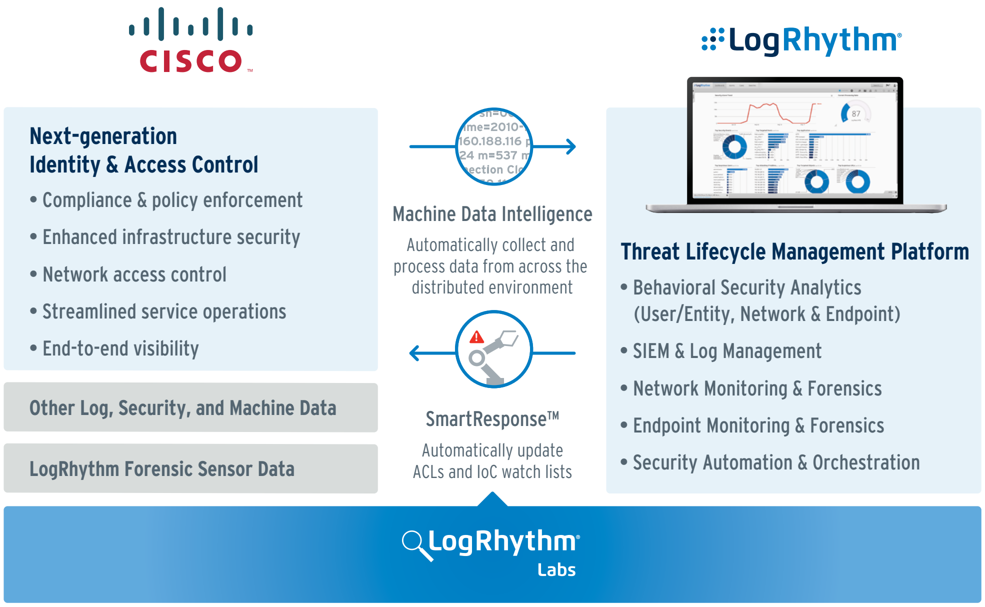
LogRhythm and Cisco Identity Services Engine (ISE): Integrated Enterprise Security

LogRhythm and Cisco have developed an integrated solution for comprehensive enterprise security intelligence and threat management. With an increasingly mobile workforce and the proliferation of Bring Your Own Device (BYOD), today's enterprises are significantly more vulnerable to attacks originating from endpoints within their own networks. Cisco Identity Services Engine (ISE) gives IT organizations the ability to monitor and control network access through identity and device-based policies applied across the infrastructure. By automatically incorporating identity and access control data from Cisco ISE, LogRhythm's advanced correlation and pattern recognition delivers real-time cyber threat protection and compliance enforcement based on up-to-date situational awareness and comprehensive security analytics.

LogRhythm and Cisco ISE allow users to monitor and secure the entire range of systems and applications across their organizations. The integration delivers:

- Deep visibility into the activities of guest accounts and devices, such as monitoring by device type (mobile, tablet, etc.), profile and posture, by integrating LogRhythm's correlation and forensic analysis capabilities with Cisco ISE's consolidated contextual information.
- Alerting and reporting on suspicious and/or unauthorized activity by integrating LogRhythm's automated behavioral analysis and correlation with Cisco ISE's endpoint profiling, posture assessment and contextual awareness.
- Continuous compliance that combines LogRhythm's extensive, out-of-the-box compliance packages with Cisco ISE's active endpoint user policy enforcement to automatically detect and respond when users or devices violate specific policies.


CISCO
Next-generation Identity & Access Control
• Compliance & policy enforcement
• Enhanced infrastructure security
• Network access control
• Streamlined service operations
• End-to-end visibility
Other Log, Security, and Machine Data
LogRhythm Forensic Sensor Data
Machine Data Intelligence
Automatically collect and process data from across the distributed environment
SmartResponse™
Automatically update ACLs and IoC watch lists
LogRhythm
Threat Lifecycle Management Platform
• Behavioral Security Analytics (User/Entity, Network & Endpoint)
• SIEM & Log Management
• Network Monitoring & Forensics
• Endpoint Monitoring & Forensics
• Security Automation & Orchestration
LogRhythm Labs

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 ISE

- Cisco Identity Services Engine (ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline service operations.
- It allows enterprises to gather real-time contextual information from multiple sources to make proactive decisions by enforcing policy across the network infrastructure - wired, wireless and remote.
- Cisco ISE is an integral component of the Cisco TrustSec® solution and uses Cisco Platform Exchange Grid (pxGrid) technology to share rich contextual data with integrated technology partner solutions.

LogRhythm and Cisco ISE are tightly integrated, combining the value of next-generation identity and access control with the threat management capabilities of LogRhythm. The combined offering empowers customers to detect internal and external threats, identify behavioral anomalies, enhance security, and enforce compliance.

LogRhythm for Integrated Enterprise Security Intelligence

- 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

Behavior Based Identity Management

Challenge:
Many organizations cannot distinguish between legitimate user behavior and suspicious activity because they can't correlate user profile data against actual user behavior. This leaves them vulnerable to threats such as compromised credentials and inappropriate user activity.

Solution:
LogRhythm can incorporate identity and access control data from Cisco ISE and correlate it against all other log and event data to create baselines for logical groupings (device type, auth group, etc.) for what should be considered "normal" behavior. This enables focused alerts regarding devices or users that ISE has prioritized as important or higher risk to identify suspicious activity or specific users engaged in behavior that violates policy.

Additional Benefit:
SmartResponse™ can initiate an automated response to any suspicious activity or behavior pattern by disabling the user's account until it can be validated. The quarantine action can be completely automated or subject to as many as three levels of authorization.

Enhanced Network Access Control

Challenge:
With the growing number of outside devices and potential access points in today's enterprise, access control is more difficult than ever before. Without the means to collect, correlate and analyze relevant data, bridging the gap between acceptable device behavior profiles and potentially suspicious activity can be almost impossible.

Solution:
LogRhythm's Advanced Intelligence (AI) Engine's multi-dimensional behavioral analysis modules automatically profile device behavior, creating whitelists of acceptable activity such as processes or services, network connections, etc. These behavioral whitelists can be correlated against device profiles within ISE to significantly enhance network visibility and rapidly identify suspicious and/or malicious activity.

Additional Benefit:
SmartResponse enforces continuous compliance and protects the network by dynamically adapting alarms, investigations and reports to stay up-to-date by automatically adding non-compliant or suspiciously behaving devices to a list and/or quarantining such devices.