LogRhythm and Cisco: Integrated Enterprise Security

In the past, desktops, business apps, and critical infrastructure were all located behind the firewall. Today, more and more is happening off-network. More roaming users. More corporate-owned laptops accessing the internet from other networks. More cloud apps allowing users to get work done without being connected to the corporate network. And more branch offices connecting directly to the internet.

By 2021, Gartner predicts the average company will have 25% of its corporate data traffic bypassing the network perimeter. When a user is participating on non-corporate protected networks, they are more vulnerable to malware and attacks, and the organization lacks visibility and protection. If you rely on perimeter security alone, you're not fully protected. These gaps open the door for malware, ransomware, and other attacks.

Organizations using cloud services need to parallel the level of protection that has been available within the perimeter to be able to detect anomalous user behavior, (including compromised accounts and malicious insiders,) enforce and demonstrate compliance, detect toxic content, ensure security best practices are being followed, and identify data exposures from over-sharing.

The Integration Provides:

The Cisco Cloud Security (Umbrella and Cloudlock) and LogRhythm integration allows organizations to:

- Gain visibility to your endpoints and users even from remote locations
- Block malicious domains and IP addresses
- Investigate malicious indicators of compromise (ie. domains, IPs, ASNs, file hashes, and email addresses)
- View a single pane of glass for all security incidents and correlation, including cloud and on-premises insights
- Prevent account compromise and data leaks in the cloud
- Detect cloud malware
- Meet compliance requirements
- Investigate security incidents and suspected data breaches
- Coordinate security across existing investments

By combining Cisco's cloud security enforcement and intelligence with LogRhythm's security data analytics and threat intelligence, customers can reduce the time to detect and contain threats, increase visibility into internet activity across all locations and users, identify cloud apps used across the business, and reduce remediation costs and breach damage.

About LogRhythm

- Empowers organizations to rapidly detect, respond to and neutralize cyber-threats
- Provides a holistic platform for end-to-end Threat Lifecycle Management, uniquely unifying next-gen SIEM, log management, network & endpoint forensics, advanced behavior analytics & machine learning, and security automation and orchestration
- Delivers rapid compliance automation and assurance, and enhanced IT intelligence
- Consistent market leadership including recognition as a Leader in Gartner's Magic Quadrant since 2012

About Cisco Cloud Security

- Cisco Umbrella a Secure Internet Gateway (SIG) that provides the first line of defense against threats on the internet, wherever users go.
- Umbrella delivers complete visibility into internet activity across all locations, devices, and users, and blocks threats before they ever reach your network endpoints.
- Cisco Cloudlock is the cloud-native Cloud Access Security Broker (CASB) that helps accelerate use of the cloud.
- Cisco Cloudlock secures your cloud users, data, and apps, combating account compromises, data breaches, and cloud app ecosystem risks, while facilitating compliance through a simple, open, and automated API-driven approach.

The Cisco Cloud Security and LogRhythm partnership enables customers to gain cross-platform visibility into activity and cross-reference data across both on-premises and cloud environments. This enables the aggregation of cloud security intelligence with other data within LogRhythm for comparative analytics and superior security.

LogRhythm for Unified Threat Lifecycle Management

- Dynamic defense for detecting and stopping unauthorized network threats
- Multi-dimensional behavioral analytics to deliver real-time security intelligence
- Deep visibility into all aspects of user, network and endpoint behavior activity throughout the IT environment
- Tight integration for consolidated threat management

Automated Data Enrichment and Threat Enforcement (Umbrella)

Challenge:
As threats evolve, organizations purchase more and more point solutions to mitigate new risks. While this results in more data available for analysis, many organizations struggle to prioritize threat indicators, and build effective integrations between their disparate systems.

Solution:
With the "out-of-the-box" Umbrella and LogRhythm integration, organizations achieve faster identification of threats and reduced infections. **Umbrella Investigate** sends threat intelligence about domains, IPs, and file hashes to LogRhythm's AI Engine, providing additional context to prioritize the most concerning alarms. Additionally, malicious domains and IP addresses found by LogRhythm can be added to Umbrella to be automatically enforced globally.

Additional Benefit:
Organizations have the rich context needed to prioritize threat response and speed up investigations. In addition, organizations can accelerate time-to-value with automated, up-to-date protection across all users, no manual intervention required.

Comprehensive Visibility On-Premises and in the Cloud (Cloudlock)

Challenge:
Security professionals today do not have full visibility of cloud activity and how it relates to on premise events, thus creating a blind spot to determine threat to the organization's critical assets, such as account compromise, insider threats or unauthorized data exfiltration.

Solution:
The **Cloudlock** integration provides security professionals with a complete picture of threats and risk posture of their infrastructure. **Cloudlock** provides security incidents from your sanctioned applications as well as risk posed from the unsanctioned applications. These range from data leak incidents to user behavior. The wide variety of events such as exposure of sensitive information, sharing of sensitive content, offsite access, and application behavior provides rich indicators of compromise and shows in-depth risk profile of a customer's cloud infrastructure.

Additional Benefit:
Administrators can create and execute, or leverage existing LogRhythm SmartResponse™ actions from an alarm or investigation to enable dynamic, precise, and automatic actions such as automatically locking down a compromised account to reduce the risk of data exfiltration.