Securing Privileged Activity in the Age of AI

Modern Defense for Privileged Accounts and Autonomous Agents

Why Privileged Accounts Are Still a Prime Target

Privileged accounts—administrators, executives, and service accounts—control access to critical systems and sensitive data. Attackers know this. A single compromised privileged account can lead to large-scale data exfiltration, operational disruption, or stealth persistence.

The risk is growing. According to the Ponemon Institute, insider threats now cost organizations $17.4 million annually, with 45% of breaches involving insider misuse or negligence. Each incident averages $2.7 million, and most organizations still take weeks to detect these threats.

The New Challenge: AI and Autonomous Agents

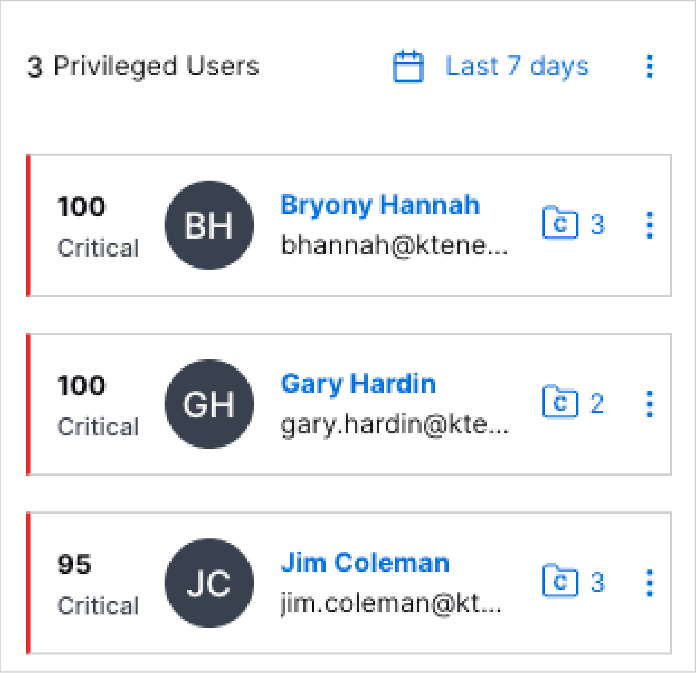
AI-driven tools and autonomous agents often operate with elevated privileges. If compromised or misused, they can become powerful attack vectors. Without visibility into agent behavior, security teams lack the context needed to detect privilege abuse and emerging threats.

The Exabeam Advantage: Behavioral Analytics for Humans and AI

Exabeam extends traditional user and entity behavior analytics (UEBA) with Agent Behavior Analytics (ABA), giving security operations teams the ability to:

- **Monitor AI-driven processes and agents** for abnormal activity, ensuring they don't become insider threats.
- **Detect privilege escalation and misuse** across humans and machines.
- **Prevent AI misuse** by enforcing behavioral guardrails and monitoring sensitive data access.

Exabeam combines behavioral analytics, automated investigations, and risk scoring to help security teams detect threats others miss.



3 Privileged Users | Last 7 days

100 Critical	BH	Bryony Hannah bhannah@ktene...	3
100 Critical	GH	Gary Hardin gary.hardin@kte...	2
95 Critical	JC	Jim Coleman jim.coleman@kt...	3

Figure 1.

Threat Center provides a watchlist for privileged users and entities, making it easy monitor threat escalation of business critical assets.

How Exabeam Secures Privileged Activity

Exabeam delivers end-to-end coverage for privileged activity threats with agentic automation, behavioral analytics, and prebuilt content.

Detect Anomalous Privileged Behavior

Exabeam automatically identifies privileged accounts and assets from directory services and privileged access management (PAM) systems. It establishes baselines for normal activity and flags anomalies using detection models mapped to MITRE ATT&CK® techniques such as T1078: Valid Accounts and T1003: Credential Dumping. Suspicious activity is scored and prioritized so analysts can focus on the riskiest incidents.

Investigate With Context and Speed

Automated timelines tell the full story of user, asset, and agent activity—normal and abnormal—into a clear, chronological view. Analysts no longer need to write queries to understand historical behavior. The combination of automation and context accelerates investigations and reduces mean time to respond (MTTR).

Key Capabilities

Challenge 1: Detect Privileged and AI-Driven Threats

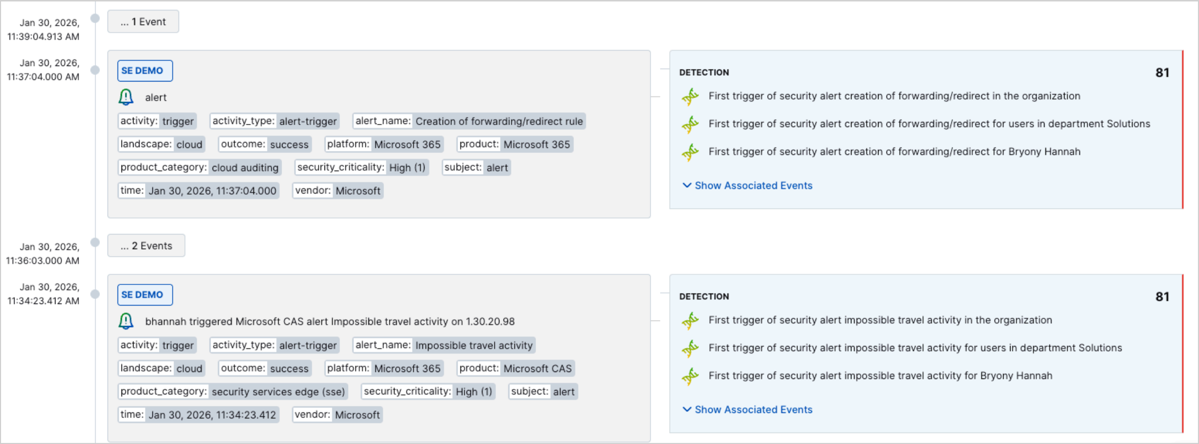
Traditional tools struggle to identify privileged accounts and assets, making it difficult to detect attacks involving privilege misuse or AI-driven processes.

Solution

Exabeam ingests context from directory services and PAM systems to classify privileged accounts such as domain controllers, administrators, and executives. UEBA establishes baselines for normal activity across users and assets, while ABA monitors agents for suspicious or unexpected actions. Anomalies are flagged using detection models mapped to the ATT&CK framework, scored for risk, and prioritized for investigation.

Benefit

Detect privilege misuse and monitor AI-driven processes to reduce insider risk and investigation time.



Jan 30, 2026,
11:39:04.913 AM

... 1 Event

Jan 30, 2026,
11:37:04.000 AM

SE DEMO

alert

activity: trigger | activity_type: alert-trigger | alert_name: Creation of forwarding/redirect rule
landscape: cloud | outcome: success | platform: Microsoft 365 | product: Microsoft 365
product_category: cloud auditing | security_criticality: High (1) | subject: alert
time: Jan 30, 2026, 11:37:04.000 | vendor: Microsoft

DETECTION 81

First trigger of security alert creation of forwarding/redirect in the organization

First trigger of security alert creation of forwarding/redirect for users in department Solutions

First trigger of security alert creation of forwarding/redirect for Bryony Hannah

Show Associated Events

Jan 30, 2026,
11:36:03.000 AM

... 2 Events

Jan 30, 2026,
11:34:23.412 AM

SE DEMO

bhannah triggered Microsoft CAS alert Impossible travel activity on 1.30.20.98

activity: trigger | activity_type: alert-trigger | alert_name: Impossible travel activity
landscape: cloud | outcome: success | platform: Microsoft 365 | product: Microsoft CAS
product_category: security services edge (sse) | security_criticality: High (1) | subject: alert
time: Jan 30, 2026, 11:34:23.412 | vendor: Microsoft

DETECTION 81

First trigger of security alert impossible travel activity in the organization

First trigger of security alert impossible travel activity for users in department Solutions

First trigger of security alert impossible travel activity for Bryony Hannah

Show Associated Events

Figure 2.

This Threat Timeline shows compromised insider bhannah accessing a new departmental server for the first time.

Challenge 2: Gain Continuous Visibility and Accelerate Investigations

Security teams often lack visibility into privileged activity and cannot continuously monitor privileged users, assets, and agents for suspicious behavior.

Solution

Exabeam provides complete visibility by automatically aggregating security alerts and events into timelines, without requiring analysts to write queries. Watchlists centralize privileged accounts, assets, and agents for continuous monitoring. Analysts can quickly investigate anomalies using guided checklists and behavior-based threat hunting tools.

Benefit

Accelerate investigations and reduce MTTR from days to hours.

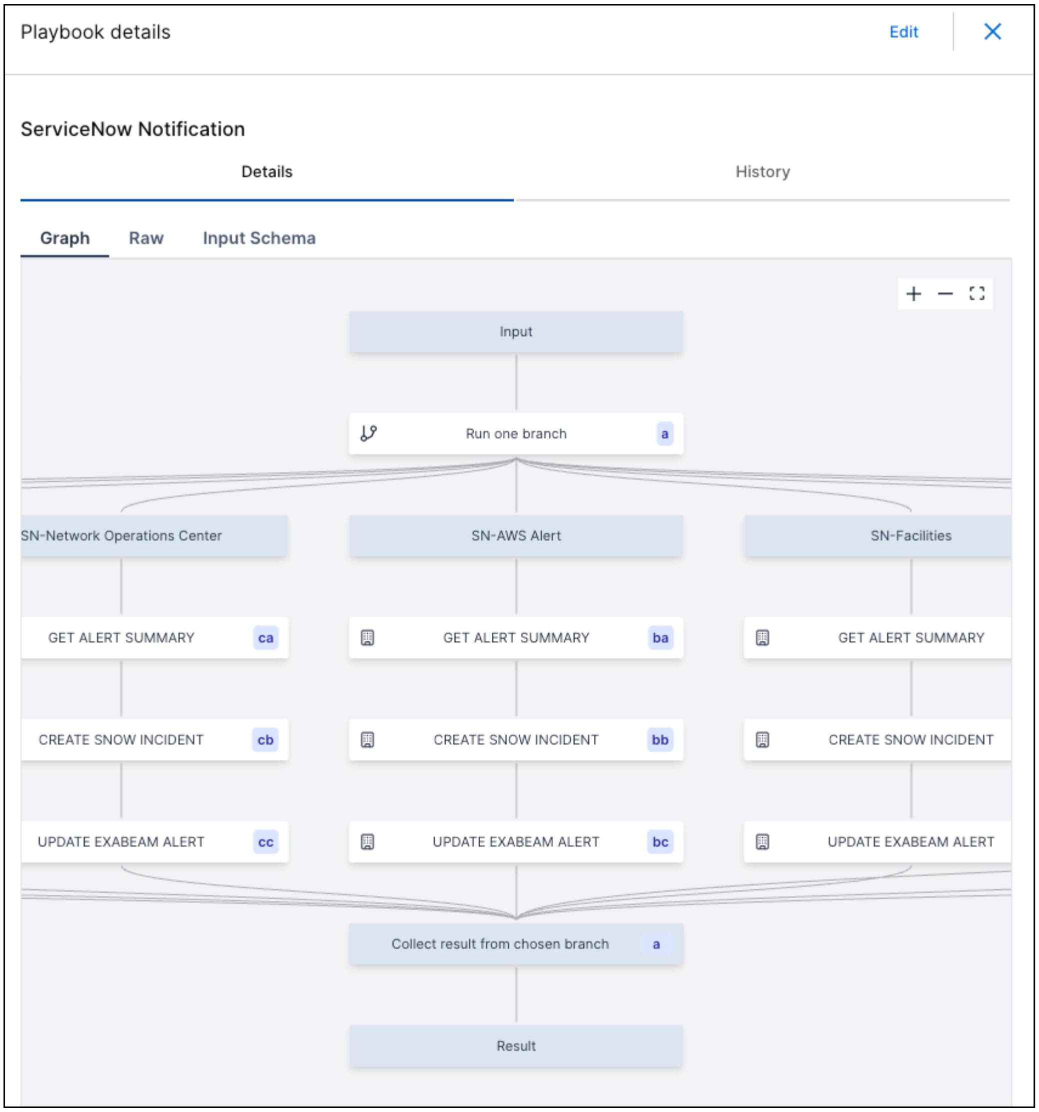


Figure 3.

This privileged activity playbook automates response actions through ServiceNow.

Challenge 3: Respond Quickly and Consistently

Coordinating response actions across multiple tools can take hours or days, leaving organizations exposed to ongoing risk.

Solution

Exabeam orchestrates response to privileged activity incidents across your security stack using security orchestration, automation, and response (SOAR) playbooks. Integrations with hundreds of security and IT products enable automated actions such as suspending accounts or agents, resetting credentials, and enforcing MFA.

Benefit

Improve operational efficiency and reduce MTTR with automated workflows that contain threats before they escalate.

Use Case Content

To provide coverage for privileged activity, Exabeam has identified key data sources and built content for collection, detection, investigation and response.

Key Data Sources

- Asset logon and access
- Authentication and access management
- VPN and zero trust network access
- Application activity
- Privileged access management and activity
- File monitoring
- Remote logon activity
- DLP alerts
- Web activity

Key Detection Rule Types

- Abnormal activity on domain controllers
- Executive account activity
- Privileged account activity
- Disabled account activity
- Privileged asset activity
- Privileged process execution

MITRE Technique & Tactic Coverage

- T1078: Valid Accounts
- T1059: Command and Scripting Interpreter
- T1204: User Execution
- T1003: OS Credential Dumping

Response Actions

- Contact user/manager/HR department via email
- Add user or asset to a watchlist
- Block, suspend, or impose restrictions on users involved in the incident
- Rotate credentials/expire/reset password
- Prompt for reauthentication via MFA
- Remove user from group
- Clear user session
- Get asset/user/process info
- Kill process

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam™

Learn more at
www.exabeam.com →