets/2/73/RES157496/report>



### Top industries

- Finance
- Healthcare
- Telecommunication
- Retail
- Manufacturing
- Utilities





### Key findings

- Compliance regulations remain a strong factor in use of SIEM technology<sup>1</sup>
- Offer SaaS and cloud-hosted models<sup>2</sup>
- Provide customizability for customers<sup>2</sup>
- Provide true analytics and operations<sup>2</sup>
- Map to the MITRE ATT&CK framework<sup>2</sup>
- Have a vision for extended detection and response (XDR)<sup>2</sup>

# Market landscape

## SIEM target audience

<b>Security Executive (CISO)</b> Securely enable the business, manage IT risk and compliance, report to the Board		Buyer
<b>Security Director</b> Oversees Security Operations, Incident Response and report on MTTD, MTTR		Buyer
<b>Tier 3 Analysts</b> Threat hunting; system tuning for better detection		Influencer
<b>Tier 2 Analysts</b> In-depth investigations; incident response		Influencer
<b>Tier 1 Analysts</b> First line triage – detect threats; gather info and escalate to Tier 2		Influencer

## Market landscape

Customers have  
enough data, but  
not enough insights

44%

of alerts are not investigated

54%

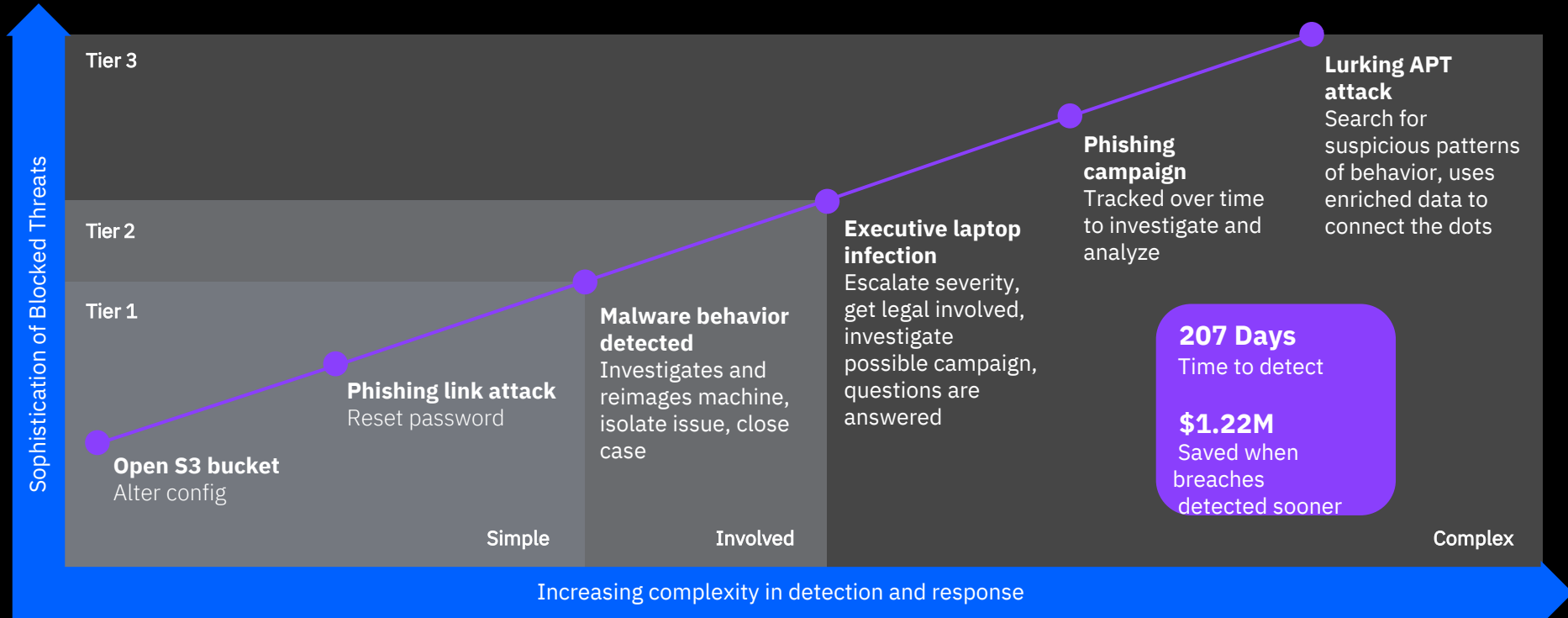
legitimate alerts are not remediated

36%

say “keeping up with alerts” is top concern

# Market landscape

The job keeps getting tougher for SOC teams – an opportunity for IBM Security Business Partners





# Client pain point #1

## Problem

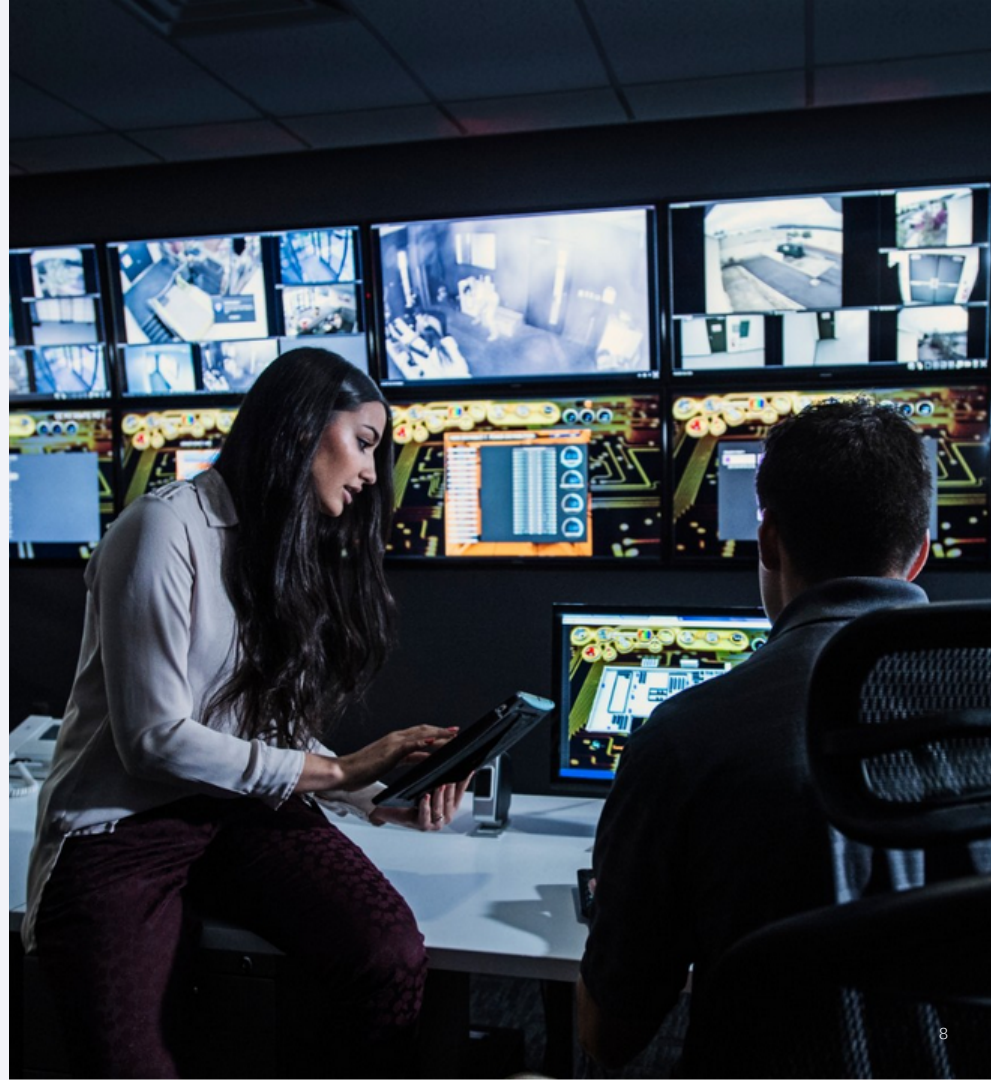
### Lack of visibility

Disparate security data across a growing number of tools both in the cloud and on-premise limits visibility while increasing vulnerability to attacks, complicating compliance reporting.

## Solution

### Complete visibility and real-time insights

- A single pane of glass to view data from endpoints, network devices, cloud environments, applications
- Real-time insights into user behavior
- Integration with 600+ tools and services
- Out-of-the-box content for GDPR, ISO 27001 and HIPAA





# Client pain point #2

## Problem

### Undetected threats

High volumes of alerts overburden security teams who need to quickly identify and prioritize the most critical threats in real-time and understand the full chain of threat activity.

## Solution

### Context to discern what requires action

- Threat intelligence feeds to reduce false positives
- Adherence with the MITRE ATT&CK framework
- Links seemingly unconnected events to identify threat activity
- Identifies and isolates known and unknown threats
- Visualized use case coverage and expert threat intelligence



# Client pain point #3

## Problem

### **Skill shortage**

Scarcity of skilled security staff requires a unified workflow and guided response in order to reduce churn and increase productivity of SOC analysts.

## Solution

### **Streamlined SOC operations**

- Alerts, automation, and AI-driven analysis that help security staff accurately triage incidents faster
- Dynamic, adaptive playbooks, guided response, and case management to resolve incidents with agility and confidence
- Automation and orchestration across security and IT operations



# What is IBM Security QRadar?

QRadar is a market-leading Security Information and Event Management (SIEM) solution that helps you defend against growing threats while modernizing and scaling security operations through integrated visibility, detection, investigation, and response.

## With QRadar, you can:

- Gain complete visibility into on-premise and hybrid, multi-cloud environments
- Detect threats in real time with advanced analytics and threat intelligence embedded with deep expertise
- Prioritize and automate alert triage by leveraging IBM Watson to speed up to 60x faster
- Respond to threats faster and more efficiently with orchestration and automation, case management and dynamic playbooks
- Scale rapidly with out of the box support for thousands of security use cases and integrations
- Accelerate compliance and manage regulatory risk with support for GDPR, ISO 27001, HIPAA and more



# What is IBM Security QRadar?

## QRadar capabilities

**SOLVE  
SECURITY  
CHALLENGES**

**DETECT  
ADVANCED  
THREATS**

**DETECT  
INSIDER  
THREATS**

**SECURE  
CLOUD  
RESOURCES**

**PROTECT  
CRITICAL  
DATA**

**EFFECTIVELY  
RESPOND TO  
INCIDENTS**

**PRIORITIZE  
AND MANAGE  
RISKS**

**PROVE  
COMPLIANCE**

RESPONSE

HUNT THREATS, RESPOND FASTER AND CONTINUOUSLY IMPROVE

**IBM Security  
App Exchange**

Seamless  
integration and  
content to  
augment  
platform.

DETECTION &  
INVESTIGATION

APPLY M/L, AI AND ADVANCED ANALYTICS TO DETECT, CONNECT, PRIORITIZE AND INVESTIGATE THREATS

VISIBILITY

COLLECT DATA ACROSS THE ENTIRE ENVIRONMENT

DEPLOYMENT  
MODELS

**ON PREM**  
HW, SW, VM

**AS A SERVICE**  
SaaS, Managed Service

**CLOUD**  
AWS, Azure, Google Cloud

**HYBRID**  
On-prem, SaaS, IaaS

# QRadar differentiators

## Complete visibility

Gain comprehensive visibility into enterprise-wide data across network, endpoint, cloud, user and applications.

## Automated investigations

Automated alert investigation driving faster more consistent and accurate responses using AI, supervised learning and federated search.

## Integrated response

Outsmart, outpace and outmaneuver threats by using dynamic playbooks, automation and orchestration. Also, satisfy privacy regulations using privacy breach reporting.

## Prioritized threat detection

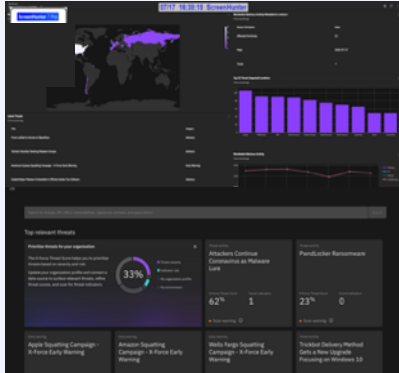
Track threats as they progress, prioritize critical events and investigate potential incidents using behavior chaining and global threat intelligence.





# Significantly improve your security operations with QRadar

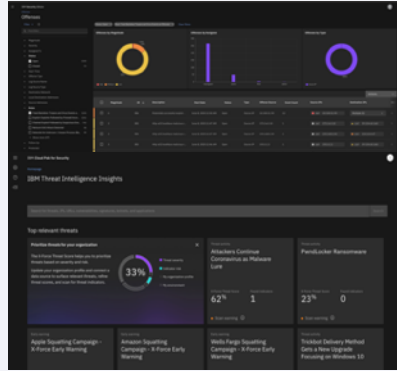
## Visibility



600+

validated integrations to reduce risk and MTTD

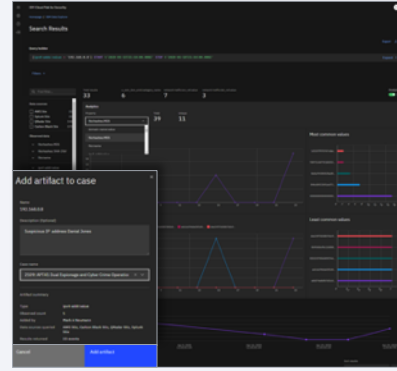
## Detection



51%

increase in ability to detect attacks

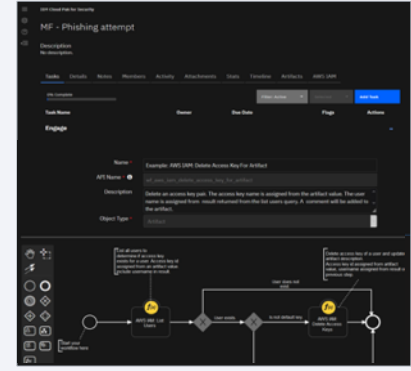
## Investigation



60x

faster investigation time using IBM Security QRadar Advisor with Watson

## Response



8x

increase in speed to respond to security incidents using IBM Security SOAR

# Deploy QRadar with IBM Cloud Pak for Security

The integration between QRadar and Cloud Pak for Security will allow security analysts to work the threat lifecycle from detection to response in a single, unified interface.



## On Premise

All In One (AIO)  
Hardware,  
VM Distributed,  
Hybrid



## On Cloud

SaaS, IaaS,  
CP4S, 3<sup>rd</sup> Party  
Marketplace



## As A Service

From IBM MSSP  
Partner

*“The future of IBM’s security analytics platform is based on its Cloud Pak For Security platform, built in on OpenShift cloud-native architecture and based on its RedHat acquisition, which seeks to deliver multiple security services in the IBM Cloud”*

— Forrester

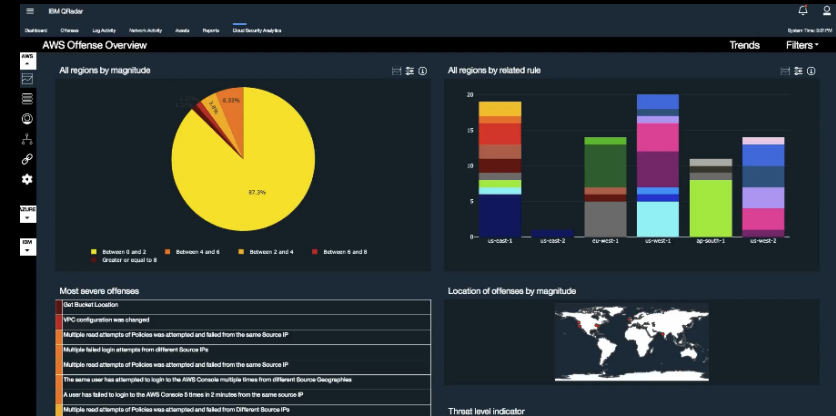
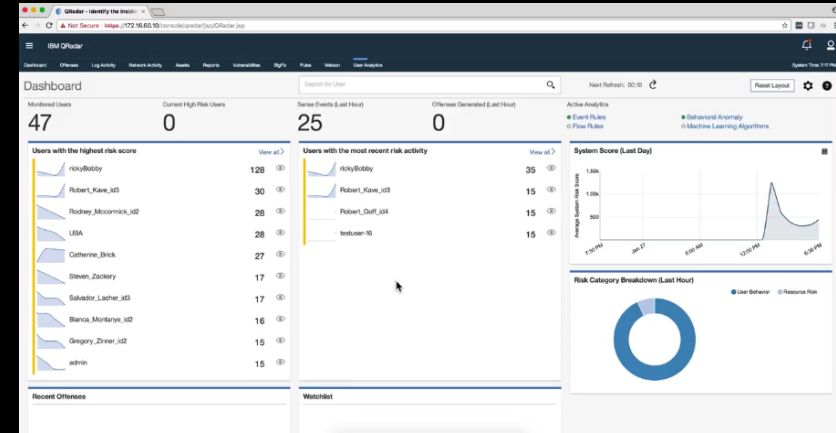


# Try free edition for yourself

Explore a trial of QRadar on Cloud:

- Delivers elastic scalability and rapid time to value
- Ingests vast amounts of data from on-premises and cloud
- Correlates related activities to prioritize incidents
- Enables real-time analytics to accurately identify threats
- Helps address audit and compliance requirements



Get started [here](#)



# Demand generation for QRadar

Paid social, paid search, competitive targeting, email nurture streams

Highest rated for current Security Analytics offering, subtext below:  
2020 Forrester Wave™



 QRadar

Find threats as your business grows

[Learn more](#)

Ad - <https://www.ibm.com/ibm/qradar>


**Automate Intelligence - Attack Threats Proactively**

Gain Intelligent Insights Into Your Most Critical Threats w/ **IBM QRadar Security Analytics**. Go Beyond Individual Alerts to Identify & Prioritize Potential Incidents. See How with **IBM**. Let's Talk. Schedule Time with Sales. Cross environment support. Chat, Call, or Email **IBM**.

Ad - <https://www.ibm.com/siem/gartner>

**IBM Security QRadar - SIEM Gartner Magic Quadrant**

Gartner Named **IBM Security a Magic Quadrant Leader**. Register for the Report to Learn Why. Gain Intelligent **Security Analytics** for Insight Into Your Most Critical Cyber Threats. Automate containment. Automate intelligence. Cross environment support. Let's Talk.

 QRadar

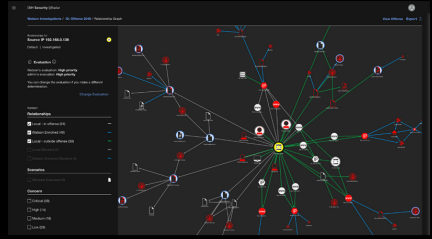
Real-time threat detection with IBM QRadar SIEM

[Learn more](#)

Manage security threats through modern, seamless workflows.

A seamlessly integrated threat management workflow is critical to detection, investigation and response. See how IBM Security QRadar's SIEM analytics and modern UI enable security teams to accelerate threat management workflows.

[Start the demo](#)



# Your investment

Get started quickly and grow as fast as your time investments allow

## Sign-up, start learning, start selling

- Register for IBM PartnerWorld
- Sign-up for Seismic
- Register for QRadar on Cloud Free Trial
- Review interactive demos and tutorials

## Build employee skills in as little as 3 weeks

- 2 technical credentials
- 1 sales credential
- Required to earn channel incentives
- Time Cost

## Increase your rewards

- Complete advanced technical certifications & badges
- Demonstrate sales success
- Achieve customer satisfaction targets
- Time Cost

Can be accomplished concurrently

# QRadar: new license example

Co-Led/BP-Led segment  
incentive rates

Partner incentive  
potential\*

*Average sale cycle:  
6 to 9 months*

*Timing for initial deployment:  
30 to 60 days*

Incentive type	Incentive rates	Comments
<b>Estimated average deal size for QRadar – \$100,000</b>		
Sales incentive	10%	Sales incentive rewards Business Partners for the opportunities they generate and the value they bring through the different stages in the sales cycle which result in the sale of IBM new license software to the end user.
Focus offering incentive	10%	Focus offerings incentive rewards Business Partners for selling eligible IBM product offerings which are core to IBM's strategy with value (applicable when transaction also received sales incentive or engagement incentive).
Growth client accelerator incentive (BP Led only)	15%	Growth Client Accelerator rewards Business Partner for selling in the BP-Led (Growth) customer segment with value (applicable when transaction also received Sales Incentive or Engagement Incentive).
Engagement incentive	10%	Engagement Incentive rewards Business Partners for their role and post-sales value-add activities they bring which result in the sale of IBM New License software to the End User and implementation and usage of the newly acquired IBM licenses.
Value-add distributor channel margin	Contact VAD	IBM Distributors have sole discretion to determine the amount (if any) of channel margin shared with the reseller. Resellers should discuss the channel margin with their distributors.
Additional BP-provided services revenue	1 x deal size	Potential additional BP services negotiated and provided by BP to clients.
Maximum potential margin	30% (Co-Led) 45% (BP-Led) +VAD margin	Earnings on your first deal may defray the cost of your time investment.

\*For planning purposes only, incentives for GOE clients and VAD margin paid at time of transaction; incentives for non-GOE clients are paid back-end. Incentives above are worldwide rates; some Geos or Markets may vary. Refer to <https://www.ibm.com/partnerworld/program/compliance/ibm-product-groups-exhibits> for parts eligibility and <https://www.ibm.com/partnerworld/incentives/ipe-software-new-license> for detailed incentive descriptions

# QRadar on Cloud: SaaS example

Co-Led/BP-Led segment incentive rates

Partner incentive potential\*

*Average sale cycle: 6 to 9 months*

*Timing for initial deployment: 30 to 60 days*

Incentive type	Initial subscription rates	Contract extension rates	Comments
<b>Estimated average deal size for QRoC – \$100,000</b>			
Land incentive	10%		Rewards Business Partner who acquires a new customer or move clients to IBM-hosted SaaS offerings.
Deal registration	5%	5%	Incentive protection when BP registers SaaS deals in MySA and becomes the IBM Business Partner of Record for SaaS.
Stay engaged		10%	Receive recognition for staying engaged and ensuring clients extend or renew eligible SaaS subscriptions.
Long term commitment	5%	5%	Rewards when Business Partner resells to extend IBM-hosted SaaS offerings for qualifying items for a coverage term of 24 months or longer.
Value-add distributor channel margin	Contact VAD	Contact VAD	IBM Distributors have sole discretion to determine the amount (if any) of channel margin shared with the reseller. Resellers should discuss the channel margin with their Distributors.
Maximum potential margin	20% +VAD margin	20% +VAD margin	Earnings on your first deal may defray the cost of your time investment.

\* For planning purposes only, all SaaS incentives and VAD margin are paid at time of transaction. Refer to <https://www.ibm.com/partnerworld/program/compliance/ibm-product-groups-exhibits> for parts eligibility and <https://www.ibm.com/partnerworld/incentives/ipe-software-saas> for incentive descriptions. Incentives above are worldwide rates; some Geos or Markets may vary.

# QRadar go-to-market resources

Develop your strategy for delivering QRadar to your clients and/or prospects

[Product overview](#)

Review the latest about the solution

[Product tour](#)

Explore the offering components with an Interactive tour

[Demo](#)

Experience a 1x1 demo and see how you can help clients detect and prioritize threats

[Free trial](#)

Adopt cloud SIEM and focus your resources on monitoring threats and insider attacks

[Enablement](#)

Build your sales and technical knowledge with a comprehensive roadmap

[Competencies](#)

Earn solution competencies to differentiate your skills in the marketplace

[Community](#)

Join our community to interact with IBM, clients and peers

[IBM Services](#)

Available option to offer to clients, if needed

# QRadar demand generation tools

Drive demand and engage with your clients and/or prospects about QRadar

## [Co-Marketing Funding](#)

Leverage IBM co-marketing funding to enhance your marketing plans

## [Digital Campaign](#)

Drive leads through customized content throughout all stages of the buyer journey

## [Client facing assets and messaging](#)

Leverage high performing content to build pipeline and progress deals

## [Use cases](#)

Understand client needs to streamline conversations



# Global QRadar customers



NRGi



The  
Weather  
Company  
An IBM Business



CargillsBank  
BANKING ON THE HUMAN SPIRIT



unibank



dairygold  
Golden Volleys, Growing Naturally



EXCELLIUM



ATEA



SOGETI



WaveStrong  
Information Security Professionals

# Contact us

## Worldwide

Scott Watson  
Business Partner Success  
IBM Security  
[sawatson@us.ibm.com](mailto:sawatson@us.ibm.com)

Dawn Farrell  
Business Partner Marketing  
IBM Business Partner Ecosystem  
[dfarrell@us.ibm.com](mailto:dfarrell@us.ibm.com)

Megan Grohman  
Ecosystem Offering Management  
IBM Security  
[mroseberry@us.ibm.com](mailto:mroseberry@us.ibm.com)

## Geo

### **North America**

Randy Long  
Business Partner Ecosystem Leader  
IBM Security  
[randy.long@us.ibm.com](mailto:randy.long@us.ibm.com)

### **EMEA**

Gonzalo de la Hoz  
Business Partner Ecosystem Leader  
IBM Security  
[gonzalo\\_delahoz@es.ibm.com](mailto:gonzalo_delahoz@es.ibm.com)

### **APAC**

Kittipong Asawapichayon  
Business Partner Ecosystem Leader  
IBM Security  
[kittipon@th.ibm.com](mailto:kittipon@th.ibm.com)

# Thank you!

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://@ibmsecurity)

[youtube.com/ibmsecurity](https://youtube.com/ibmsecurity)

© Copyright IBM Corporation 2021. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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 image features the IBM logo, which consists of the letters 'IBM' in a bold, sans-serif font. Each letter is formed by eight horizontal white stripes of equal thickness, set against a dark blue background that has a subtle gradient from top to bottom.