IBM Security

CISCO

IBM Security and Cisco Security: Addressing Ransomware

Protect against ransomware attacks

What we're hearing from customers

"Help my organization better protect against ransomware attacks."

Ransomware has quickly become one of the fastest growing and profitable types of malware ever seen. According to the Cisco Annual Cybersecurity Report, ransomware is growing at a yearly rate of 350 percent and campaigns can generate up to $60 million in a single exploit kit, costing billions of dollars in damages to organizations.

Like any attack vector, businesses want to prevent ransomware and combined solutions from Cisco and IBM Security do this with a high degree of accuracy. Mechanisms to prevent known ransomware types and detection of the new, unknown variants are critical to protecting critical assets. Cisco and IBM offer best-in-class solutions to safeguard businesses with solutions reinforced by lessons learned from the extensive customer base of both organizations as well as their threat research teams, Cisco Talos® and IBM X-Force. Even with these controls, there is always the risk of ransomware getting in, but Cisco and IBM have extensive tools to help organizations respond with speed and confidence.

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.

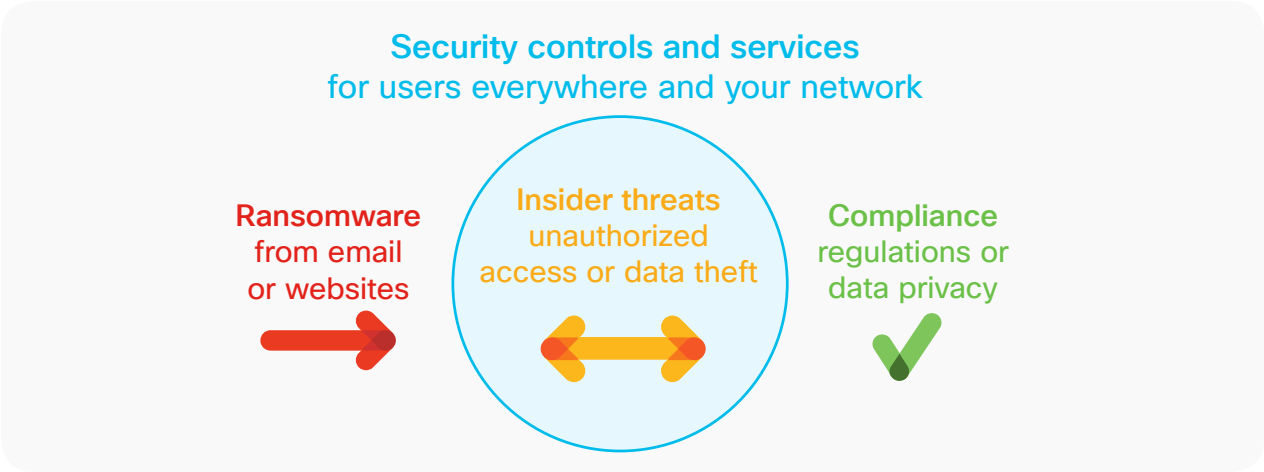
IBM Security

CISCO

Prevention for known ransomware

Raising the bar of entry by proactively improving fundamental security controls can help joint customers reduce the attack surface and incidents experienced. This solution includes IBM QRadar Vulnerability Manager, which regularly scans the environment for security vulnerabilities and uses advanced analytics to enrich the results of those scans, lowering risk and automating compliance checks. Cisco® Email Security products close off the most common attack vector by blocking known ransomware variants from entering the network. Additionally, technologies like Cisco Umbrella™ prevent users from accessing known malicious domains and block URLs that could house malware.

In the rare instances that ransomware gains a foothold in the network, tools like Cisco Identity Services Engine (ISE) would restrict lateral movement found in some of the newer ransomware variants. A companion solution, Cisco Firepower® Threat Defense (FTD) firewalling functions at critical locations, restricts application usage through various gateways, and blocks malicious activity.



Detecting unknown variants of ransomware

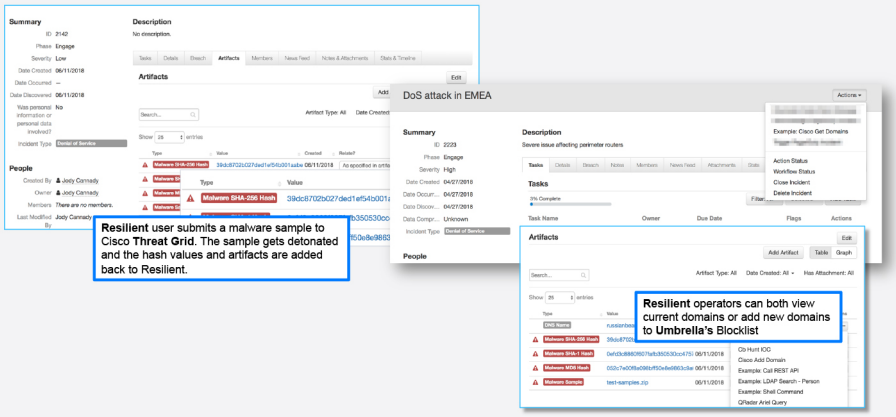
Due to the rate of evolution of ransomware threats, it's important to have technologies capable of detecting the new, unknown threats. Leveraging Cisco Advanced Malware Protection (AMP) extensions and Cisco Email Security Appliance (ESA) and Web Security Appliance (WSA) can identify suspicious files to quarantine and detonate within Cisco Threat Grid before they reach the end user. To further augment threat detection, Cisco AMP is deployed across Cisco Firepower Next-Generation Firewall (NGFW) Intrusion Prevention System (IPS) and AMP for Endpoints products to keep known ransomware executables off the impacted systems, including patient zero. All of these products are supported by a wealth of data analytics from the Cisco Talos security intelligence teams.

In instances where ransomware is first seen or time bombed or has lateral movement such as with Wannacry, we see secondary detection play a critical role. Cisco and IBM Security are delivering joint capabilities to accelerate the detection of ransomware threats during an attack. The IBM QRadar Security Analytics Platform provides complete visibility into logs and events across all environments, identifying suspected ransomware threats early in the attack cycle, then generating prioritized alerts as the attack progresses through the kill chain. This allows analysts to look at more of the "suspect" risks to identify more of the unknown threats and reduce the impact of these ransomware variants. QRadar is further bolstered by direct feed from IBM X-Force Exchange, a threat intelligence platform that enables organizations to rapidly research and stay ahead of emerging threats, including actionable intelligence to identify and remediate ransomware activity.

Responding to ransomware

Automation between resilient and Cisco speeds up response time

Cisco Threat Grid and IBM Resilient



If an attack manages to evade detection and compromise a host, additional actions must be taken to identify and respond to potential exposure. Cisco Threat Grid's threat intelligence and integrations with IBM QRadar (including QRadar Watson and Network Insights add-ons) can help security teams to accelerate the identification of the ransomware variant, the root cause, and how the malware entered and tunes detection mechanisms based on lessons learned. Further threat analysis such as suspicious domain containment findings within Cisco Umbrella Investigate and Enforcement and all Cisco and IBM integrated products can then be pulled into an incident report via integrations with the IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform. The Resilient platform would generate a ransomware playbook, containing all of the technical and business process steps to respond to the attack with automated and manual actions driven across the relevant security tools. This playbook will be updated and can dynamically change as the incident evolves to keep the team inside and outside the Security Operations Center, or SOC aligned on the relevant next steps Findings and best practices can then be shared with the security communities via Cisco Talos and IBM X-Force Exchange to further strengthen detection of all 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 Security'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 attack continuum.

These services include professional and managed security services from IBM Security. IBM Security services help organizations cope with ransomware attacks and other critical security incidents and work to eradicate threats and otherwise minimize their impact to business. For example, after the Petya attacks, IBM Security X-Force released their Petya Advisory, which provided an overview of Petya as well as recommendations to help prevent such attacks.

IBM cyber resilience services provide an additional layer for countering ransomware attacks by providing an orchestrated resilience approach that helps identify risks, protect applications and data, and rapidly recover IT.

IBM Security

CISCO

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 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

C22-742561-00 07/19