Overview

Cisco and IBM Security have developed integrations to assist customers throughout the attack lifecycle. We'll discuss how integrations between Cisco® Advanced Malware Protection for Endpoint (AMP4EP) and IBM QRadar and Resilient can help customers prioritize threats when malicious activity occurs, and remediate after attacks are identified.

AMP4EP removes known bad activity before it impacts the network. QRadar Security Analytics is then able to inspect more of the suspect malicious activity helping customers to prioritize threats against identified attack vectors, and to respond to the most urgent first.

Once malicious activity has been identified, the integration with Resilient helps you remediate and notify adjacent teams.

Cisco and IBM: Better Together

Keeping up with the ever-evolving security needs of modern organizations is a challenge, and in many instances requires different products from a large number of vendors. Cisco and IBM are coming together to provide integrated security solutions that help you reduce the number of security vendors, increase visibility and coverage of those security products and correlate the sources of data so you can make better, faster security decisions – all with award-winning products and tailored services.
Benefits

Cisco AMP4EP with IBM QRadar
- QRadar ingests threat events and telemetry directly from AMP4EP
- Threats identified by AMP4EP can be correlated and prioritized on a consolidated dashboard with other events in QRadar
- QRadar integration with IBM Resilient speeds the incident response process by moving seamlessly from detection to remediation

Cisco AMP4EP with IBM Resilient
- AMP4EP integrates with Resilient for efficient, coordinated breach response
- Faster response means less opportunity for malware to cause damage
- Relevant data can be pulled from AMP4EP into Resilient and linked to an incident
- Resilient can quickly quarantine malicious files across the entire AMP4EP deployment

Trends and challenges

The Cisco CISO Benchmark study reported that vendor consolidation is a huge trend that accelerated between 2018 and 2019, which indicates that CISOs want less-complicated security solutions that speed up detection and remediation times. The Cisco and IBM security partnership aims to do just this with a complete set of integrations available free of charge on The IBM App Store, plus a full selection of services, including managed services.
How it works

The Cisco AMP for Endpoints integration with IBM’s QRadar provides a consolidated view of security events across endpoints in a single dashboard, eliminating the need to toggle between tools and monitoring of real-time endpoint threat detection. Security analysts can search, correlate and analyze AMP for Endpoints threat events within QRadar. Then, they can quickly drill down into threats detected by AMP; including identifying the user who initiated the attack, which machine the threat originated from and which file triggered the attack.

The Cisco AMP for Endpoints integration with IBM Resilient combines enrichment and containment in one consolidated tool; providing the actionable insights needed to accelerate threat detection and incident response. Analysts within Resilient can investigate AMP for Endpoints events for possible malicious activities. Security teams can then automatically pull findings into an incident, rapidly drill down on a threat detected for further analysis and quickly quarantine any malware detected.

The Cisco Security and IBM Security advantage

The ongoing collaboration between Cisco Security and IBM Security helps organizations strengthen their security posture against increasingly sophisticated cyber attacks. Rather than working in silos, 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.