Keeper Security Launches Native Jira Integrations to Unify Security Incident Response and Privileged Access Governance

New Jira integrations connect security alerts, access requests and approvals into a single, governed workflow while keeping enforcement centralised in Keeper

LONDON, UNITED KINGDOM, March 4, 2026 /EINPresswire.com/ -- Keeper Security, the leading zero-trust and zero-knowledge Privileged Access Management (PAM) platform, today announces two new native Atlassian Jira integrations. The integrations with the widely-used issue and Project Tracking software embed security incident response and privileged access governance directly into existing Jira workflows while keeping access enforcement centralised in Keeper.

Jira plays a central role in how organisations manage security incidents, operational requests and change workflows. Security alerts are tracked and triaged in Jira, with remediation tasks assigned and approvals documented as part of the workflow. Yet in many environments, incident response and access enforcement remain disconnected, relying on manual handoffs, email approvals or ad hoc processes that introduce risk and delay. Keeper's Jira integrations close this gap by unifying security detection, response and access governance into a single operational flow while keeping enforcement, encryption and audit controls centralised within the Keeper platform.

The integrations consist of two Forge-based applications serving distinct but complementary roles. The Jira ITSM integration handles security events and incidents, while the Jira Workflow integration (https://docs.keeper.io/en/keeperpam/secrets-manager/integrations/jira-workflow) governs how access is requested and granted in response to those events or broader operational needs. Together, they connect detection, response and access enforcement in Jira, with Keeper remaining the system of record for security controls. The Jira Workflow integration leverages Keeper's Commander Service Mode (https://docs.keeper.io/en/keeperpam/commander-cli/service-mode-rest-api), ensuring cryptographic operations remain within the customer's environment and preserving Keeper's zero-knowledge security model.

"Security teams don't just investigate incidents in Jira; they also coordinate the access changes required to resolve them," said Craig Lurey, CTO and Co-founder of Keeper Security. "This industry-first integration extends privileged access approvals and workflow into the tools that security and IT teams use every day, ensuring that strict encryption controls are still in place."

With Keeper's Jira ITSM integration, security alerts generated by Keeper can be automatically created as Jira issues, ensuring incidents are captured, prioritised and tracked without manual ticket creation. Each issue includes full event context and structured alert data, enabling teams to assess impact and begin remediation immediately.

From there, access-related actions required to resolve an incident or operational request can be initiated directly from Jira using the Jira Workflow integration. Teams can request access to Keeper Vault resources, shared folders, service accounts or protected systems as part of the same workflow used to manage the incident or task. The integration also supports Endpoint Privilege Manager (https://www.keepersecurity.com/endpoint-privilege-management/) approvals, allowing administrators to review and act on privilege elevation requests directly within Jira.

Access requests support configurable expiration windows, enabling time-bound access with no standing privileges. All access enforcement, cryptographic controls and session auditing remain within Keeper, ensuring Jira functions as a workflow interface rather than a security boundary.

This unified approach allows organisations to:

- Eliminate insecure side channels such as email approvals or screenshots
- Unify incident response and access remediation in a single system of record
- Enforce least-privilege access consistently across cloud, hybrid and on-prem environments
- Maintain complete audit trails across alerts, approvals and access events

The Jira integrations support both team-managed and company-managed Jira projects and are built on the Atlassian Forge platform for Jira Cloud environments. Flexible field mapping allows organisations to align Keeper alert data and access workflows with existing Jira configurations, issue types and priorities. By embedding access governance into Jira workflows without decentralising enforcement, Keeper enables organisations to modernise security operations while preserving the zero-trust and zero-knowledge architecture required for compliance, audit and risk management.

"These integrations reflect Keeper's broader platform strategy," added Lurey. "Security workflows should adapt to how teams work, but enforcement should never be fragmented. Jira is where decisions happen. Keeper is where access is controlled."

Keeper offers a rich set of integrations that help companies unify and strengthen their security and identity workflows while reducing manual overhead. Keeper connects with identity providers and Single Sign-On (SSO) systems and supports automated user provisioning via System for Cross-domain Identity Management (SCIM) tools, making onboarding and offboarding smoother and more secure. Keeper also integrates with Security Information and Event Management (SIEM) tools to feed real-time credential and access activity into broader security monitoring and

compliance dashboards, among other integrations. For business customers, these integrations streamline authentication, improve threat detection and compliance, enhance visibility into access activity and boost operational efficiency by tying Keeper into existing enterprise tools and workflows.

Keeper's new Jira integrations are available now. For more information, visit www.keepersecurity.com.

###

About Keeper Security
Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognised for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organisations to defend against modern adversaries at www.keepersecurity.com.

Learn more: KeeperSecurity.com

Media Contact

Charley Nash, Account Manager
Keeper Security
charley@eskenzipr.com
Visit us on social media:
Facebook
Instagram
LinkedIn
X
YouTube
TikTok
