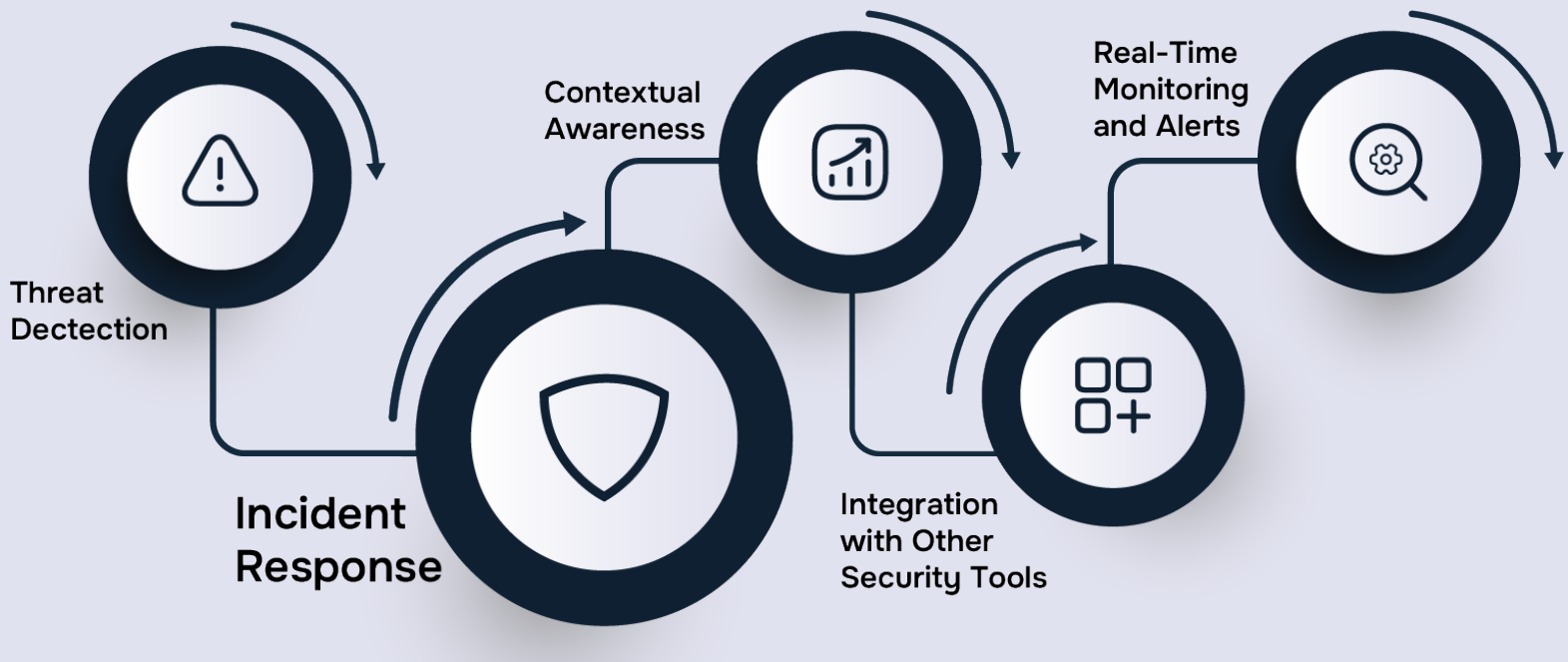
SaaS Incident Response Guide

Dynamic Defense for Your Ecosystem

82% of cyberattacks target identities within SaaS applications. But you can take steps today to protect your expanding SaaS universe.

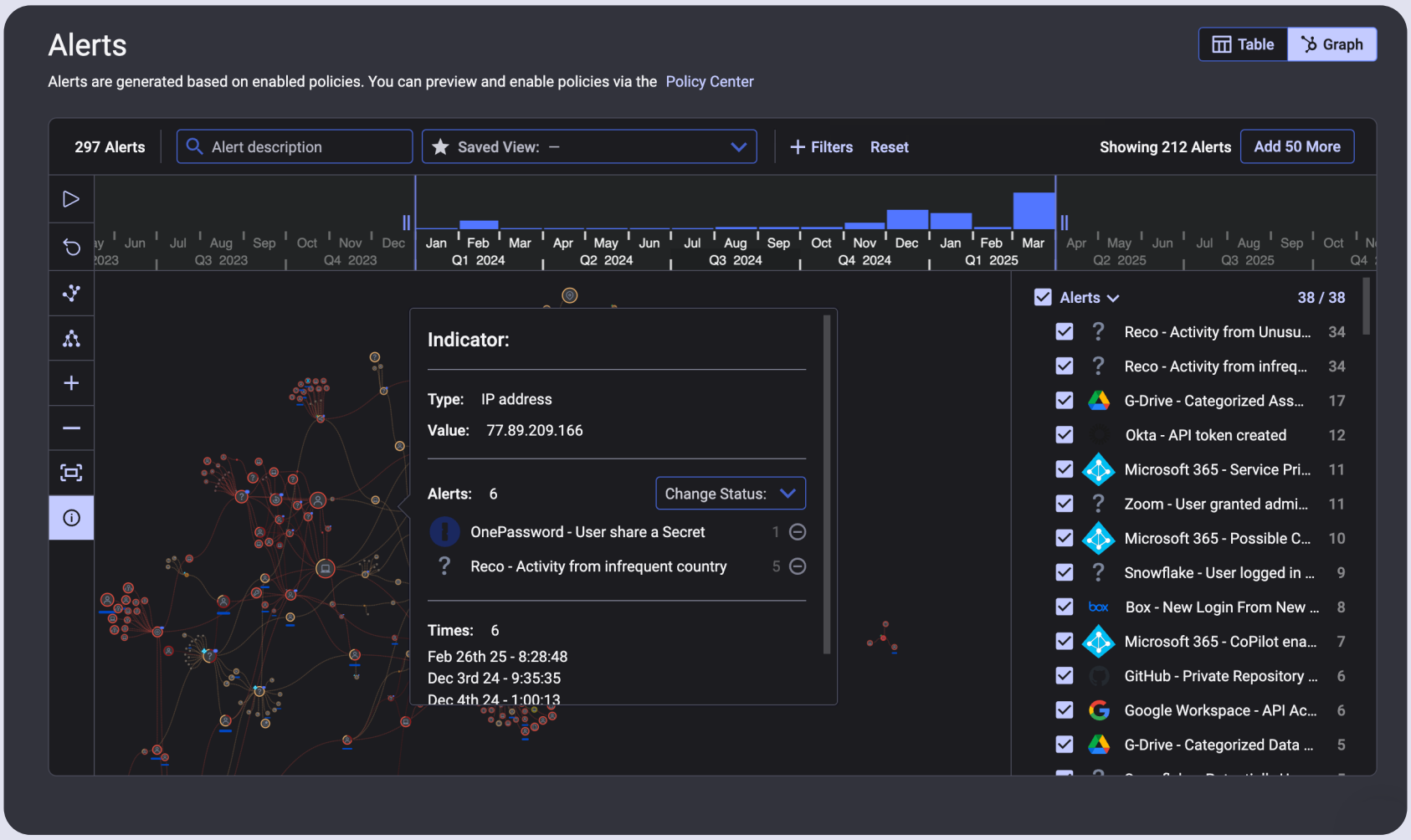


How Reco Closes the Gap Created by Event Sprawl

Dynamic SaaS Security with Knowledge Graph Intelligence

The Reco Knowledge Graph provides unmatched contextual awareness across the entire SaaS ecosystem, mapping all connections, users, and data flows in real time. Our graph-based approach rapidly identifies attack paths and provides comprehensive visibility that traditional SIEM/SOAR solutions miss.

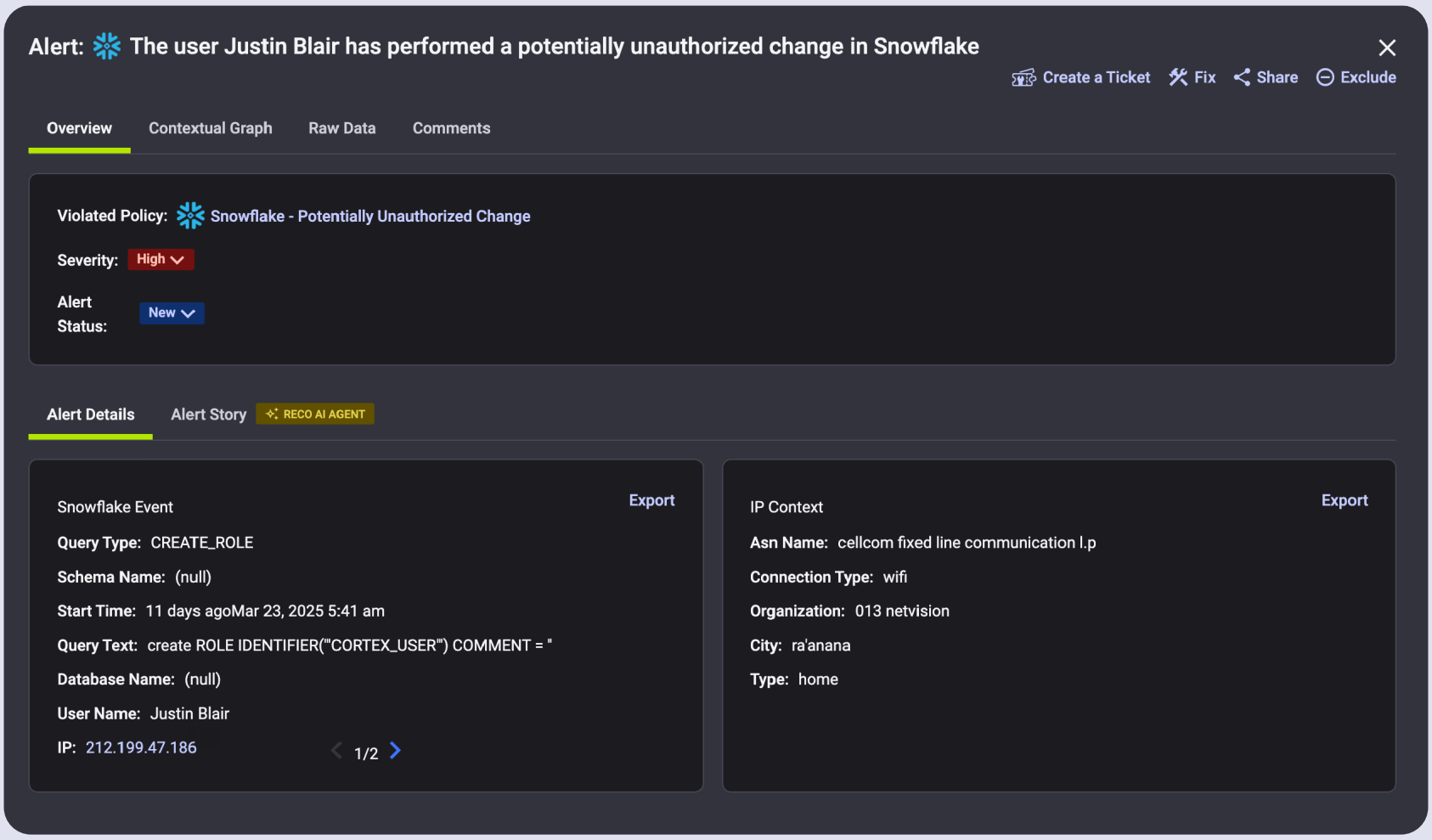
Customer Use Case: One customer is seeing 50% fewer security incidents. That's because of the context Reco provides that filters out noisy alerts and our proactive posture management that keeps risks to a minimum. That means tighter security and more focus on tasks that matter.



AI Agent-Driven Response Orchestration

Reco AI Agents—such as the Alerts Agent, Identities Agent, and Impossible Travel Agent provide immediate, actionable intelligence with detailed remediation steps. These agents reduce the Mean Time to Respond by automating the analysis and providing clear, contextual insights that eliminate manual investigation.

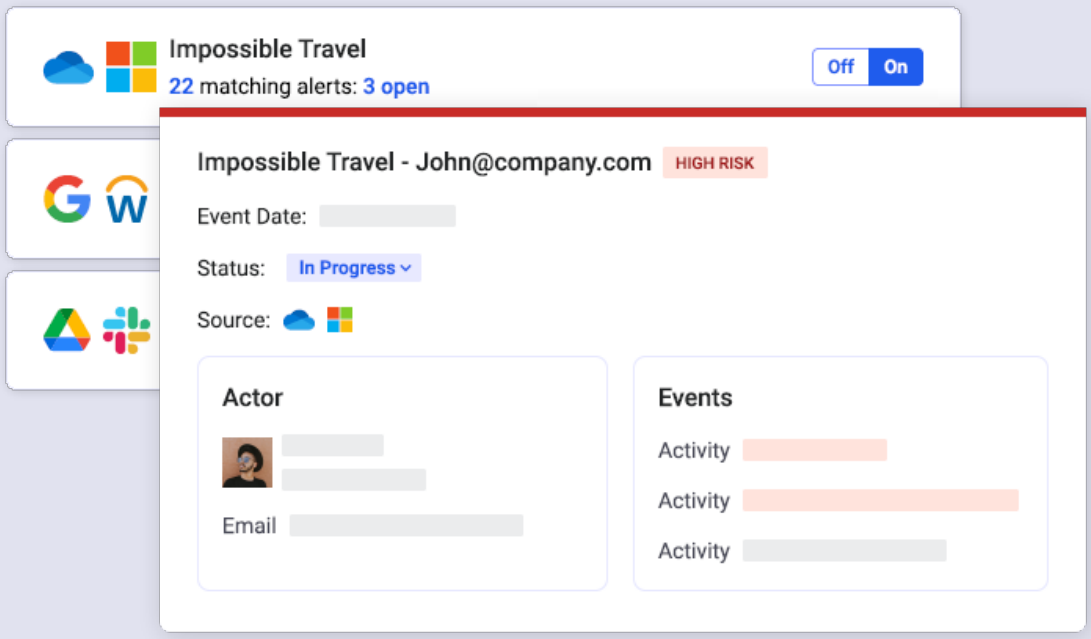
Customer Use Case: Reco AI Agents helped Watco, a leader in transportation save seven mins on average when responding to an alert.



Cross-Application Identity Threat Detection

Reco detects sophisticated identity-based attacks that traditional perimeter or single-application focused tools miss, including threats that move laterally across multiple SaaS apps.

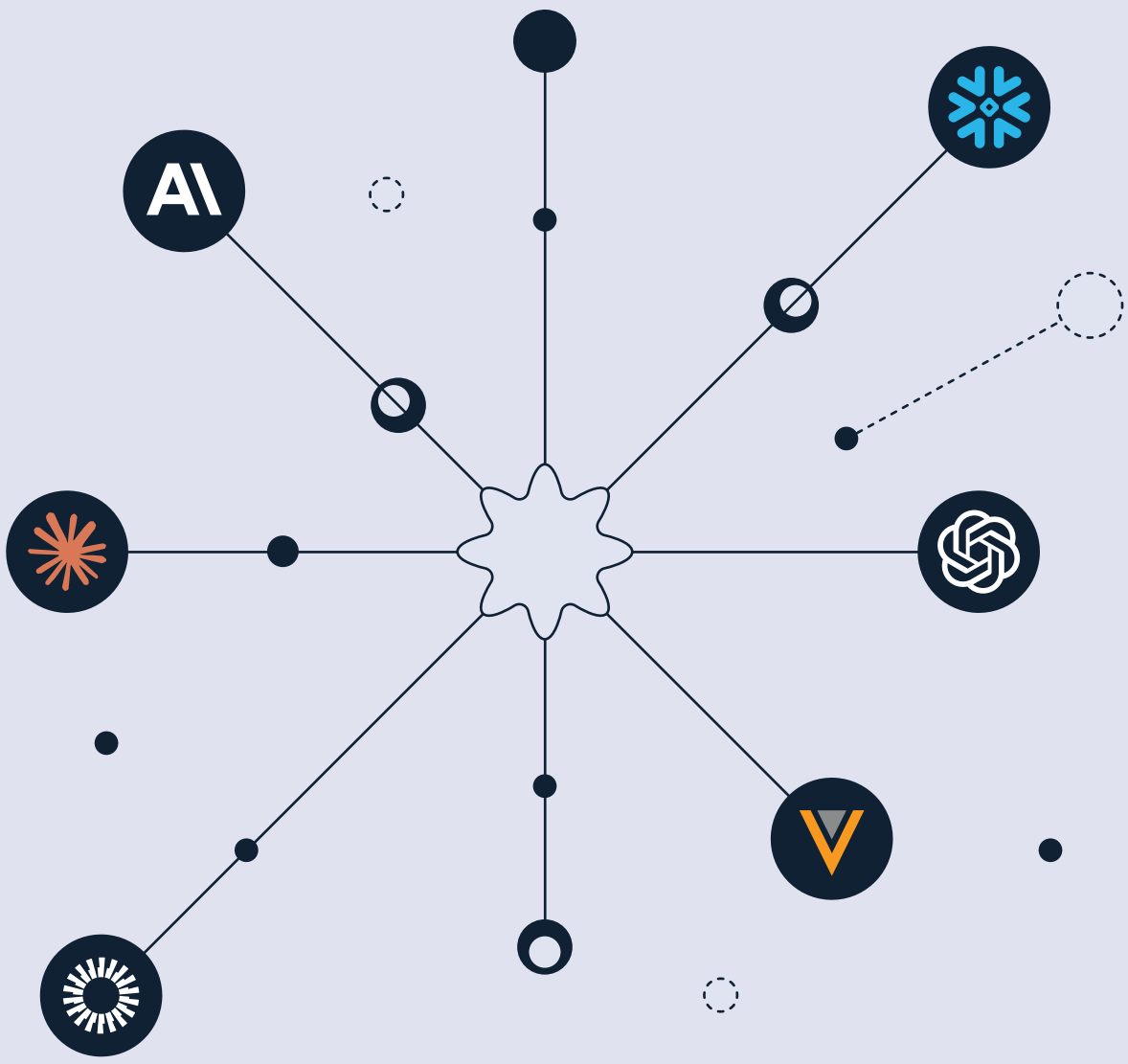
Customer Use Case: Reco helped another customer spot potential insider threats that would otherwise remain hidden in the noise. Reco flags when an employee shares a file with their personal email. This complete context flows directly to a SIEM, enabling the SOC team to make informed decisions and respond appropriately.



Reco Continuously Monitors for Potential Data Exposure

- **90% reduction in SOC team alert triage time** through contextual awareness and AI-driven insights.
- **Support for new apps in days, not quarters** from our SaaS App Factory™. This prevents a requirement to learn new events, messages and index them in your SIEM/SOAR.
- **Detection of identity threats in minutes** vs. industry average of 250+ days.
- **Comprehensive coverage across the five types of SaaS Sprawl**—App, AI, Configuration, Identity, and Data.

The Reco Advantage—Continuous Context with the Knowledge Graph



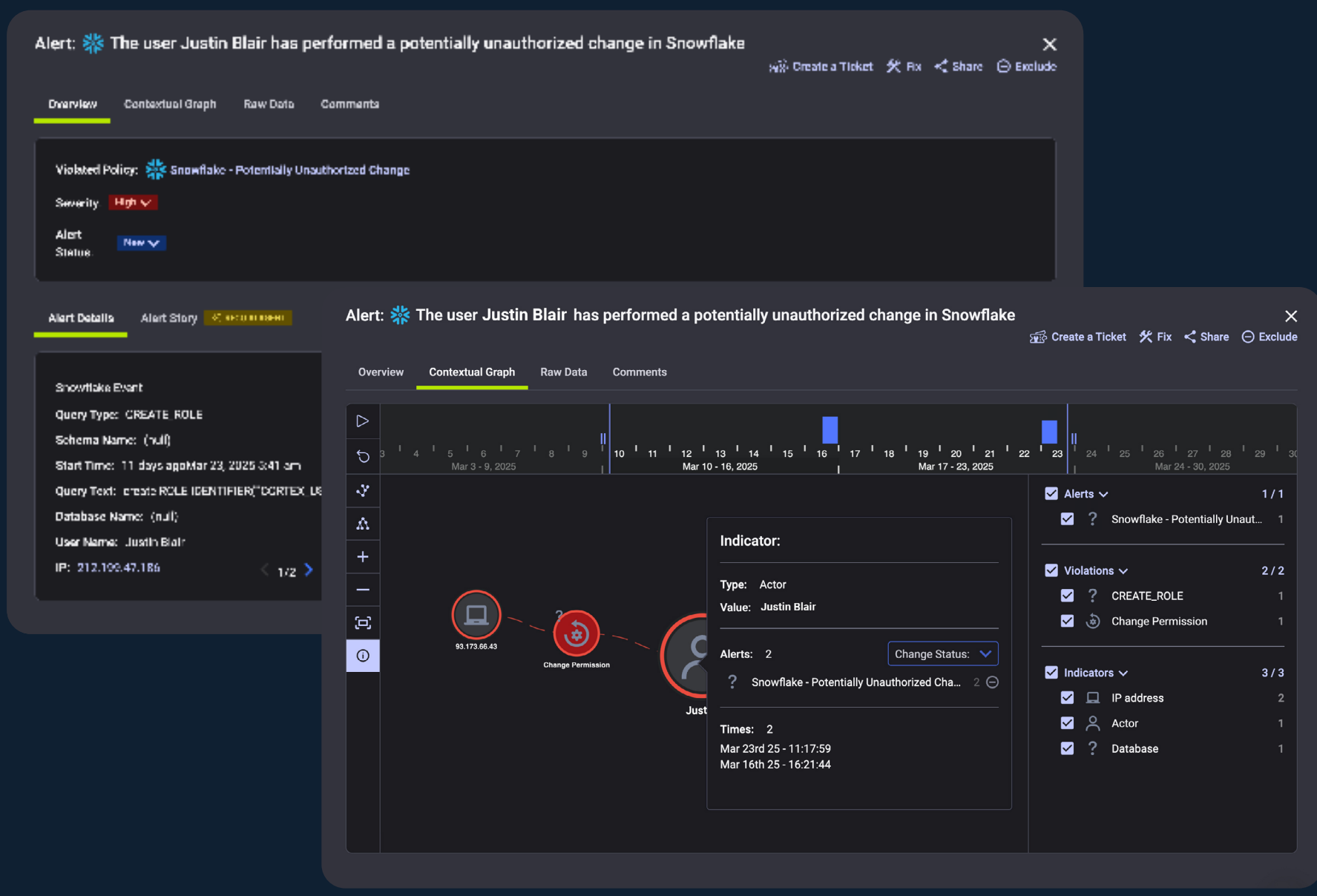
Reco's proprietary Knowledge Graph provides unprecedented contextual awareness across your entire SaaS ecosystem. Supercharged by our SaaS App Factory, it processes limitless SaaS data in real time, mapping risk across every app, user, and connection—no noise, just accuracy.

- **Complete visibility** across all sanctioned and shadow SaaS applications.
- **Identity consolidation** across multiple platforms to provide a unified risk view.
- **Behavioral baselines** established automatically for users, groups, and applications.
- **Business context enrichment** that prioritizes alerts based on data sensitivity and business impact.
- **Real-time mapping** of all SaaS-to-SaaS connections and potential attack paths.

AI Agents Derived from the Graph

Our specialized AI agents leverage the Knowledge Graph to provide unmatched threat detection and response through context-rich alerts with risk insights, AI-driven prioritization, and streamlined investigations. View in Reco, share via Slack or email for faster response.

- **Impossible Travel Agent:**
  - Alert: Same user logged in from Tokyo and New York within 2 hours.
- **Former with Access Agent:**
  - Alert: Ex-employee still has active admin privileges to financial systems.
- **Alerts Agent:**
  - Alert: High-risk configuration drift detected in 3 critical applications with detailed remediation steps.
- **Identity Risk Assessment Agent:**
  - Alert: User has excessive privileges across 7 applications with access to sensitive data.
- **Local Account Detection Agent:**
  - Alert: 12 local admin accounts created outside of centralized identity management.



Powerful Checks, Real-World Protection

Reco's targeted security posture checks directly align with breach-prevention best practices:

Lock Sessions to IP: Prevent unauthorized access from unknown IP addresses, a vulnerability exploited in breaches affecting major organizations.

Identity Verification on Email Changes: Safeguard accounts from unauthorized takeover attempts, protecting sensitive customer and internal data.

MFA Enforcement for Admins and Users: Block credential-based attacks that compromised Colonial Pipeline and similar organizations by ensuring strong authentication.

Email Authentication (SPF & DMARC): Protect your domain from spoofing and phishing attacks, similar to incidents affecting organizations like Marriott.

Legacy Authentication Blocking: Defend against attacks targeting legacy protocols, such as those exploited in the 2020 Microsoft Exchange breaches.

Conditional Access for Admin Portal: Prevent privilege escalation attacks, reducing risks like those encountered by Uber.

Secure External Storage Integrations: Mitigate data exfiltration risks similar to the Capital One breach by enforcing secure storage practices.

Maximize Failed Login Unlock Timeout: Reduce risks of brute-force attacks by enforcing proper timeout restrictions.

Certificate-Based Authentication Enforcement: Strengthen identity verification and reduce unauthorized access through enforced certificate-based authentication.

Restrict OAuth Parameters: Prevent unauthorized API usage and mitigate security breaches related to improper OAuth handling.

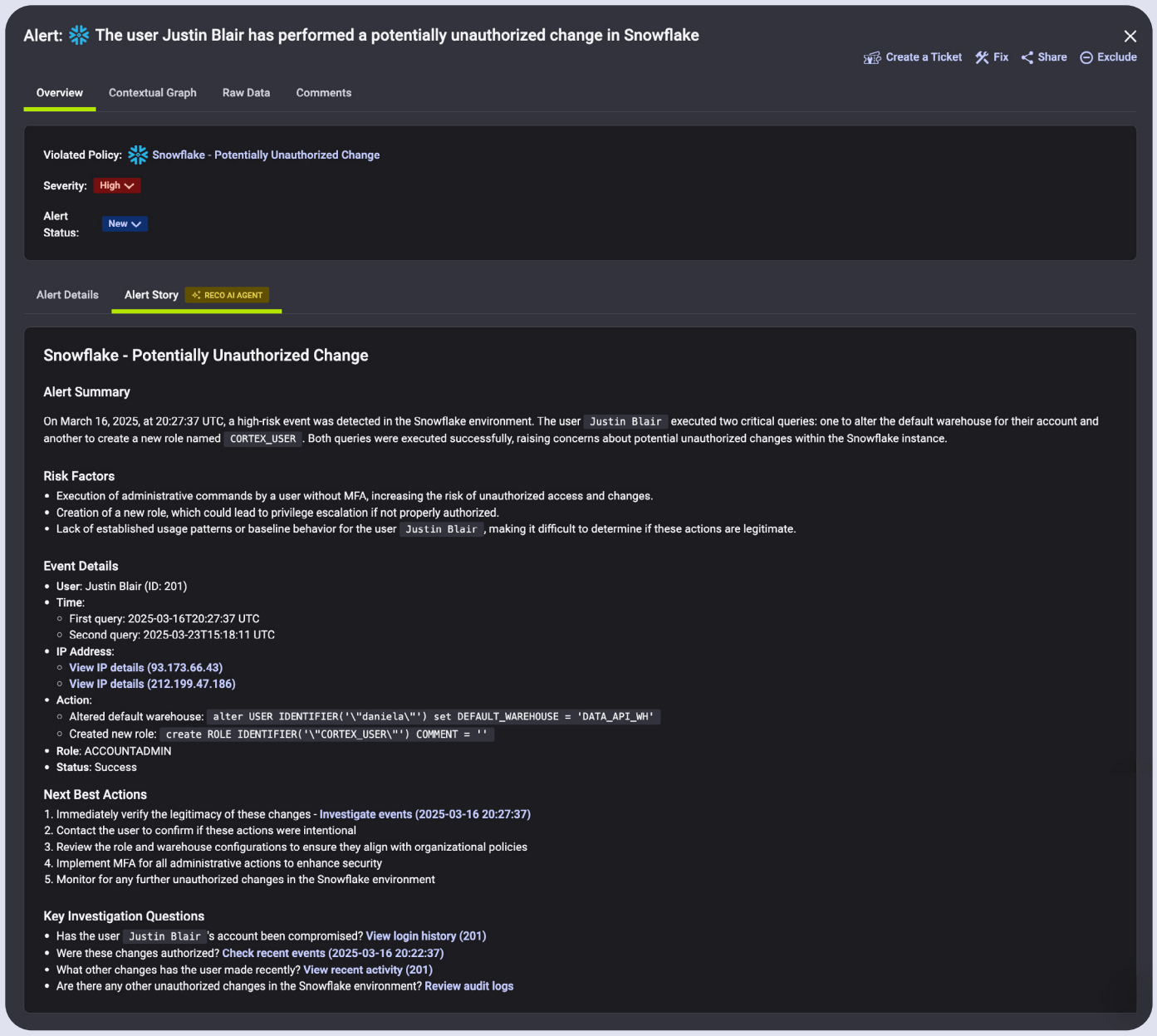
Cut Risk, Boost Efficiency

Detect Threats in Minutes, Not Months

Reco delivers comprehensive threat detection with **200+** out-of-the-box detection rules mapped to the MITRE ATT&CK framework, ensuring you're protected against known attack vectors from day one. Our ML-powered anomaly detection identifies behavioral deviations without requiring manual rule creation, catching threats that traditional solutions miss. With cross-application correlation, we detect complex attack patterns spanning multiple SaaS environments, giving you visibility into sophisticated threats that would otherwise go unnoticed. Automated threat hunting continuously scans for indicators of compromise specific to SaaS, proactively identifying threats before they can impact your business. Finally, our risk-based prioritization eliminates alert fatigue by focusing on high-impact threats, ensuring your security team addresses what matters most.

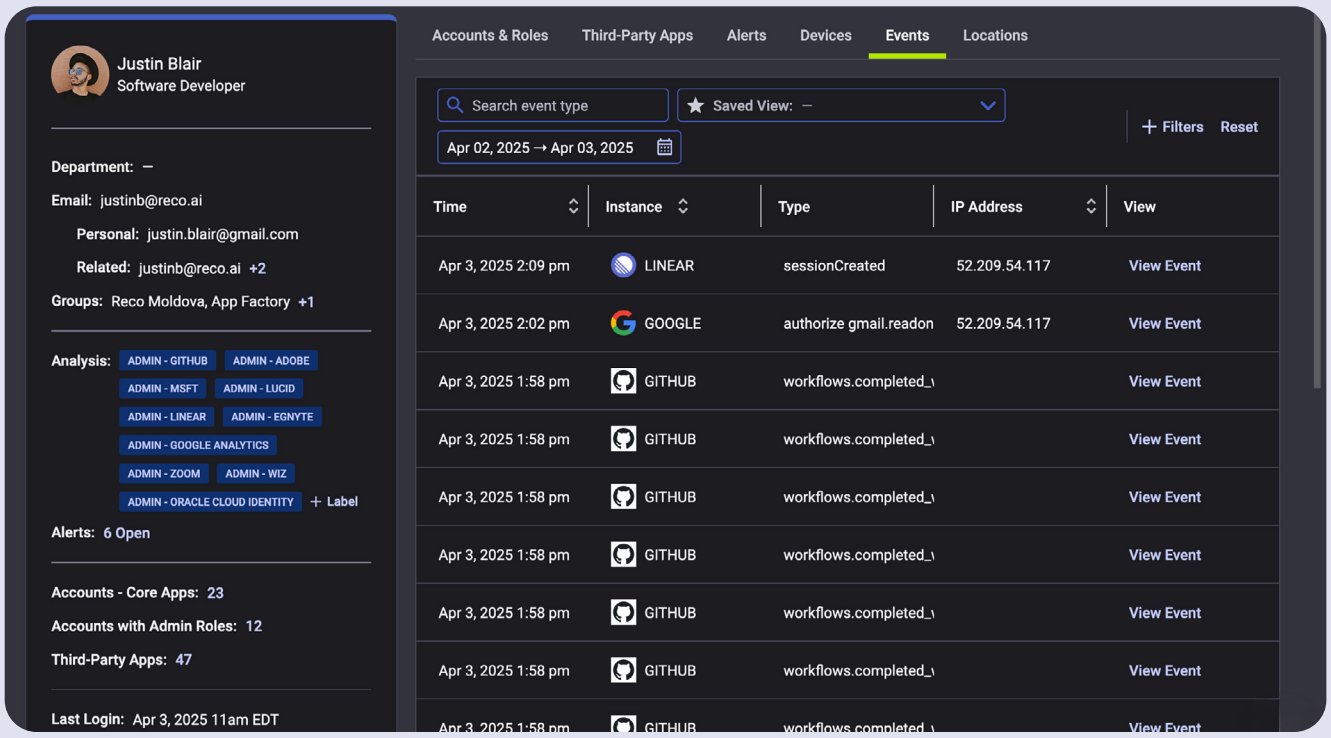
Accelerate Incident Response

Reco enhances your security response capabilities with rich contextual alerts that include user metadata, application context, and business impact, giving you complete visibility into potential threats. Our Alerts Agent provides comprehensive attack timelines and recommended remediation steps, streamlining your incident investigation process. With one-click remediation through integration with your existing security stack, you can respond to threats instantly without switching between platforms. Automated response workflows for common incident types further accelerate your mean time to resolution, while human-readable audit trails support compliance requirements and enable thorough forensic analysis when needed.



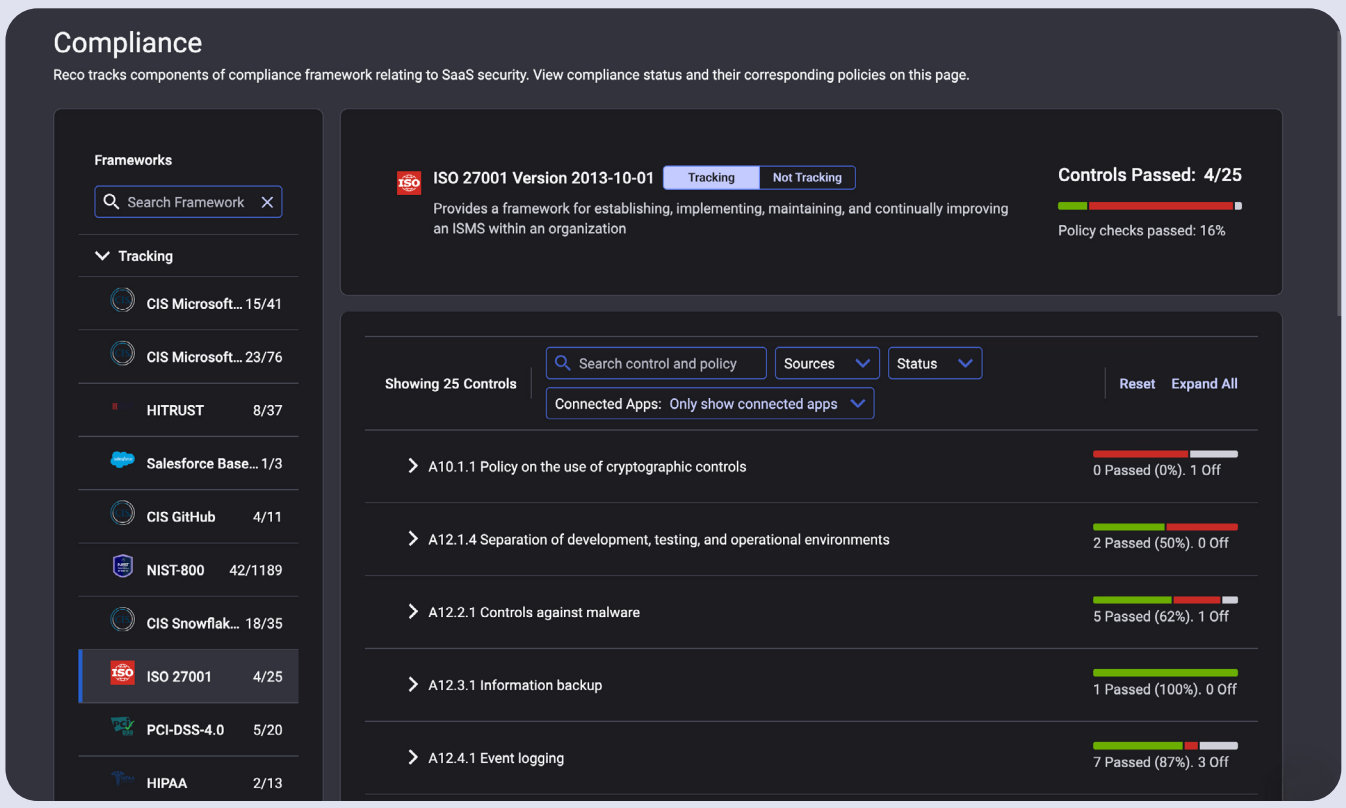
Streamlined Operations, Reduced Costs

Reco streamlines your security operations with pre-ingested and normalized data that eliminates the need for costly SIEM data indexing, giving you immediate access to actionable intelligence. We deliver a 90% reduction in SOC team alert triage time through contextual awareness and AI-driven insights, allowing your analysts to focus on what matters most. Our multi-tenant architecture enables efficient client management for service providers, while white-label reporting capabilities let you generate client-ready security assessments that reflect your brand. The entire solution comes with turnkey deployment requiring minimal configuration, getting you operational with enterprise-grade SaaS security in record time.



Expanded Service Offerings

Reco empowers your service offerings with comprehensive SaaS security assessments that identify high-risk applications and configurations, enabling you to deliver immediate value to clients. Expand your portfolio with identity threat hunting as a value-added service, uncovering potential compromises before they lead to breaches. Our platform supports compliance reporting for regulatory frameworks including SOC2, ISO 27001, and GDPR, helping your clients meet their governance requirements with minimal effort. The executive-level dashboards create powerful visuals for client security reviews, demonstrating your security program's effectiveness at a glance. Complete your offering with incident response retainer services backed by Reco's advanced detection capabilities, providing your clients with peace of mind that expert help is always available when needed.



> **With Reco's Knowledge Graph and AI agents, we can detect and respond to identity threats across our SaaS ecosystem in minutes instead of months. The pre-built integration with our existing security stack has dramatically reduced our incident response time while giving us unprecedented visibility into our SaaS identity risks.**
>
> Chief Information Security Officer,
> Fortune 500 Financial Services

Real-World Breach Incidents—How Reco Detects & Prevents

Breach Incident: The Cloud Provider Token Exposure

The Breach: In January 2024, **Snowflake** reported that hackers had breached internal systems and accessed encrypted customer data and credentials. The attackers exploited a token validation issue in a third-party application to gain initial access, then moved laterally to access internal systems.

Legacy SaaS Security Tools: Traditional tools failed to detect the compromised tokens or the unusual access patterns between the third-party application and sensitive internal resources.

How Reco Would Detect:

- **Knowledge Graph Detection:** Reco's Knowledge Graph identifies the abnormal authentication pattern and unusual data access flows between the third-party app and Snowflake systems.
- **3rd-party App Risk Assessment Agent:**
  - Alert: Critical third-party application shows unusual token usage patterns.
- **Identity Risk Assessment Agent:**
  - Alert: Service account accesses sensitive data repositories outside normal usage pattern.
- **Alerts Agent:**
  - Alert: CRITICAL: Potential token-based attack in progress. Unusual access patterns detected between third-party applications and internal systems with a comprehensive timeline.

Proactive Remediation: Automatically revoke suspicious tokens, isolate affected systems, and provide detailed mapping of all potentially compromised data.

Breach Incident: The Social Engineering Attack

The Breach: In September 2023, MGM Resorts suffered a devastating cyber attack that shut down hotel key card systems, slot machines, and reservation systems. Attackers used social engineering to gain access to the help desk by impersonating an employee, convincing IT staff to reset credentials and provide system access.

Legacy SaaS Security Tools: Traditional security tools couldn't detect the legitimate-looking password reset or the unusual activities performed by the compromised account because they lacked contextual awareness of normal help desk procedures.

How Reco Would Detect:

- **Knowledge Graph Detection:** Reco's Knowledge Graph would identify the unusual sequence of events - help desk call followed by password reset followed by immediate privileged actions.

- **Identity Risk Assessment Agent:**
  - Alert: Help desk reset account performing administrative actions inconsistent with the user's historical behavior patterns.

- **Impossible Action Agent:**
  - Alert: Recently reset user account accessing critical systems never previously accessed by this user.

- **Alerts Agent:**
  - Alert: CRITICAL: Potential social engineering attack detected. Recently reset credentials used to access multiple sensitive systems in rapid succession. Timeline shows password reset followed by immediate privileged access.

Proactive Remediation: Automatically flag suspicious credential resets, provide comprehensive audit trail of all actions taken after credential changes.

Breach Incident: The Banking Customer Data Breach

The Breach: In 2023, banking giant Santander suffered a data breach affecting 14,000 customer accounts in the UK. Attackers gained access to the bank's systems through compromised employee credentials, allowing them to access sensitive customer data including names, addresses, and account information.

Legacy SaaS Security Tools: Conventional security tools couldn't identify the abnormal data access patterns because the attackers were using legitimate employee credentials and accessed systems that employees typically use.

How Reco Would Detect:

- **Knowledge Graph Detection:** Reco would map normal data access patterns for each role and identify deviations in volume, timing, and frequency.

- **User Behavior Agent:**
  - Alert: Employee accessing 14,000 customer records in 2 hours - 10x normal volume.

- **Data Access Agent:**
  - Alert: Administrative account viewing customer financial data outside of normal business hours and across unusual geographic regions.

- **Alert Agent:**
  - Alert: HIGH RISK: Potential data exfiltration detected. Employee account showing abnormal access patterns to customer databases with detailed timeline of affected records.

Proactive Remediation: Automatically limit the number of records accessible in a time period, implement additional authentication for bulk data access, and provide comprehensive audit of all accessed records.

Breach Incident: The Persistent Advanced Threat

The Breach: In January 2024, Microsoft disclosed that the Russian state-sponsored threat actor Midnight Blizzard (also known as Nobelium/Cozy Bear) had breached its corporate systems. The attackers used a password spray attack to compromise a legacy non-production test tenant account that wasn't protected by MFA. They then used this access to gain entry to a small number of email accounts belonging to Microsoft's senior leadership team and cybersecurity employees.

Legacy SaaS Security Tools: Traditional security tools failed to detect the unusual access patterns because the attack used a valid account and the lateral movement was subtle and carefully targeted. The attackers specifically went after high-value email accounts with sensitive information about their own investigation.

How Reco Would Detect:

- **Knowledge Graph Detection:** Reco's Knowledge Graph would map the unusual connection between a legacy test account and executive email access, flagging this as a high-risk access path.

- **Identity Risk Assessment Agent:**
  - Alert: Legacy test account accessing executive email systems with no previous access history.

- **Impossible Action Agent:**
  - Alert: Non-production account performing production-level access to sensitive communication systems.

- **Alert Summary Agent:**
  - Alert: CRITICAL: Potential targeted attack on executive communications. Test account showing unusual access patterns to senior leadership email accounts with comprehensive timeline of accessed data.

Proactive Remediation: Automatically block suspicious access paths between test environments and production systems, enforce strict segmentation between environments, and provide detailed forensic analysis of all accessed email content.

reco

Reco is a Dynamic SaaS Security Platform that protects your SaaS ecosystem at every stage of its lifecycle. From discovery of all apps, AI agents, and shadow tools to continuous posture management, identity governance, and real-time threat detection, we ensure security and compliance without disrupting business agility. With Reco, organizations gain full visibility, proactive protection, and automated response to evolving SaaS risks.

Request a Demo