IBM Security

CISCO

IBM Security and Cisco Security: Addressing Insider Threats

Gain insight and take action on insider threat activities

What we're hearing from customers

"Help my organization apply more focus on insider threat activities."

From joint engagements across the world, the IBM and Cisco alliance continues to identify insider threats as a top customer concern, and our partnership is uniquely positioned to address this threat vector with advanced integrations, consulting, and managed services.

Insider threats—whether malicious insider, compromised internal hosts, or compromised credentials—are among the costliest and hardest to detect. In many instances, the insider threat does not leverage malware or exploits during the activity and adheres to "acceptable use" policies. Two-thirds of total data records compromised last year were the result of inadvertent disclosure, and insider threats are the cause of 60 percent of cyber attacks. Additionally, according to the Ponemon Institute's "2018 Cost of Insider Threats" report, the average cost of insider-caused incidents was $8.76 million in 2017—more than twice the $3.86 million global average cost of all breaches during the same year.

While controls and access are important, this isn't a problem that is solved by a Next-Generation Firewall (NGFW) or Next-Generation Intrusion Prevention System (IPS) alone. Organizations need a layered, multipronged defense approach that protects and remediates across the entire threat kill chain. The IBM and Cisco alliance helps customers across this attack lifecycle for insider threats with defensive technologies to block known bad activity and additional capabilities and analytics to quickly prioritize suspicious actions and remediate the malicious activity.

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 best-of-breed solutions 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.

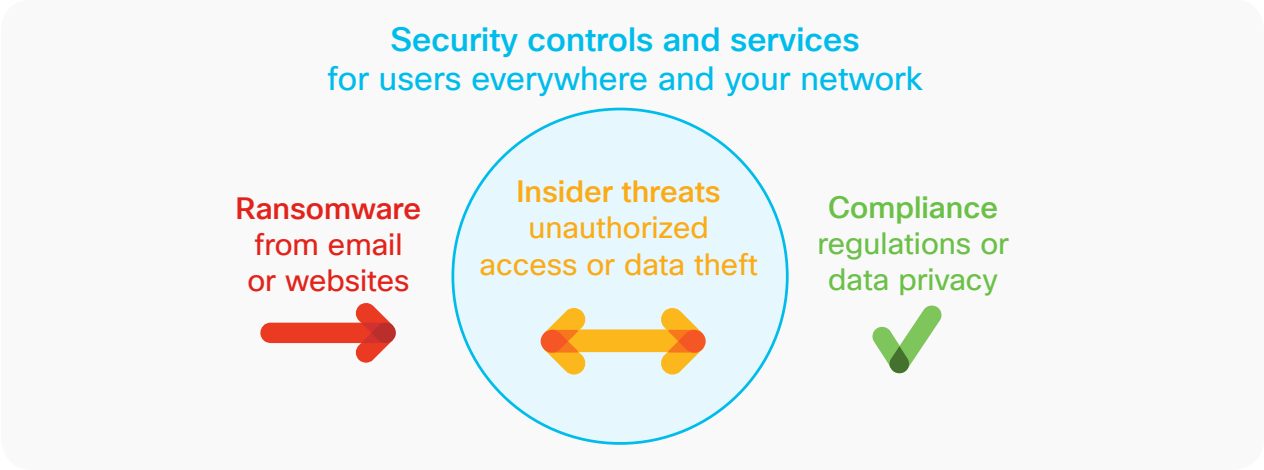
IBM Security

CISCO

Prevention: Reducing the attack surface

While absolute prevention of targeted attacks may be difficult to maintain, raising the bar of entry for attackers is necessary for customers to reduce the number of incidents they experience. Cisco and IBM Security have complimentary toolsets to reduce exposure to insider threats. Cisco® Identity Services Engine (ISE) (powered by Cisco DNA Center™) ensures appropriate network segmentation to limit east-west traffic and limit role-based access to reduce undesired access to resources. A companion solution, the Cisco Firepower® Threat Defense (FTD) firewall and IPS functions at critical locations to restrict application usage and user access through various gateways and block malicious activity. With IBM Guardium Data Protection, identification and classification of critical data assets can be added to the list of policy assignments that reduce the overall attack surface.

In addition, if the attack is due to compromised assets that phone home (for example, command and control), Cisco Umbrella™ uses its DNS knowledge to block malicious destinations before a connection is ever established.



Accelerate threat detection: Identifying unknown threats inside the network

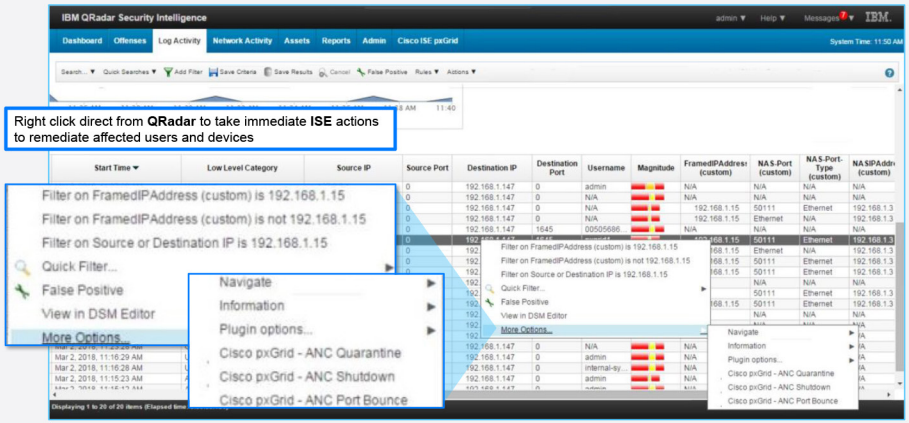
As mentioned before with insider threats, many times the attacks don't leverage malware or exploits to accomplish their goals; they leverage privileged access entitled to machines or users. Cisco and IBM have joint solutions targeted at investigating the suspicious activities that could result in compromised systems/credentials as well as prioritizing investigation of suspicious activities performed by your internal systems.

In some instances, systems and users are compromised as a result of new attacks against them. Here we see technologies like Cisco Advanced Malware Protection (AMP) flag suspect activity as it flows through your NGFW or Cisco Email Security Appliance (ESA) or Web Security Appliance (WSA) technologies. Cisco Stealthwatch® inspects transactional audits (for example, NetFlow, IPFIX, and so on) to look for behavioral indicators of compromise (for example, Bob in accounting is permitted to access our financial servers, but he doesn't normally download so much of the information, nor does he normally make large uploads immediately afterward). With the addition of Encrypted Traffic Analytics (ETA) to Stealthwatch's suite of tools, it has improved capabilities to identify encryption and find malicious activity traversing encrypted channels without ever having to decrypt the information. IBM QRadar builds upon detection provided by Cisco FTD, Stealthwatch, AMP, and other tools to prioritize and correlate threats from logs events and network traffic so security teams can quickly identify and scope insider threats based on potential business impact. Additional solutions, QRadar User Behavioral

Analytics (UBA), QRadar Advisor with Watson, and IBM Guardium Data Protection can drive faster investigations, helping teams to understand employees' relationships with data and baseline behavior, dynamic alerts, data masking and blocking, and user quarantines. Integration with tools like Cisco ISE further allows IBM QRadar to not only associate the activity to the user credentials used, but also take action against those users through rapid threat containment functionality in Cisco ISE to quarantine the user and lock down network access.

Detect suspicious activity and quarantine bad actors directly from QRadar

Cisco ISE App for QRadar



Response and remediation: Orchestrated threat response

Depending on how quickly security teams have responded to the attack, it is possible that additional actions must be taken to identify potential exposure. Cisco Stealthwatch, Cisco Umbrella Investigate, IBM QRadar, and IBM QRadar Advisor with Watson give security teams the ability to leverage the audit trails of all network activity to identify additional risk and perform postmortem analysis. The IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform provides a place for incident responders to conduct threat investigations as well as remediation and breach analysis in an organized and repeatable fashion. This includes insider threat response playbooks, automating key functions through integrations with QRadar, Cisco AMP, and Cisco Umbrella, and providing the coordination and communications strategy across teams and inside and outside the Security Operations Center, or SOC (for example, updating segmentation or user access policies within ISE). These workflows help companies understand not just the technical elements of the defense, but also how to orchestrate incident response across people, processes, and technology. Findings and best practices can then be shared with the security communities via Cisco Talos® and IBM X-Force® Exchange to further strengthen detection for all of the products. This comprehensive and integrated toolset enables security teams to achieve faster, more intelligent incident response and mitigation.

Professional services and managed services

These technical capabilities are supported by Cisco and IBM's services organizations and business partners comprised of experts who are dedicated to ensuring that the right policies and best practices are leveraged to gain the maximum benefit for these products across the entire threat kill chain. These services include professional and management security services from IBM Security. IBM Security services can help with identity and access strategy and assessment, governance and administration services, and design and deploy services. To operate and deliver continuous improvements and optimization to client's Identity and Access Management, or IAM program, IBM offers managed identity services. IBM also offers Privileged Access Management (PAM) as a service as well as cloud IAM services. In addition, to specifically combat insider threats, IBM offers insider threat protection services.

IBM Security

CISCO

The Cisco and IBM Security advantage

The ongoing collaboration between IBM Security and Cisco helps organizations 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.

Next steps

Download joint product apps:
IBM Security App Exchange

Additional resources:
cs.co/ibmsec and 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

C22-742560-00 07/19