Security SaaS in the cloud

Identify, stop, and respond to today’s sophisticated security threats. Team with IBM for cognitive, cloud-based solutions.

IBM **Security**

Cybercrime will cost the world USD 6 trillion by 2021[1]

Technology is shifting toward the cloud, providing advantages and agility never before seen in IT security.

Software-as-a-service (SaaS), a natural extension of cloud-based solutions, helps accelerate responses and reduce the cost and complexity of security tools. Market trends indicate that SaaS is already in huge demand, and IDC found that in 2018, 62 percent of companies spent their IT budgets on subscription-based services and predicts that spend will grow to above 80 percent in the coming two years.[2] This continuing trend creates strong new business opportunities for service providers.

The average cost of a data breach is now estimated to be $3.86 million.[3] With the deployment of cloud computing technologies, you can help your clients combat these expensive, malicious attacks and software vulnerabilities with remarkable speed, ease, and reliable uptime. Cloud-based computing can be incredibly beneficial for clients whose IT staff is limited in size and skill.

Now, more than ever, organizations are seeking security experts and world-leading SaaS solutions to protect their businesses against threats. You can capitalize on this demand by helping your clients identify, prevent, and respond to security threats—quickly and affordably with IBM Security SaaS.

IBM Security provides a diverse and extensive SaaS portfolio of cognitive cloud-based solutions along with attractive IBM Business Partner programs. This powerful combination helps you win new markets, develop new skills, and build a profitable SaaS offering.

IBM Security SaaS for service providers

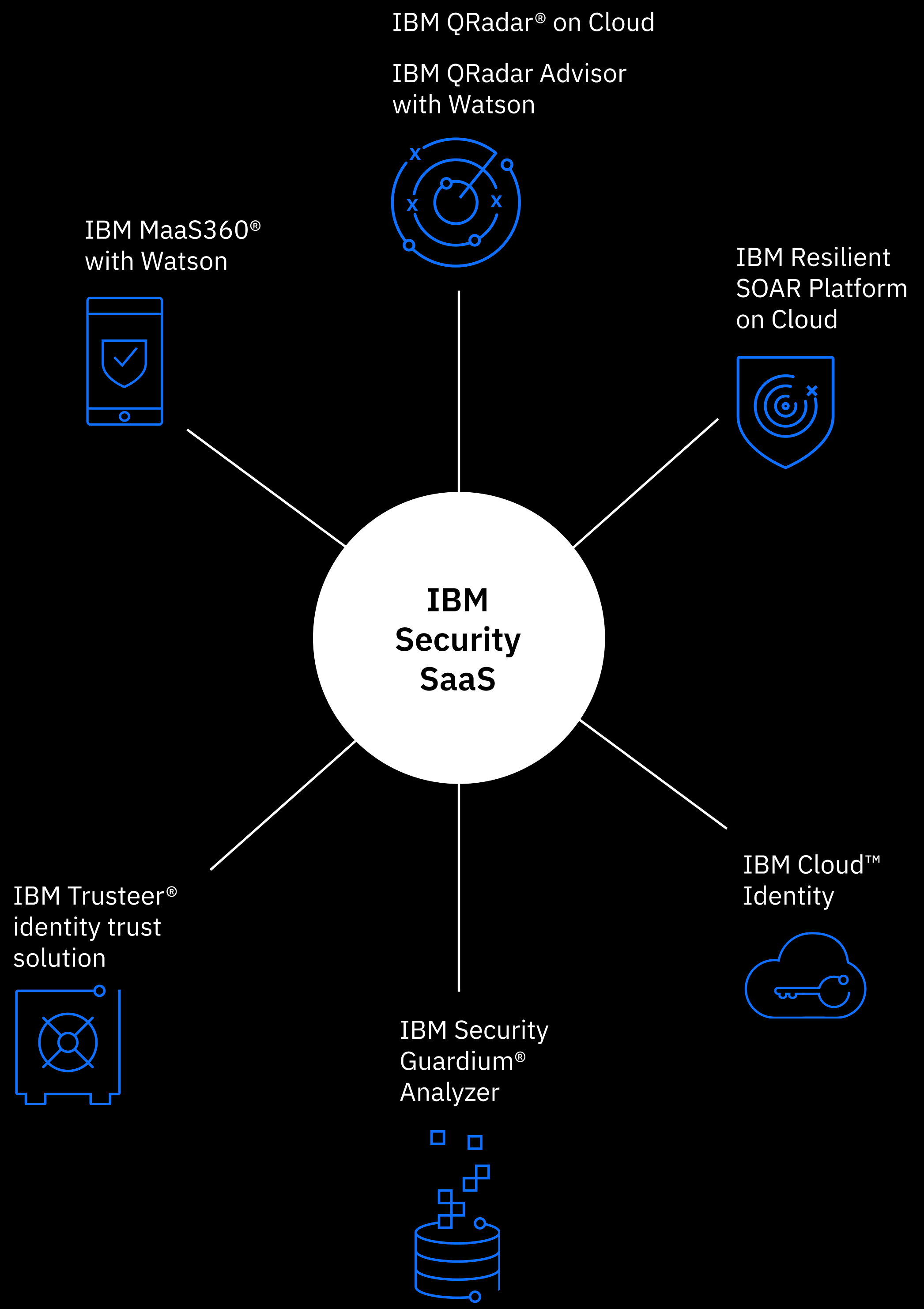
The IBM Security SaaS portfolio complements your existing service offerings, providing full-featured security capabilities at a faster time to value. Our SaaS security solutions combine artificial intelligence (AI) and intelligent orchestration with the agility of the cloud to help you:

– Optimize infrastructure and operational efficiency to maximize margins.
– Build a profitable business with recurring revenue streams.
– Accelerate time to market with best-of-breed cloud services.
– Expand IT expertise and customer reach.

Designed by cloud and security experts, IBM SaaS solutions will prepare you today for the cyberthreats of tomorrow. Adding these services to your own portfolio will enhance the value of your business, helping you achieve greater client satisfaction, scalability, and profit.

Learn more about IBM Security, an industry leader, on the web.

Discover more about the managed security service provider (MSSP) program.


IBM QRadar® on Cloud
IBM QRadar Advisor with Watson
IBM MaaS360® with Watson
IBM Resilient SOAR Platform on Cloud
IBM Security SaaS
IBM Trusteer® identity trust solution
IBM Cloud™ Identity
IBM Security Guardium® Analyzer

IBM QRadar Advisor with Watson

Automate your SOC with AI

QRadar® Advisor empowers security analysts to drive consistent investigations and make quicker and more decisive incident escalations, resulting in reduced dwell times and increased analyst efficiency.

IBM QRadar Advisor can streamline the initial incident assessment phase for the front-line security operations center (SOC) analyst by monitoring the alert queue, collecting investigative data and context for root cause diagnosis, and aligning attacks to the MITRE ATT&CK framework. IBM QRadar Advisor also guides analysts on the next-best action based on learnings from the local environment that assist in making the escalation process more efficient. Additionally, QRadar User Behavior Analytics enables QRadar Advisor to investigate suspicious user behavior automatically and address insider threats.

Learn more about how IBM QRadar Advisor can help automate and augment your security operation center.

51%

of organizations report having a problematic shortage of cybersecurity skills in 2018[4]

IBM QRadar on Cloud

Deliver security intelligence and analytics

IBM QRadar® on Cloud enables security teams to collect, correlate, and analyze information from across data silos—including the cloud—to automatically detect and prioritize threats. It offers access to IBM QRadar capabilities without having to manage the infrastructure.

QRadar on Cloud provides you with a starting point for cloud-delivered security intelligence. This starting point comes from a trusted vendor, delivering industry-leading security information and event management (SIEM) technology, backed by expert services and support.[5] Over time, you have the option to continue the migration to a fully outsourced solution. With deep visibility into both cloud and on-premises infrastructure, QRadar on Cloud can help your organization stay a step ahead of the latest threats.

Discover more: IBM QRadar on Cloud

70%

of IBM QRadar customers say out-of-the-box correlations are very valuable[6]

IBM MaaS360 with Watson

Help secure and enable endpoints with a cognitive approach

The IBM MaaS360 with Watson™ solution is designed for chief information officers (CIOs) who are responsible for managing and securing smartphones, tablets, laptops, desktops, wearables, and Internet of Things (IoT) devices across their organizations. IBM MaaS360 with Watson is the only platform that delivers a cognitive, AI approach to unified endpoint management (UEM) to enable endpoints, end users, and everything in between, including apps, content, and data.[7]

Delivered from a best-in-class cloud, IBM MaaS360 is recognized for its fast, simple, and flexible deployment model.[8] It is offered in an open platform, making integration with existing apps and systems seamless and straightforward. IBM MaaS360 solution provides around-the-clock customer support and consulting services to maximize success and net a quick return on your investment.

With thousands of global customers of all sizes and industries, IBM MaaS360 helps organizations secure corporate data, enable user productivity, and comply with industry regulations.

Learn more about IBM MaaS360 with Watson solution on the web.

Start a trial of IBM MaaS360 solution with Watson at no charge.

47%

of global infrastructure technology decision makers say they are implementing, have implemented, or are expanding, upgrading implementation of UEM[9]

IBM Trusteer

Seamlessly establish digital identity trust across the omnichannel journey

IBM Trusteer® combines continuous digital identity assurance and user-friendly authentication with a scalable and agile cloud platform powered by fraud and risk expertise. It helps businesses assess risk in real time, while providing a seamless customer experience. Intelligence services, infused with layers of AI, create operational efficiencies, which further help reduce costs.

Welcoming the right customers in—while keeping fraudulent activity out—helps businesses protect their brands and enables them to deliver a frictionless experience that can help accelerate growth and digital adoption.

Read the IBM Trusteer Solution Overview to learn more about establishing digital identity trust.

20%

of customer authentication attempts to access their accounts fail[10]

IBM Security Guardium

Identify and classify regulated data risks

IBM Security Guardium® Analyzer helps compliance managers, data managers, and IT managers get started on their data security and compliance journeys by locating regulated data in on-premises and cloud databases, classifying it, identifying vulnerabilities, and helping users take a risk-based approach to data protection.

With IBM Security Guardium Analyzer for data risk analysis, you can:

- Find regulated data using a next-generation classification engine and pre-built data patterns to efficiently find and classify personal and sensitive-personal data
- Uncover risk using a specialized risk scoring technique based on the vulnerability posture of the underlying database and the amount of sensitive data classified.
- Take action with detailed remediation recommendations.
- Improve communication between compliance managers and DBAs, including sharing actions that DBAs need to take to reduce compliance-oriented risk.

Discover more: IBM Security Guardium Analyzer

Watch a demo

2 billion

records were exposed by improperly configured systems in 2017[11]

IBM Cloud Identity

Improve control over who can access business and IT resources

IBM Cloud Identity offers uncomplicated identity and access management capabilities. It supports users' requirements for the applications necessary for their jobs, business leaders' needs to increase productivity for a greater competitive advantage, and IT requirements to more rapidly respond to the needs of the business.

IBM Cloud Identity is simple to deploy and can easily connect to on-premises and cloud-based applications. Employees, consumers, administrators, and application owners gain a seamless user experience, enabling organizations to easily add new SaaS applications with simple business rules governing who can access what, and whether strong authentication beyond username and password is required.

Get a complimentary trial of IBM Cloud Identity.

By 2022, IDaaS will be the chosen delivery model for more than

80%

of new access management purchases, up from 50% today[12]

IBM Resilient SOAR Platform

Empower security operations and response with plans for action

IBM Resilient® empowers security teams to quickly and intelligently analyze, respond to and mitigate incidents. It is one of the industry's only platform with Intelligent Orchestration enabling teams to integrate and automate people, processes, and technologies from a single view.

Intelligent orchestration dramatically accelerates and sharpens response by seamlessly combining incident case management, orchestration, automation, and intelligence into a single platform. The IBM Resilient platform seamlessly combines incident case management, orchestration, automation, and intelligence into a single platform, improving visibility and speeding time to value.

Discover more: IBM Resilient Incident Response Platform

Top cost saving factor

An incident response team can reduce the cost of compromised error by

USD 14 per record[13]

Monetize your SaaS business with IBM

IBM Security is a marketplace leader for SaaS technology. It's also recognized for its best-in-class IBM Business Partner programs. This winning combination equips service providers with capabilities to capture new markets, develop new skills, and grow profits. IBM Business Partners have the added benefits of:

- Go-to-market options: Implement contract terms that range from monthly rental to annual purchase to help build a recurring revenue stream while retaining control of the customer relationship.
- Enablement resources: Enhance your security as a service expertise with resources that include how-to guides, market intelligence, technical support, solution roadmaps, and other helpful tools.
- Co-marketing funds: Leverage IBM funding and marketing assets to help generate demand and increase sales.
- SaaS opportunity management: Utilize My Sales Activity (MySA) to manage your opportunities with one consistent user experience that integrates IBM sales activity tools and processes.
- PartnerSuccess360 (PS360): Get visibility into your clients' SaaS usage and entitlements to help drive smarter SaaS lifecycle conversations.
- IBM SaaS financing: Low rates for stand-alone, prepaid SaaS structures, annual or multiyear.

IBM also strives to provide service providers with personalized support and access to resources that help build, sell, and deploy SaaS solutions. By leveraging IBM PartnerWorld®, you have access to the following programs that can help differentiate and add margin to your SaaS offerings:

- Marketing resources
- Selling resources
- Training resources

Discover more: Spark, the IBM Security Business Partner Community

Join IBM PartnerWorld®

IBM Managed Security Service Provider (MSSP) Program

Help solve your clients' critical security issues and drive your own profitability with a security system that's built on an integrated, industry-leading portfolio. The IBM cybersecurity immune system integrates a wide range of security solutions powered by analytics and orchestration. As an MSSP, you're equipped with a comprehensive toolkit to drive the following critical business outcomes for your clients:

- Prove compliance
- Stop threats
- Grow business

Partnership models for IBM Security MSSPs

The IBM Security MSSP Program is flexible, aligning and supporting your business model and your client's requirements. You can use reseller models when your clients prefer to own the technology or embedded models when you want to deliver technology wrapped in a managed security service.

Discover more about the MSSP program.

The IBM Embed Partner Program.

Learn more about the IBM Reseller Program.

Benefits of becoming an IBM Security MSSP

Solutions

- Access solutions from IBM's industry leading portfolio.
- Apply innovative AI security solutions.
- Access professional and consulting services to develop your managed security business.

Support

- Leverage marketing development funds to drive your business forward.
- Obtain business planning supported by value-added distributors and IBM Security specialists.
- Access to IBM's ecosystem of resellers and technology alliance Business Partners.

Training

- Find technical and sales training on IBM Security Learning Academy at no charge.
- Develop your expertise with security competency programs.
- Learn more with in-person sales, tech sales, and master-skills classes.

For more information

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 IBM 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.

To learn more about IBM Security and talk to an IBM Security representative, visit ibm.com/security.

To learn more about joining PartnerWorld, start here.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2019

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.

Sources:
1. Steve Morgan. “Top 5 cybersecurity facts, figures and statistics for 2018.” *CSO*, January 23, 2018.
2. Eric Newmark. “CloudView 2018: Visualization of Worldwide Survey Results.” *IDC*, June 2018.
3. “Cost of a Data Breach Study: Global Overview.” *Ponemon Institute,* 2018. https://www.ibm.com/security/data-breach
4. Jon Olstik. “Cybersecurity Job Fatigue.” *ESG*, February 6, 2018.https://www.esg-global.com/blog/cybersecurity-job-fatigue
5. “Magic Quadrant for Security Information and Event Management.”*Gartner,* December 3, 2018. https://www.ibm.com/security/security-intelligence/qradar
6. “QRadar Security Intelligence Client Study.” *Ponemon Institute*, 2018. https://www.ibm.com/account/reg/signup?formid=urx-35940
7. “Magic Quadrant for Unified Endpoint Management Tools.” *Gartner,* July 23, 2018. https://www.gartner.com/doc/reprints?id=1-54RIAG7&ct=180628&st=sb
8. “Magic Quadrant for Enterprise Mobility Management Suites.” *Gartner,* June 8, 2015. http://s.nsit.com/content/dam/insight/EMEA/uk/insightcloud/airwatch/Magic_Quadrant_for_Enterprise_Mobility_Management_Suites.pdf
9. Ryan Schwartz, et al. “The Forrester Wave™: Unified Endpoint Management.” *Forrester,* November 21, 2018. https://securityintelligence.com/the-forrester-wave-unified-endpoint-management-q4-2018-new-acronyms-new-leaders-and-how-device-management-has-evolved/
10. Pascual and Marchini. “Preserving Trust in Digital Financial Services: The Role of Identity and Authentication.” *Javelin Strategy and Research*, September 2018. https://community.ibm.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=8db66f67-e74a-f52d-b9b4-5da715608654&forceDialog=0
11. “IBM X-Force Threat Intelligence Index 2019.” *IBM Security*, February 2019. https://www.ibm.com/security/data-breach/threat-intelligence
12. Gregg Kreizman. “Gartner Magic Quadrant for Access Management.” *Gartner*, June 18, 2018. https://www.gartner.com/en/documents/3879469
13. “Cost of a Data Breach Study: Global Overview.” *Ponemon Institute*, 2018. https://www.ibm.com/security/data-breach