Exabeam and Centrify Partner to Improve Security by Providing Enhanced Visibility for Compromised Users and Hosts

Exabeam, the fastest growing next-gen security information and event management company, and Centrify, the leading provider of Zero Trust Security through the power of Next-Gen Access, have partnered to deliver a robust solution that secures enterprises against cyber threats that target today’s hybrid IT environment of cloud, mobile, and on-premises.

The combined Exabeam and Centrify solution helps security analysts by providing enhanced visibility for compromised users and hosts.

HOW THE EXABEAM AND CENTRIFY JOINT SOLUTION WORKS

INTEGRATION BENEFITS

- Enhanced visibility for compromised users and hosts
- Increased detection of credential-based attacks, insider threats, and lateral movement via data science and behavioral modeling
- Accelerated incident investigation and SOC automation using Exabeam’s user session timelines to triage security anomalies
HOW THE EXABEAM AND CENTRIFY JOINT SOLUTION WORKS (CONTINUED)

• The Exabeam Security Intelligence Platform ingests logs directly from Centrify Next-Gen Access infrastructure services via a Syslog feed.
• Exabeam parses, normalizes, and enriches the log data with context from the customer’s environment. Behavior modeling and analytics are used to baseline user behavior.
• Exabeam then analyzes the baseline user behavior to detect anomalous authentication activity. By leveraging Centrify event data, Exabeam Advanced Analytics is used to detect and alert on abnormal privilege escalation by monitoring process creation activity on the endpoint.
• Exabeam session-based processing engine stitches all user activity into a timeline. The risk engine then modifies risk scores that generate notifications when certain thresholds are exceeded.

CHALLENGE

In today’s threat landscape, credential-based attacks involving compromised or malicious insiders are more common than ever. Such attacks are notoriously difficult to detect. They can evade perimeter defenses by using legitimate credentials to impersonate employees, escalate privileges, and—in some cases—create highly privileged, phantom user accounts to access valuable business data.

SOLUTION

The joint Exabeam and Centrify solution enables security teams to monitor and protect organizations against credential-based threats, in addition to critical security threats arising from privileged users.

Exabeam’s Security Intelligence Platform connects identity information from Centrify’s Next-Gen Access with other user activity data. It helps accurately assess risk, identify threats, and reconstruct incident timelines regarding anomalous, privileged escalation threats. And pre-built incident timelines help analysts quickly understand the scope and nature of detected attacks by automating what was previously a manual investigation process.

ABOUT CENTRIFY

Centrify delivers Zero Trust Security through the power of Next-Gen Access. The Centrify Zero Trust Security model assumes that users inside a network are no more trustworthy than those outside the network. Centrify verifies every user, validates their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience. Centrify’s Next-Gen Access is the only industry-recognized solution that uniquely converges Identity-as-a-Service (IDaaS), enterprise mobility management (EMM) and privileged access management (PAM). Over 5,000 worldwide organizations, including over half the Fortune 100, trust Centrify to proactively secure their businesses.

Centrify is a registered trademark of Centrify Corporation in the United States and other countries. All other trademarks are the property of their respective owners.

ABOUT EXABEAM

Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information. The Exabeam Security Intelligence Platform uniquely combines a data lake for unlimited data collection at a predictable price, machine learning for advanced analytics, and automated incident response into an integrated set of products. The result is the first modern security intelligence solution that delivers where legacy security information and event management (SIEM) vendors have failed. Built by seasoned security and enterprise IT veterans from Imperva, ArcSight, and Sumo Logic, Exabeam is headquartered in San Mateo, California. Exabeam is privately funded by Lightspeed Venture Partners, Cisco Investments, Norwest Venture Partners, Aspect Ventures, Icon Ventures, and investor Shlomo Kramer.

For more information, please contact Exabeam at info@exabeam.com