Solution overview

IBM Security and Cisco Security: Getting Ahead of Compliance

Maintain data privacy and regulatory compliance

What we're hearing from customers:

"Help my organization maintain data privacy and regulatory compliance."

Compliance continues to be a top concern based on feedback from our joint clients. The IBM and Cisco alliance is uniquely positioned to effectively manage an organization's risk, compliance, and governance with advanced integrations, consulting, and managed services.

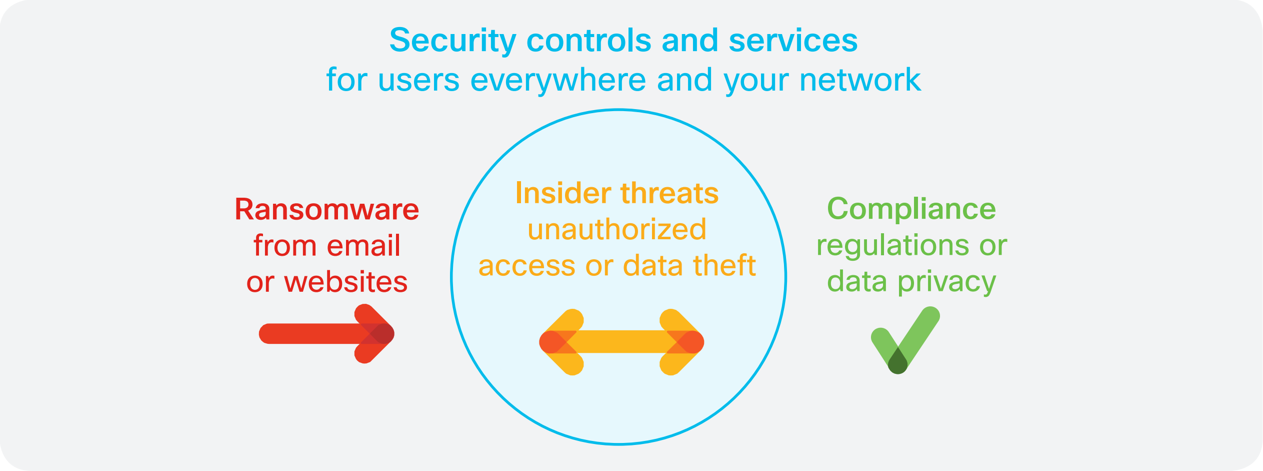
Organizational risk profiles continue to expand beyond internal perimeters and now include exposure from customers, partners, vendors, and Bring-Your-Own-Device (BYOD) programs with access to enterprise assets. With this increased risk, data privacy and compliance are no longer a check-the-box; they're mission critical. Sixty-four percent of security executives globally feel that adhering to compliance requirements is a "very" or "extremely" effective way to keep data secure, and 69 percent of executives plan to hire an outside technology firm to better allocate their resources and help manage security risks and compliance requirements.

Better together

IBM Security and Cisco have partnered to address the growing need for deeper collaboration. Chief Information Security Officers (CISOs) are demanding best-of-suite solutions versus siloed products as some enterprises are managing up to 85 tools from 45 different vendors. The IBM and Cisco strategic alliance delivers more effective security via integrated solutions, managed services, and shared threat intelligence while simplifying vendor relationships for joint customers.

Detecting threats to compliance

Despite the best controls in place to minimize the attack surface, attackers are still finding security weaknesses and new methods to exploit networks. Cisco and IBM Security are working together to help organizations quickly discover malicious activities and efficiently remediate threats while complying with strict regulatory timelines. Cisco Stealthwatch and ISE can monitor user behaviors on the network to look for policy violations or network behavioral indicators of compromise. IBM builds upon these capabilities with QRadar's visibility into event traffic to prioritize suspected threats on the network. Furthermore, IBM QRadar has out-of-the-box compliance packages that provide security teams with the ability to implement and report on security and privacy controls in order to comply with a range of compliance and policy controls. This is further empowered by the IBM Security QRadar User Behavior Analytics (UBA) app, providing ready-to-go anomaly detection, behavioral rules, and analytics while leveraging the curated log and activity data already in QRadar—thereby speeding time to insights. The combined functionality helps security analysts become more productive and manage compliance threats more efficiently.


Security controls and services
for users everywhere and your network
Ransomware from email or websites
Insider threats unauthorized access or data theft
Compliance regulations or data privacy

Preventing compliance violations with planning and controls

The IBM Security and Cisco alliance understands that raising the bar of entry helps joint customers reduce the attack surface and adhere to compliance and privacy controls, including GDPR, HIPAA, PCI, ISO27001, and FISMA. This solution includes IBM MaaS360 Mobile Device Management to ensure all systems and endpoints are patched, maintained, and managed to meet compliance standards. Cisco Firepower® Next-Generation Firewall (NGFW) further hardens the network perimeter while providing enforcement points. A companion solution, Cisco® Identity Services Engine (ISE) (powered by the Cisco DNA Center™) orchestrates who is using the network and sets policies to ensure appropriate role-based access controls and that user governance stays current (zero trust). Cisco Stealthwatch® gives visibility into traffic on the network to provide insights into how systems communicate, allowing operators to form better policies. To further reduce the attack surface, IBM Guardium Data Protection classifies critical data assets and adds them to the list of policy assignments, preventing data loss from databases, data warehouses, and big data environments while ensuring the integrity of information and automating compliance controls and audits. IBM Guardium working in parallel with the IBM QRadar Security Information and Event Management (SIEM) platform can provide security teams with a better understanding of their asset inventory and vulnerabilities including PII data and at-risk assets while complying with external regulations by leveraging prebuilt reports and templates.

Responding to compliance threats and compromises

In the event of a breach, many organizations must comply with cybersecurity and privacy regulations that require additional actions be taken to identify potential exposure and notify regulatory bodies and those affected. Cisco Stealthwatch, Cisco Umbrella™ Investigate, and IBM QRadar give security teams the ability to leverage the audit trails of all network activity to identify additional risk and perform postmortem analysis. Cisco ISE can review and update role-based access controls and segmentation policies. The IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform further complements the response toolset by orchestrating incident response across people, processes, and technology and providing a single, auditable record of all aspects of the incident. If a data breach has occurred, the Resilient platform can then add tasks to the playbook to guide the privacy and legal teams through the breach response process for more than 170 state, federal, and global privacy reporting regulations. All reporting information is consolidated in the one platform, and dashboards and reports help management track their status.

Professional services to assist and enhance compliance strategy

Cisco and IBM Security can help organizations maintain data privacy and regulatory compliance with services and security programs designed with compliance at the forefront of product development. The attack continuum's technical capabilities are supported by Cisco and IBM's services organizations and business partners and are comprised of consultants and implementation experts who are dedicated to ensuring that the proper policies and best practices are leveraged to gain the maximum benefit for these products across the entire attack continuum.

Services include assistance with the implementation, management, and maintenance of these technologies to help customers achieve a more effective and compliant security posture. IBM Security Strategy, Risk, and Compliance Services helps address evolving regulatory requirements and helps protect your business from growing threats. Learn to better manage your risks, compliance, and governance by teaming with our services experts. We provide an objective evaluation of your security controls, mechanisms, and goals, utilizing proven best practices and industry standards. Based on this assessment, we can help you develop an actionable plan for optimizing IT resources and better manage for compliance. We provide secure framework and risk assessment services, PCI compliance advisory services, SAP security, GRC strategy services, and much more. Overall, the services help with evaluation and provide recommendations for better management of risks, compliance, and governance.

The Cisco and IBM Security advantage

The ongoing partnership between IBM Security and Cisco helps organizations strengthen their posture against increasingly sophisticated cyber attacks. Rather than working in silos, these two leading security providers are collaborating to deliver solutions and share threat information that empower clients to rapidly detect and respond to threats while simplifying vendor relationships.

Next steps

Download joint product apps:
IBM Security App Exchange

Additional resources:
cs.co/ibmsec and https://www.ibm.com/security/community/cisco

Opportunities and connections:
For IBM: cisco-ibm-security@us.ibm.com,
and for Cisco: cisco-ibm-security@cisco.com

C22-742562-00 07/19