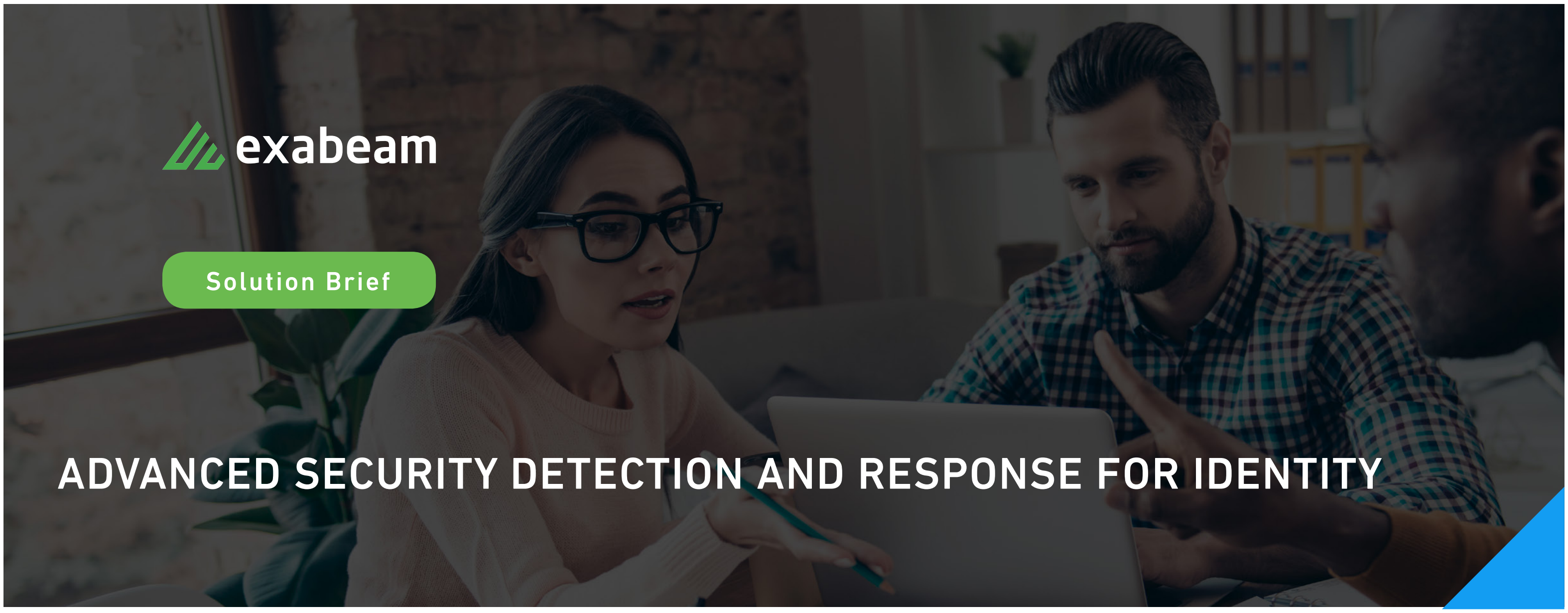


exabeam

Solution Brief

# ADVANCED SECURITY DETECTION AND RESPONSE FOR IDENTITY

DUO

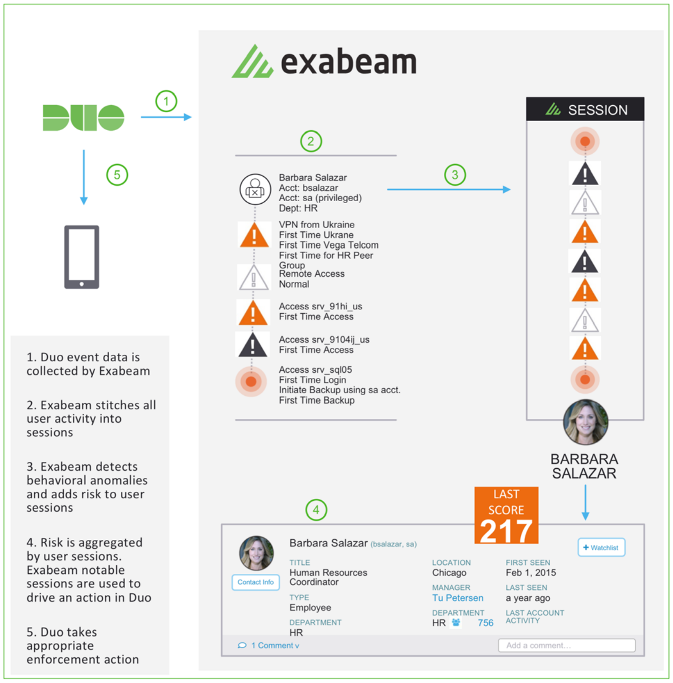
## INTEGRATION BENEFITS

- Provides complete visibility into your users' authentication activity
- Automatically identifies and detects security attacks, such as suspicious authentication attempts and credential compromise
- Supports zero-trust principles by invoking continous, strong user authentication and device verification
- Takes proactive action for risky behavior and requires high-risk users to perform step-up authentication
- Increases operational efficiency by providing higher accuracy alerts for security analysts, helping save time and resources

According to the 2018 Verizon Data Breach Investigations Report, stolen credentials continue to top the list of causes for data breaches. Many organizations still focus on securing their network perimeter instead of how they secure their extended enterprises. By adopting a zero-trust security model, organizations can better position themselves to respond to credential-based attacks by shifting their focus from protecting legacy single, large perimeters to protecting every user and device within the organization.

Exabeam, the fastest growing next-gen security information and event management company, and Duo, the leading provider of Unified Access Security (UAS) and multi-factor authentication, have partnered to deliver a robust identity monitoring solution that enables organizations to detect, investigate, and respond to security threats in real-time. The combined Exabeam and Duo solution help security analysts to proactively detect security threats before they become critical and help automate the investigation process, saving them time and critical resources.

## HOW THE EXABEAM AND DUO JOINT SOLUTION WORKS



Barbara Salazar
Acct: bsalazar
Acct: sa (privileged)
Dept: HR

VPN from Ukraine
First Time Ukrane
First Time Vega Telcom
First Time for HR Peer Group
Remote Access
Normal

Access srv_91hi_us
First Time Access

Access srv_9104ij_us
First Time Access

Access srv_sql05
First Time Login
Initiate Backup using sa acct.
First Time Backup

Barbara Salazar (bsalazar, sa)

TITLE: Human Resources Coordinator
TYPE: Employee
DEPARTMENT: HR
LOCATION: Chicago
MANAGER: Tu Petersen
DEPARTMENT: HR 756
FIRST SEEN: Feb 1, 2015
LAST SEEN: a year ago
LAST ACCOUNT ACTIVITY

1. Duo event data is collected by Exabeam

2. Exabeam stitches all user activity into sessions

3. Exabeam detects behavioral anomalies and adds risk to user sessions

4. Risk is aggregated by user sessions. Exabeam notable sessions are used to drive an action in Duo

5. Duo takes appropriate enforcement action

## HOW THE EXABEAM AND DUO JOINT SOLUTION WORKS (CONTINUED)

- The Exabeam Security Intelligence Platform  ingests rich identity context and authentication data via Duo's logs API. Exabeam parses, normalizes, and enriches the log data with context from the customer's environment. Behavior modeling and analytics are used to baseline credential usage.
- Exabeam then analyzes the baseline user behavior to detect suspicious log on/log off and account management behavior.
- 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. If a threshold is exceeded, Exabeam initiates a response by prompting for Duo Adaptive Multi-Factor Authentication to verify the user.
- If the user approves, the incident is closed. If the user doesn't approve or doesn't respond, Exabeam takes containment actions against the user through Duo to disable that user account, reduce their access, add them to a watch list, revoke credentials, and/or send an email to the SOC team.

## CHALLENGE

Most of the biggest data breaches—judged either by number of records breached or the importance of stolen data—have involved attackers leveraging stolen user credentials to gain access. However, many organizations continue to struggle with similar credential-based threats. This is largely because they still focus on securing their network perimeter instead of closing the gap between identity management and security controls. To protect organizations against credential-based threats and sensitive data exfiltration, they require effective, real-time prevention, detection, and response for all suspicious account activity.

## SOLUTION

The joint Exabeam–Duo solution enables security teams to monitor and protect enterprises against credential-based threats. Exabeam Security Intelligence Platform ingests Duo logs via API integration. Exabeam then analyzes that information and adds meaningful context to detect suspicious login activities—including logins from unusual locations, credential sharing, and account compromise. You can then take immediate action and require high-risk users to perform step-up authentication or containment actions like disabling the user account, reducing their access, or deny authentication attempts.

## 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 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 Norwest Venture Partners, Aspect Ventures, Icon Ventures, Lightspeed Venture Partners, and investor Shlomo Kramer. Follow us on Facebook, Twitter, and LinkedIn.

## ABOUT DUO SECURITY

Duo Security is the leading provider of Unified Access Security (UAS) and multi-factor authentication. Duo Beyond, the company's category defining zero-trust security platform, enables organizations to provide trusted access to all of their critical applications, for any user, from anywhere, and with any device. The company is a trusted partner to more than 12,000 customers globally, including Dresser-Rand, Etsy, Facebook, Paramount Pictures, Random House, Zillow and more. Founded in Michigan, Duo has offices in Ann Arbor and Detroit, as well as growing hubs in Austin, Texas; San Mateo, California; and London, UK. Visit Duo.com to find out more.