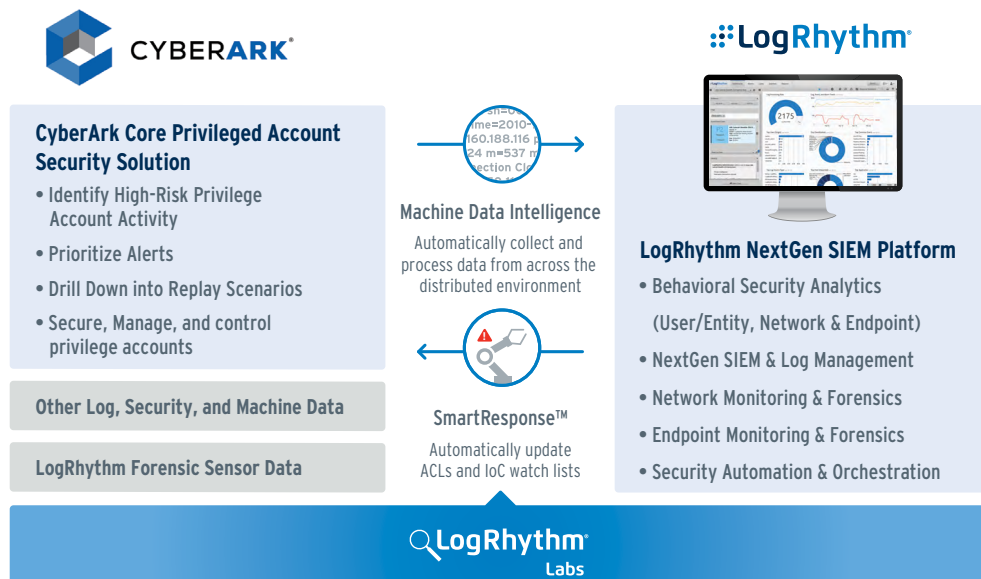


The LogRhythm and CyberArk partnership delivers a real-time privileged activity monitoring solution. By combining the CyberArk Privileged Account Security Solution with the LogRhythm NextGen SIEM platform, security analysts and audit teams can access the information they need to identify and respond to the most critical incidents – those involving privileged accounts – and meet demanding compliance requirements.

The integration allows users to:

- Link events triggered through privileged accounts with the individuals who initiated them; reveal who had access to which systems and data when and for what purpose
- Quickly investigate alerts by replaying exactly what transpired with video playback revealing the user’s actions. Compile all related forensic evidence to optimize response times
- Review command-level data sent to LogRhythm when anomalous activity is detected (e.g. credit card information is being copied); remotely locate and monitor the session in real-time via CyberArk Core Privileged Account Security; if required, automatically suspend or terminate sessions that contain high-risk events
- Monitor changes within the CyberArk Vault by sending activity logs to LogRhythm every time a privileged user accesses the vault to make changes (e.g. creates a new administrator account)
- Use LogRhythm’s out-of-the-box compliance reports to identify privileged users who access your most sensitive assets, modify configuration settings and run programs on the network

By integrating CyberArk’s Privileged Account Security Solution with LogRhythm’s NextGen SIEM platform, security teams are able to monitor and protect privileged activity and gain unified, real-time visibility across the organization to identify critical security threats. The solution generates exceptionally detailed forensic evidence, including tracking and reporting on all privileged activity, meeting audit and regulatory compliance requirements.



About LogRhythm

- Empowers organizations to rapidly detect, respond to, and neutralize damaging cyberthreats with 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



CYBERARK

About CyberArk

- CyberArk is the global leader in privileged account security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline
- CyberArk delivers the industry’s most complete solution to reduce risk created by privileged credentials and secrets
- The company is trusted by the world’s leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders
- CyberArk is headquartered in Petach Tikva, Israel, with offices throughout the Americas, EMEA, Asia Pacific, and Japan. To learn more about CyberArk, visit www.cyberark.com

LogRhythm and CyberArk are tightly integrated, combining the value of best-of-breed privilege account security solution with the threat management capabilities of LogRhythm's NextGen SIEM. For a comprehensive analysis of all system and user data presenting the highest level of risk, CyberArk provides a bidirectional data feed with the LogRhythm NextGen SIEM platform whereby privileged data and log files are jointly exchanged. The combined offering empowers customers to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise 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

Combined Data Sharing for End-to-End Threat Management

Challenge:

Organizations need the ability to correlate data from their disparate security products and services all while distinguishing real threats from false alarms.

Solution:

LogRhythm can incorporate the data from CyberArk Privilege Account Solution into automated advanced correlation rules. LogRhythm's correlation rules deliver highly focused alerts that identify when an organization is experiencing a privilege account incident or suspicious activity within their environment.

Additional Benefit:

SmartResponse™ plug-ins are designed to actively defend against attacks by initiating actions that can mitigate cyber threats. By reducing the time to perform common mitigation steps, SmartResponse helps prevent high-risk incidents from escalating.

Defend Against Insider Threats

Challenge:

Cyber attackers target privileged accounts in order to reach the heart of the enterprise and gain access to sensitive, valuable data. To protect these accounts and the critical resources to which they provide access, organizations require comprehensive controls to effectively monitor, detect, and respond to all privileged account activity in real-time.

Solution:

By integrating CyberArk's Privileged Account Security Solution with the LogRhythm NextGen SIEM platform, security teams can monitor and protect privileged activity and gain unified, real-time visibility across the organization to identify critical security threats. The solution generates exceptionally detailed forensic evidence, including tracking and reporting on all privileged activity, meeting audit and compliance requirements.

Additional Benefit:

If suspicious or malicious user activity occurs, LogRhythm SmartResponse can leverage the CyberArk Response Manager to modify the security policy of or disable a privileged account.