Exabeam and Wiz

Enhanced Cloud Security Through Comprehensive Threat Detection

Executive Summary of the Integration

The shift from on-premises to dynamic cloud applications, infrastructure, and collaboration creates a new set of security challenges for organizations. An estimated 40% of breaches result from data stored in multiple environments.[1] One of the biggest challenges is a lack of unified visibility across a broader attack surface, making it more difficult to identify threats.

The Exabeam New-Scale Security Operations Platform applies AI and automation to security operations workflows, combining security information and event management with behavior analytics for a holistic approach to threat detection, investigation, and response (TDIR). The integration with Wiz provides enhanced visibility across the cloud environment, consolidating data and improving situational awareness.

Market Challenge

Security monitoring sprawl represents a huge challenge for enterprise organizations, and recent surveys reveal enterprises are managing more than 50 security tools. As more organizations migrate to the cloud, securing cloud infrastructure becomes a high priority. Wiz data shows that 57% of organizations use more than one cloud.[2] Addressing security issues in these environments is more complex. The rapid expansion of cloud footprints and the rise of advanced threats targeting cloud assets exacerbate the challenge.

Comprehensive Threat Detection, Investigation, and Response for Cloud Environments

The AI-driven New-Scale Security Operations Platform from Exabeam combines security information and event management (SIEM), user and entity behavior analytics (UEBA), and analyst workflow automation to provide security operations center (SOC) teams with complete visibility into threats and streamlined security. The cloud-native platform enables rapid data ingestion, hyper-fast querying, and automated investigations so analysts can detect, investigate, and respond to threats faster and more accurately. Running on a cloud-native platform, New-Scale storage capabilities allow customers to store increasingly large volumes of data. This allows them to track mean time to respond (MTTR) and service-level agreements (SLAs) over time to maximize their impact to the business.

The integration with Wiz allows Exabeam customers to leverage Wiz's comprehensive cloud security insights. By ingesting Wiz's cloud security data, Exabeam delivers centralized visibility into security incidents across the threat plane, strengthening and streamlining threat detection, investigation, and response. SOC teams can improve the security and resiliency of their cloud environment and boost the overall security posture.

[1] Cost of a Data Breach Report 2024, IBM

[2] The State of the Cloud 2023, Wiz

Benefits of the Integration

- **Accelerate cloud threat detection** by consolidating security data and incidents across security tools and Wiz to automate detection.
- **Increase visibility into cloud security risks** by ingesting Wiz Issues into Exabeam to gain a comprehensive view of cloud infrastructure attack paths.
- **Simplify onboarding and management** with pre-built mappings from Wiz to Exabeam and by integrating Wiz into existing workflows with a preconfigured Wiz tile and webhook collectors.

Top Use Case

- **Situational awareness** - The ability to quickly understand an organization's current threat landscape, the associated risks, and the effectiveness of risk mitigation measures.
- **Challenge:** Without centralized visibility, security practitioners would have to pivot between multiple tools, Wiz, and Exabeam to identify cloud-security risks in their environments.
- **Solution:** Using the Exabeam/Wiz integration, analysts can ingest Wiz Issues into the Exabeam Cloud Security Platform to gain complete visibility from a single console and track progress of remediation over time.

Name of product to integrate with Wiz

Exabeam New-Scale Security Operations Platform

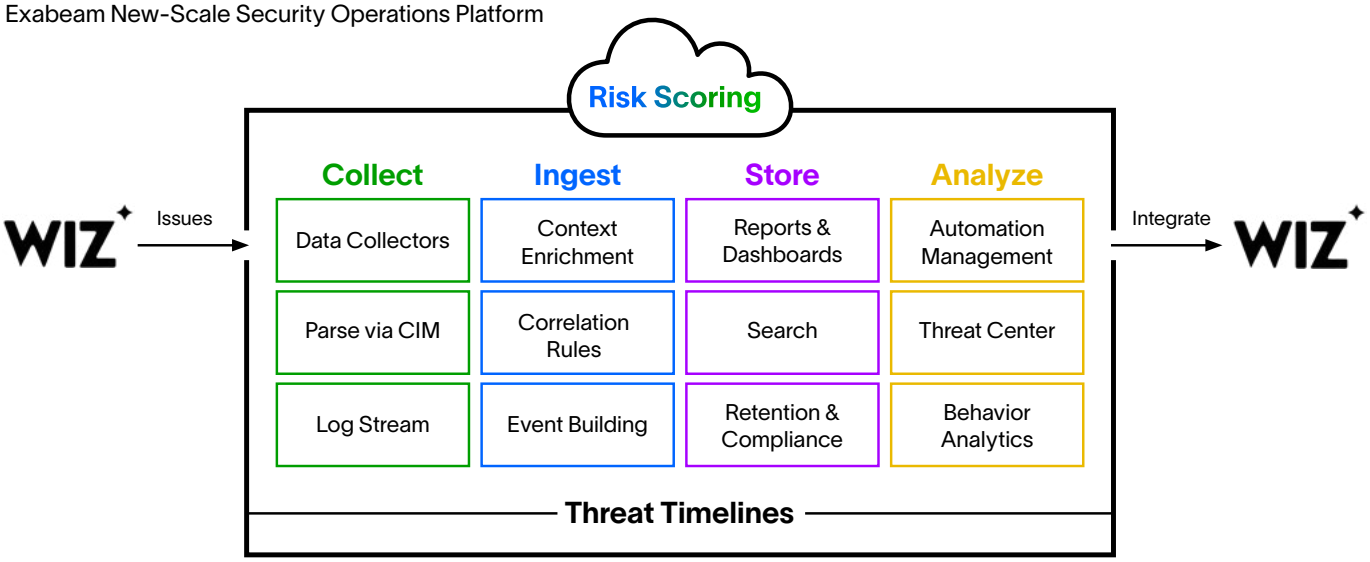

Figure 1. Wiz data is ingested into Exabeam and enriched with context for combined UEBA and correlation-based incident detection and prioritization. Automation Management allows custom notification and webhooks back into Wiz systems.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam

Learn more at
www.exabeam.com →