

# Introducing the IBM Security App Exchange

*The premier collaboration site for expanding  
the capabilities of IBM Security solutions*



---

## Highlights:

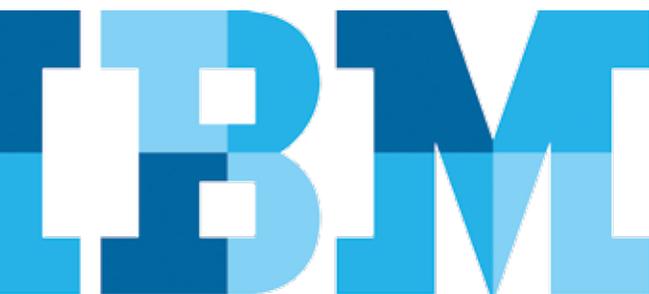
- Provide clients with a single website for accessing a wide range of validated IT security technology enhancements
  - Strengthen network defenses by leveraging insights and add-ons from complementary IBM Business Partner solutions, IBM Security developers and your industry peers
  - Leverage IBM Security technologies as an open platform for developing security applications and sharing content across platforms
  - Enable key components, such as IBM® QRadar® Security Intelligence Platform, to collect more security intelligence data and present it in a holistic manner
- 

A war is raging out there. Every minute of every day, cybercriminals are devising, developing and introducing new and increasingly sophisticated security threats. The global threat landscape is evolving so rapidly that enterprises strain to stay ahead of the next attack, infusion of malware or instigation of fraud. Security professionals face the daunting challenge of making informed, intelligent decisions and springing to action, often with no time to spare.

In such a hostile environment, how can you pinpoint the attacks? How can you determine their impact? How can your security team keep up with all these challenges? Ultimately, how can you quickly and easily improve the security solutions you have in a nimble fashion that addresses the latest threats?

Rapid response is essential to staving off security incidents and plugging vulnerabilities; however, adopting a preemptive approach based on actual experience and best practices is just as critical. The good news is that you don't have to do it alone. The IBM Security App Exchange can help you integrate and utilize the collective knowledge of your peers, who are also constantly working to reduce their attack surfaces.

Designed for convenient web access, the IBM Security App Exchange provides a wealth of benefits to its participants. For customers, it is an avenue for improving security threat awareness and processes, as well as for sharing and obtaining extensions to enhance and customize their IBM Security technology applications. For Business Partners, it is a platform for promoting integrated, complementary product offerings, while also contributing valuable expertise to security teams around the world.



## The IBM Security App Exchange: An ecosystem of maximized value

The pervasive nature of cybercrime underscores the urgent need for ongoing, customized security solutions that add value beyond standard product offerings. It also demands continuous improvements that address new threats and blind spots, openly communicated across the security landscape by your adversaries and allies.

IBM has built a reputation for collecting data from cutting-edge security technology solutions. Today, a growing number of partner products feed information to IBM Security QRadar, IBM BigFix®, IBM Security Network Protection and other IBM Security solutions. For example, QRadar collects log events and network flows from more than 450 applications and devices, which help it provide superior context for security incidents.

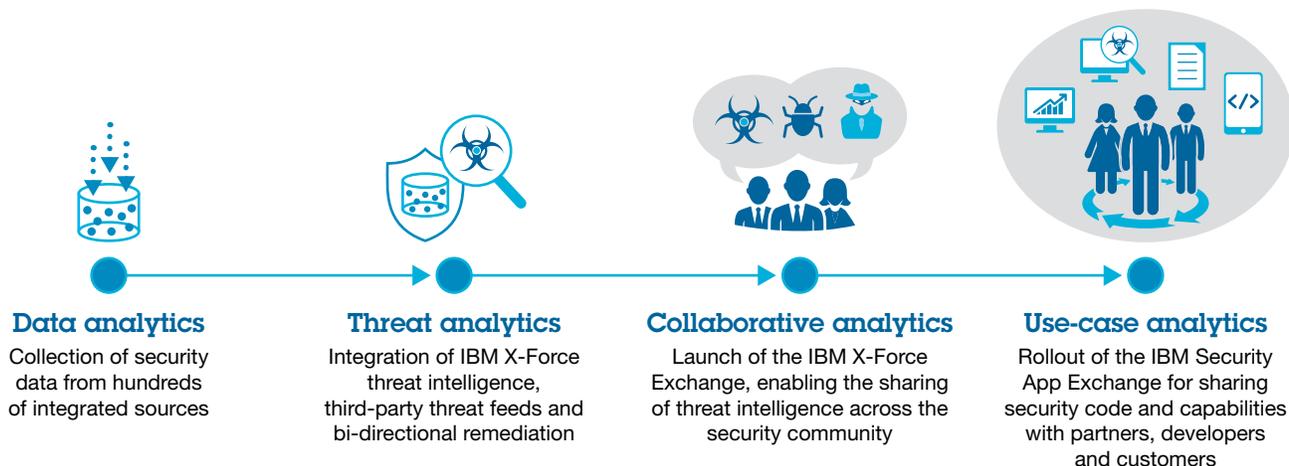
In addition to superior data collection, IBM has evolved its capabilities by integrating credible threat intelligence. IBM Security Network Protection has included IBM X-Force®

threat intelligence since its inception, while QRadar recently added the option of an X-Force intelligence feed to support console alerts about late-breaking threats. Earlier this year, the launch of the IBM X-Force Exchange expanded intelligence gathering to include third parties. This collaborative platform provides access to volumes of actionable threat data from across the globe, tracking 15 billion security events daily in more than 130 countries. It is a 24x7 operation dedicated to keeping companies ahead of the latest threats, and that's exactly the impetus behind the IBM Security App Exchange.

Knowing about a new threat is useful, but finding a solution to defeat it is even better. The IBM Security App Exchange enables participants to share code or post solutions that limit the attacker advantage and help diminish the value of exploit kits and other cybercriminal tools. New application programming interfaces (APIs) and the IBM Security App Exchange will help tip the scale back toward network defenders. It's a win-win in every respect.

---

### The evolution of “collaborative defense” in IBM Security solutions



---

The IBM Security App Exchange is the latest step in the evolution of “collaborative defense” technology integrations in IBM Security solutions.

## The IBM Security App Exchange: How it works

Among the early key assets of the IBM Security App Exchange are QRadar extensions and applications, which include rules, reports, searches, reference sets, custom properties, analytics and dashboards, historical data analysis plug-ins and QRadar applications—leveraging the open QRadar Extension Framework API. This content further enhances the out-of-the-box capabilities of QRadar, so security teams can realize quicker time to value by not having to “re-invent the wheel” to fight specific threats. Similar enhancements to other IBM Security solutions will be posted when they become available. And when new developments surface on the X-Force Exchange, security teams can check the IBM Security App Exchange for an off-the-shelf solution.

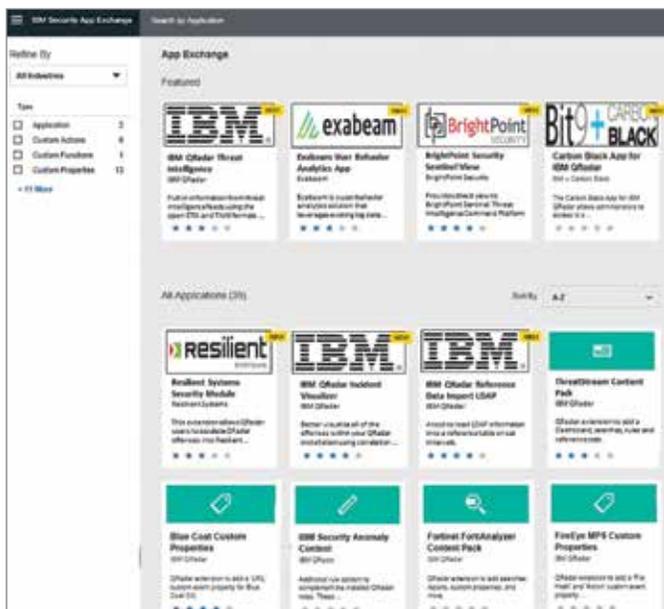
IBM and its Business Partners are actively contributing to the IBM Security App Exchange. When a partner or client creates a QRadar, BigFix, IBM Security Network Protection or other type of extension (or “app”), the IBM Security team quickly verifies the solution to ensure its validity, quality and functionality, and then posts it on the collaboration site for immediate availability.

### Case study: University of New Brunswick

In the North American cybercrime landscape, universities rank second only to healthcare in the number of attacks—and account for 17 percent of reported data breaches.<sup>1</sup> The challenge is remaining open and collaborative, while having the legal and moral responsibility to secure entrusted data. “We need a wide variety of security solutions,” says David Shipley, Director of Strategic Initiatives at the University of New Brunswick. “A holistic ecosystem that deals with next-generation firewalls, network-based malware tools, endpoint protection and advanced virtual private networks, integrated together with a security intelligence platform to share information.”

That ecosystem is QRadar, says Shipley. “QRadar is core in helping us understand both our tactical security and longer-term strategic needs. Any time we have an incident, the first tool we look at to understand what we need to do to protect ourselves is QRadar. Oftentimes in seconds, we can assess the impact of internal or external security threats. QRadar enables us to see the big picture.”

### IBM Security App Exchange home page



The IBM Security App Exchange makes it easy to find content for specific products, industries or threat categories.

---

## Enhancing QRadar deployments

The IBM Security App Exchange provides an expanded hub of QRadar content, so organizations can work together to help defeat advanced threats and improve the efficiencies of IT security teams. QRadar users can download industry-, threat-, device- and vendor-specific content from the collaboration site. Plus, they can access custom reports, dashboards, specialty analytics and threat information, leveraging the Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) standards for threat sharing.

---

## The IBM Security App Exchange: Benefits of participation

It's simple: if the bad guys are colluding, shouldn't we? Participation in the IBM Security App Exchange allows IBM, Business Partners, developers and customers to collaborate and crowdsource content, and build a comprehensive ecosystem around IBM Security offerings. The less time each of us spends developing redundant integrations, behavior analytics profiles, correlation rules and reference sets, the more time we'll all have to monitor suspicious activity, review configurations, patch vulnerabilities and conduct other activities that will reduce our exposures.

## Customer benefits

The IBM Security App Exchange helps customers:

- Address time and skills shortages
- Gain full access to IBM Security portfolio analytics with custom applications such as right-click buttons, tabs, toolbar buttons and visualizations
- Benefit from additional QRadar correlation rules development, dashboards, new visualizations, reference sets and third-party product integrations
- Rate applications based on performance, ease-of-use and other attributes
- Share newly developed content with industry peers

## Partner benefits

By joining the IBM Ready for Security Intelligence Program, and delivering IT security content via the IBM Security App Exchange, participants can expand the reach of value-added technologies that build upon IBM Security solutions, such as QRadar Security Intelligence Platform. A presence on the IBM Security App Exchange website allows Business Partners to:

- Use the IBM Security App Exchange as a channel to reach IBM customers and prospects
- Develop new services and product capabilities based on community posts and input, while mining collective knowledge across the expansive IBM Security community
- Gain wider visibility for promotional and marketing advantages, as well as new sales
- Participate in monthly newsletters sent to more than 300,000 customers, prospects, partners and IBM employees
- Engage via blogs, video references, IBM social media activities, IBM developerWorks®, IBM conferences and sales training events

## Delivering value with the IBM Security App Exchange



With content from the IBM Security App Exchange, security teams can enhance the out-of-the-box visibility of IBM Security solutions, including QRadar Security Intelligence Platform.

### Why IBM?

For years, organizations have made the most of their limited budgets by purchasing point solutions to address their myriad security concerns. But as attackers grow more sophisticated, so must an organization's defenses. IBM Security offers a broad range of technology including the key components of the IBM Threat Protection System—QRadar, IBM Security Network Protection, IBM Security Trusteer® and BigFix—working together to prevent, detect and respond to cybercriminals acting alone or in collusion.

The IBM Security App Exchange decouples new technology integrations and enhancements from formal software release cycles, so customers have more flexibility to extend their IBM Security defenses without adding complexity to the basic

solutions. The platform builds upon the new security intelligence application development framework available in QRadar version 7.2.6 and later. And rest assured, all new integrations, applications and add-ons are validated by IBM development before they're posted to the website and made available for downloading.

The IBM Security App Exchange integrates the threat intelligence of the X-Force Exchange collaboration website and builds on the open and robust platform of QRadar as the focal point for IBM Security technology integration. It is the premier collaboration site for sharing software enhancements to IBM Security products, providing customers, Business Partners, system integrators and IBM with an integrated ecosystem for maximizing the capabilities of IBM Security solutions.

## For more information

To learn more about the IBM Security App Exchange and discover new ways to extend your IBM Security solutions, visit: [apps.xforce.ibmcloud.com](http://apps.xforce.ibmcloud.com)

## About IBM Security

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.



© Copyright IBM Corporation 2015

IBM Security  
Route 100  
Somers, NY 10589

Produced in the United States of America  
December 2015

IBM, the IBM logo, [ibm.com](http://ibm.com), QRadar, X-Force, Trusteer, BigFix, and developerWorks are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

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.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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.



Please Recycle

<sup>1</sup> Ryan Lufkin, "Data Breaches: What Your College Needs to Protect Itself," *Ellucian*, August 18, 2014. <http://www.ellucian.com/Blog/Data-Breaches-What-Your-College-Needs-to-Protect-Itself/>