Integrated threat defense with IBM Security and Cisco solutions

Gain the visibility you need to see a threat once and protect everywhere

Highlights

- Secure the enterprise infrastructure with industry-leading solutions or get security assistance with expert managed services
- Leverage actionable threat intelligence from world-renowned security experts
- Speed threat detection and response
- Take advantage of powerful insights to orchestrate and accelerate incident response
- Simplify and speed security operations center (SOC) investigations
- Download new IBM-Cisco applications (apps) with ease from IBM® Security App Exchange

Cybercriminals have become adept at working together. In fact, it's estimated that 80 percent of cyber attacks are initiated by highly organized criminal groups.[1] By contrast, there's been a glaring lack of cooperation among providers of IT security solutions.

With competition fierce, the inclination among providers has been to keep the inner workings of the security tools they design and the threat intelligence they collect out of the hands of other vendors. In short, criminals who would steal or corrupt valuable business and customer data are collaborating every day, but organizations supporting protection against those threats are not.

Because of this, security teams at individual organizations often have had little choice but to implement point solutions. Because they come from multiple vendors, however, these solutions lack integration—making it difficult to attain the visibility necessary to identify suspicious and malicious activity. Disparate solutions also make it difficult to automate—and therefore speed—threat response.

Now IBM and Cisco have joined forces to address these challenges. In an unprecedented level of collaboration among large security providers, these security leaders have created new integrations to help organizations who need:

- **Software solutions** that provide integrated defenses across networks, users and the cloud
- **Threat intelligence** that's actionable, to help combat the latest security threats
- **Managed and consulting-led services** that can help secure hybrid clouds and the enterprise infrastructure, end-to-end

Leverage an integrated threat defense architecture

A recent Cisco survey found that 65 percent of organizations use more than five security products—and 38 percent use more than 10.[2] Yet amid the growing persistence, sophistication and collaboration among criminals, security teams still have a hard time keeping up. Making matters worse, the security industry is facing a massive talent shortage—predicted to reach 1.5 million open and unfilled positions by 2020.[3] That increases the need for an integrated security approach where solutions work in concert for a systemic response—to see a threat once and protect everywhere, automatically.

To meet this need, the IBM Security-Cisco partnership provides powerful solutions and services to help existing and new IBM and Cisco clients build an integrated threat defense architecture. These offerings are based on three security imperatives:

- **Simplicity:** Eliminating complexity from security tools so deployment, scaling and ongoing management are achievable, even for teams struggling with skills shortages
- **Openness:** Designing solutions for interoperability to create an ecosystem that integrates to become vastly more powerful as products are used together
- **Orchestration:** Enabling automation of security operations so teams can detect and respond to threats more quickly, easily and effectively

---

"The power of this partnership isn't in the products alone … It is in the power of the partnership and the fact that two huge, powerful companies are putting aside their common differences to address the common threat."

—Rob Enderle, Principal Analyst, Enderle Group, TG Daily

IBM and Cisco provide integrated solutions, including software to enhance network infrastructure visibility, enrich threat investigations and speed incident response; threat intelligence for up-to-the-minute knowledge about the latest threats; and managed services to help secure the enterprise.

IBM has added new, out-of-the-box support for recently acquired Cisco products, including Cisco Umbrella (OpenDNS), Cisco StealthWatch (Lancope) and Cisco Meraki. IBM also supports more than 25 Cisco product families that work in concert with IBM QRadar, including:

- Cisco Adaptive Security Appliance (ASA)
- Cisco Sourcefire Defense Center
- Cisco Threat Grid
- Cisco AnyConnect Secure Mobility Client
- Cisco CloudLock
- Cisco Networking Software IOS for CRS, ISR, routers, switches
- Cisco Wireless LAN Controller (WLAN)
- Cisco Catalyst Operating System (CatOS) for Catalyst switches
- Cisco PIX
- Cisco IOS NetFlow and IPFIX
- Cisco Email Security Appliances (ESA) and Web Security Appliances (WSA)
- eStreamer v6.0
- Cisco Unified Communications Manager (CallManager)
- Cisco Firewall Services Module (FWSM)
- Cisco Identity Services Engine (ISE)
- Cisco Aironet
- Cisco Prime Network Control System (NCS)
- Cisco NAC Appliance
- Cisco Security Agent (CSA)
- Cisco Nexus
- Cisco Wireless Services Module
- Cisco Intrusion Prevention System (IPS)
- Cisco VPN 3000 Series Concentrators
- Cisco Secure Access Control System (ACS)

Solutions: Enhance visibility with integration

Integrations for IBM and Cisco solutions are available for download on IBM Security App Exchange. This collaborative ecosystem includes numerous add-ons for IBM QRadar® as well as a host of IBM Business Partner security apps and add-ons.

Make informed decisions at speed and scale

The goal of the IBM Security and Cisco partnership is to close the operational blind spots criminals exploit in attacks. Integrations between QRadar and Cisco solutions provide visibility across networks, endpoints, users and cloud. Two solutions provide the core of these capabilities:

- **IBM QRadar SIEM** can detect anomalies, uncover advanced threats and eliminate false positives. It consolidates log events and network flow data from thousands of devices, endpoints and apps distributed throughout a network. An advanced IBM Sense Analytics™ Engine normalizes and correlates this data and identifies security offenses requiring investigation.
- **Cisco Firepower next-generation firewall (NGFW), through integration with QRadar**, can provide extended visibility across Cisco alerts and log data—derived from Firepower NGFW, intrusion prevention and advanced malware protection capabilities—by flowing it directly into the QRadar security analytics platform.

Used together, these solutions provide:

- A cohesive view that helps security teams understand the full scope and veracity of an attack
- The ability to amplify insights using the Firepower NGFW to send packet data directly to QRadar for analysis
- Support for informed decisions at speed and scale with improved threat detection and response threats based on integrations downloadable from IBM Security App Exchange

Simplify investigations in the SOC

Sandboxing and threat intelligence are key tools for gaining the insights necessary to protect organizations from malware—and the value of each to SOC investigations can increase when they work together in a single, unified solution. A new, combined solution provides these capabilities:

- **Cisco Threat Grid sandboxing with threat intelligence, through integration with QRadar**, helps security teams query the Threat Grid database to find relevant information about attacks, malware and other threats, and use that information to resolve a threat detected by QRadar.

With this solution, security teams can:

- Determine through sandbox analysis whether or not suspicious binary files are malicious
- Avoid opening multiple apps by accessing threat intelligence through the same console analysts use for day-to-day activities
- Download the app quickly via IBM Security App Exchange

Provide insights into internal threats and compromised accounts

The IBM QRadar User Behavior Analytics (UBA) app helps to efficiently detect anomalous or malicious behavior in your organization. It analyzes user-centric events in QRadar, including events from more than a dozen Cisco products, such as the Cisco Identity Services Engine (ISE).

Use insights to speed security incident response

A new integration provides an orchestration hub to speed incident response. New and ongoing investigation and orchestration integrations between IBM Resilient® Incident Response Platform (IRP) and Cisco products can further reinforce threat intelligence.

- **Resilient IRP** provides a central hub that orchestrates the full response process dynamically, enabling faster, more intelligent response and mitigation.
- **Threat Grid integration with Resilient IRP** enables integration with Threat Grid for malware sandboxing and threat intelligence to gain insights and respond to incidents faster.

Using this integration, organizations can:

- Enable Resilient IRP security analysts to research indicators of compromise using Threat Grid threat intelligence
- Detonate suspected malware using Threat Grid sandboxing

<table>
<tr><th colspan="4">IBM Security analytics and orchestration</th><th rowspan="2">Threat intelligence collaboration</th></tr>
<tr><th>Network infrastructure visibility</th><th>Threat investigation enrichment</th><th>Insider threat containment</th><th>Incident response and orchestration</th></tr>
<tr><td colspan="2">IBM QRadar SIEM and IBM Watson for Cyber Security</td><td>IBM QRadar User Behavior Analytics</td><td>IBM Resilient Incident Response Platform</td><td>IBM X-Force</td></tr>
<tr><td>Cisco Firepower next-generation firewall (NGFW)
Cisco Intrusion Prevention System
Cisco Umbrella
Cisco CloudLock
Cisco StealthWatch
...and more</td><td>Cisco Threat Grid</td><td>Cisco Identity Services Engine</td><td>Cisco Threat Grid</td><td>Cisco Talos</td></tr>
<tr><th colspan="5">IBM and Cisco security services</th></tr>
<tr><td colspan="2">Hybrid-cloud services</td><td colspan="3">End-to-end infrastructure security services</td></tr>
</table>

IBM Security

CISCO

An integrated threat defense architecture combines powerful capabilities from security industry leaders IBM and Cisco.

Leverage the power of cognitive security

IBM Watson™ for Cyber Security augments security analysts' ability to fill gaps in intelligence, speed and accuracy by working with QRadar to make sense of structured and unstructured security knowledge. With new QRadar app integrations, organizations can automate threat investigations for cognitive security analysis, gain insights into context and more rapidly understand the seriousness of an attack.

Threat intelligence: Leverage actionable information

Threat intelligence helps organizations better understand the threat landscape and speed threat detection, correlation and response. It gives security analysts deeper insights than they could attain on their own.

Gain insights into the latest cyber threats

With security alerts and advisories constantly being updated, it can be impossible for security teams to stay abreast of the latest threats. To help fill this gap, IBM X-Force® Incident Response and Intelligence Services (IBM X-Force IRIS) and Cisco Talos Security Intelligence and Research Group (Talos) collaborate on research to help clients address challenging security problems. Reducing the playing field for attackers and making the attackers' presence known to clients are ongoing priorities.

- **X-Force IRIS** is a team of security experts that provides threat intelligence, incident response and proactive services, and remediation services.
- **Talos** provides threat detection and correlation, industry-leading expertise, and threat research and education.

Threat intelligence in action

In response to the 2017 WannaCry[2] ransomware attack, IBM and Cisco researchers coordinated their actions and exchanged insights into how the malware was spreading. Afterward, they continued the joint investigation to provide clients and the industry with the most relevant information.

Correlate threats instantly

Integration between IBM X-Force Exchange and Threat Grid greatly expands the historical and real-time threat intelligence security analysts correlate to provide clients with deeper insights.

- **X-Force Exchange** is a cloud-based platform that includes 700 TB of threat intelligence data and enables members to rapidly research the latest global security threats, aggregate actionable intelligence and collaborate with peers.
- **Threat Grid** advanced sandboxing with threat intelligence helps protect against malware. Combined with X-Force Exchange data, a malware knowledge base in Threat Grid helps users understand what malware is doing, the scope of the threat and how to defend against it.

Managed services: Simplify security, end-to-end

Managed services help security teams overcome skills and staffing shortages and gain the expertise they need to better secure the enterprise, whether on-premises, in the cloud, or a combination of the two.

Extend enterprise security to the cloud

Today, 85 percent of organizations have a multi-cloud strategy.[4] But many struggle with extending the enterprise-grade security policies they use to protect their on-premises infrastructures to cloud environments. The cloud creates new entry points into the network—for example, through software-as-a-service apps and the Internet of Things. To protect against these threats, organizations need an approach to cloud security that is different from on-premises protection.

To reduce the complexity of security in a hybrid cloud environment, IBM Managed Security Services supports Cisco security platforms in leading public cloud services, including IBM Cloud.

Solidify security, end-to-end

In addition to providing cloud-based security, IBM Managed Security Services provides a design and implementation service for a broad security assessment across the enterprise infrastructure—and a plan for putting the necessary solutions in place. This service leverages Cisco Design Zone Security Reference Architecture to deliver end-to-end security across the organization's infrastructure using:

- Firepower NGFW endpoint platform
- Firepower next-generation intrusion prevention system (NGIPS) network platform
- Cisco Threat Grid malware sandboxing and threat intelligence
- Cisco Web Security Appliance (WSA), Cisco Umbrella, Cisco Email Security Appliance (ESA), and Cisco Cloud Email Security (CES) for web and email security on-premises and in the cloud
- Cisco StealthWatch and Cisco ISE for context-aware security analysis

Why IBM?

The ongoing collaboration between IBM and Cisco is helping organizations to strengthen their posture against increasingly sophisticated cyber attacks. Rather than working in silos, as is the industry norm, these two leading security providers are collaborating to build solutions and share threat information that will empower clients to act at extreme speed and scale, to see a threat once—and protect everywhere.

For more information

To learn more about IBM Security integrations with Cisco security offerings, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

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
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
June 2017

Please Recycle

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.

[1] Caleb Barlow, "It's time for the democratization of cybersecurity data," *Security Intelligence*, November 21, 2016. https://securityintelligence.com/its-time-for-the-democratization-of-cybersecurity-data/

[2] "Cisco 2017 Annual Cybersecurity Report," *Cisco*, January 2017. http://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

[3] Julie Peeler and Angela Messer, "(ISC)^2 Study: Workforce Shortfall Due to Hiring Difficulties Despite Rising Salaries, Increased Budgets and High Job Satisfaction Rate," *(ISC)^2 Blog*, April 17, 2015. http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html

[4] "Rightscale 2017 State of the Cloud Report," *Rightscale*, January 2017. http://www.rightscale.com/lp/2017-state-of-the-cloud-report

WGS03112-USEN-00