LogRhythm and Webroot®: Integrated Security and Threat Intelligence

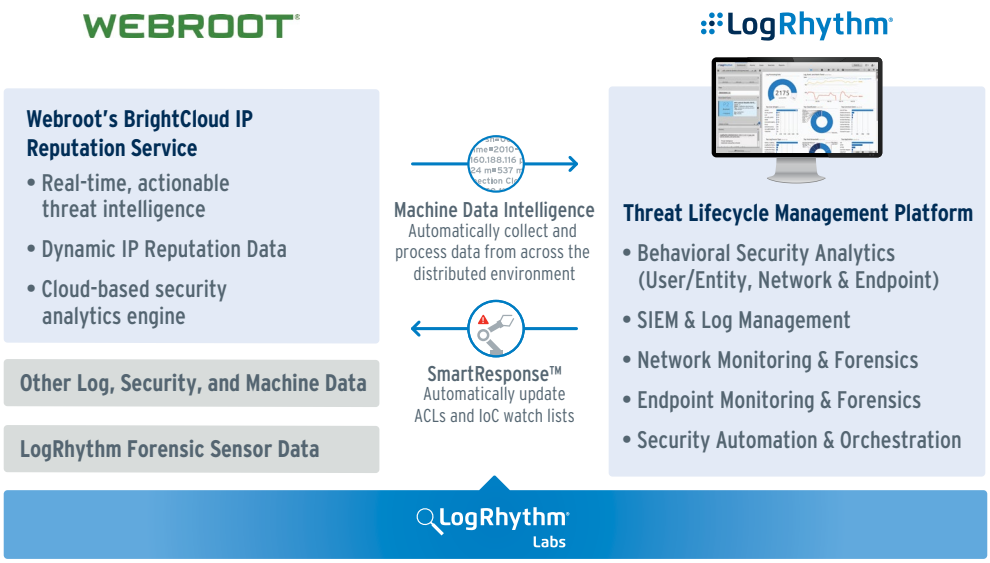
Combining actionable threat data with advanced behavioral analytics for enterprise security intelligence

LogRhythm and Webroot have developed an integrated solution for comprehensive security intelligence and threat management. LogRhythm automatically integrates actionable intelligence from the Webroot BrightCloud® IP Reputation Service with other machine data collected throughout the enterprise for comprehensive, real-time threat visibility and next generation security analytics.

The integration allows customers to:

- Continually import threat data from the Webroot BrightCloud IP Reputation Service into LogRhythm for immediate recognition of user, host, and network behavior involving malicious IP activity.
- Automate the corroboration of network activity to or from established bad IPs with other behavioral changes to hosts and users for more accurate prioritization of high risk events.
- Provide drill-down and deep forensic visibility into malicious IPs detected on the network.
- Automate the remediation of attacks by blocking communication with compromised domains to prevent data theft, block malware, and terminate APT communication with a command and control infrastructure.

By leveraging the Webroot BrightCloud IP Reputation Service with LogRhythm's Threat Lifecycle Management, customers benefit from increased threat intelligence and accurate risk management. The combined solution delivers the ability to rapidly detect, validate, and streamline incident response time to cyber-attacks.



About LogRhythm

- Empowers organizations to rapidly detect, respond to, and neutralize damaging cyberthreats by enabling Threat Lifecycle Management
- Unifies data lake technology, machine learning, security analytics, and security automation and orchestration in a single end-to-end solution
- Serves as the foundation for the artificial intelligence-enabled security operations center to secure customers' cloud, physical, and virtual infrastructures for both IT and OT environments
- Consistent market leadership including recognition as a Leader in Gartner's Magic Quadrant since 2012

About Webroot

- Webroot BrightCloud IP Reputation Service is a highly-accurate, real-time threat intelligence service that helps LogRhythm customers quickly identify malicious IPs in their network traffic.
- Once a threat is identified, the integrated solution provides deep visibility into network behavioral changes and malicious IPs, in addition to automating the remediation of attacks.
- This enables IT personnel to prioritize and remediate IP-related security incidents more quickly and limit the effects of potential breaches.
- This integrated solution now delivers LogRhythm customers the same threat intelligence that other security providers have licensed for their security solutions.

LogRhythm and Webroot are tightly integrated, combining the value of actionable threat intelligence with the threat management capabilities of LogRhythm's Threat Lifecycle Management Platform. The combined offering empowers customers to proactively defend against IP-related attacks and prioritize response efforts based on accurate, highly contextualized security intelligence.

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

Increasing Threat Intelligence

Challenge:
The immense number of exploits and attack vectors available to cybercriminals today – and the numerous communication techniques they use to mask their identities and activities – makes it difficult for information security professionals to know which incoming IP communication poses the greatest risk to their organizations.

Solution:
Webroot's BrightCloud IP Reputation Service delivers dynamic IP reputation scores on 4.3 billion IPs and identifies a list of the most dangerous (approximately 12 million). LogRhythm combines this data with advanced behavioral analytics for real-time threat intelligence with minimal false positives.

Additional Benefit:
SmartResponse™ Plug-ins are designed to actively defend against incoming IP attacks by initiating actions that offset the threat, such as automatically adding the attacking IPs to a firewall ACL. This immediately stops all activity to and from adversary groups to immediately halt an attack.

Preventing Data Breaches

Challenge:
Many organizations struggle with a lack of visibility into activity from their internal users. This includes communication with high-risk areas of the internet, such as IRC chat rooms and anonymous proxy networks (e.g. TOR). Administrators need to differentiate legitimate employee activity from suspicious employee activity.

Solution:
Webroot BrightCloud IP Reputation Service provides detailed threat data with a focus on malicious IPs, allowing organizations to better define their security policies. LogRhythm leverages this data for highly accurate threat detection, identifying users associated with suspicious botnet, proxy, and TOR communication.

Additional Benefit:
LogRhythm NetMon can automatically initiate a targeted packet capture of all outbound data being sent to a malicious IP for in-depth forensic analysis and deep understanding of the data being targeted by an attacker.

Webroot BrightCloud® IP Reputation Service can be purchased by going to [webroot.com/LogRhythm.](webroot.com/LogRhythm)