Cloud Infrastructure Entitlement Management with Prisma Cloud

Secure Multicloud Resources by Establishing Least-Privileged Access

Identity and access management (IAM) for cloud infrastructure controls how cloud identities can take action on specific resources. However, defining roles and permissions using the principle of least privilege is challenging in public and multicloud environments:

- The public cloud introduces machine identities, which have outnumbered human identities, leading to thousands of identities and resources to manage across clouds.
- Most organizations do not understand users' entitlements and access requirements.
- Each cloud service provider (CSP) has a unique IAM policy model and taxonomy.

Organizations striving to implement Zero Trust practices and least-privilege principles require a unified multicloud view across IAM policies, with process automation across cloud accounts, resources, and policies.

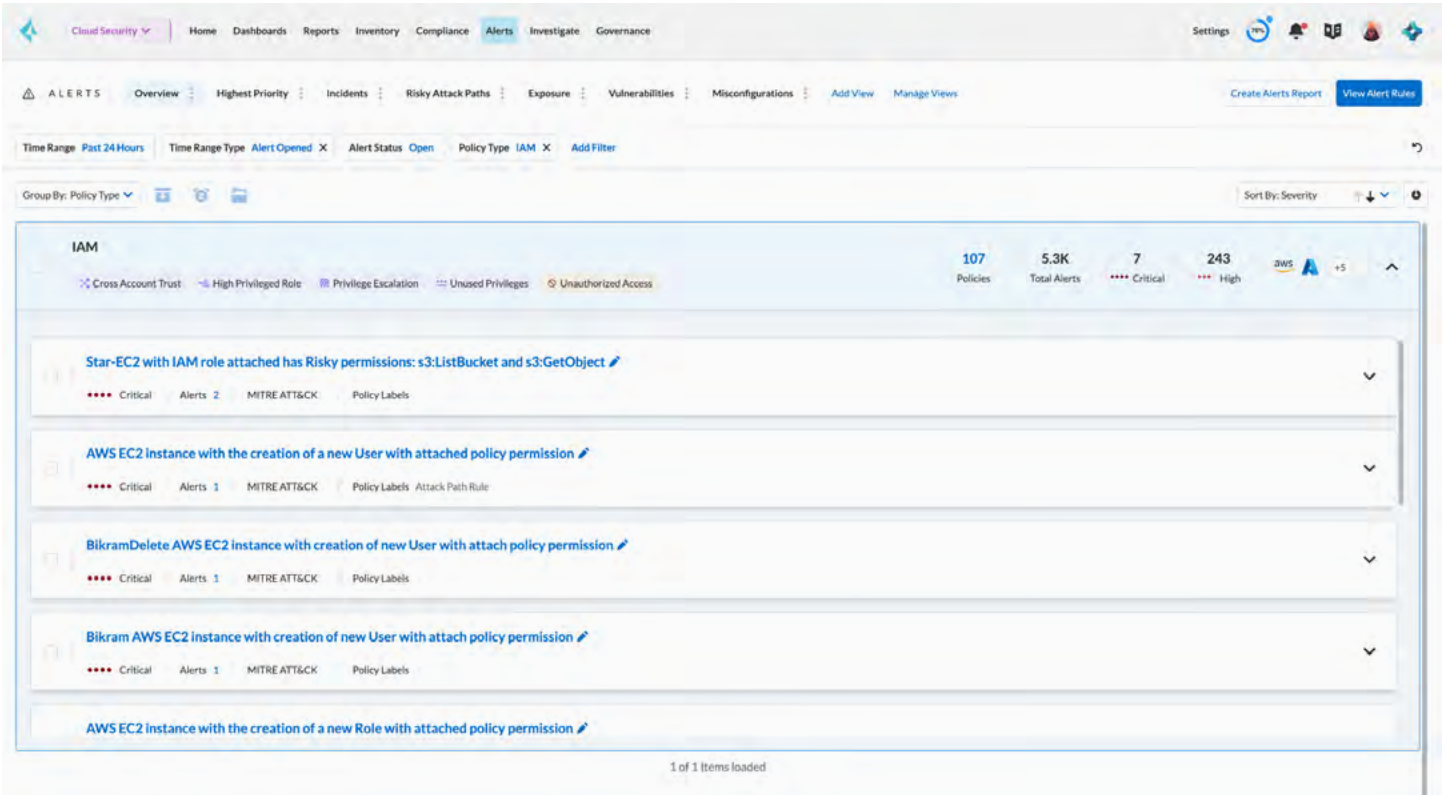

Figure 1: Overview of critical IAM alerts

Control Access and Net-Effective Permissions

Cloud Infrastructure Entitlement Management (CIEM) in Prisma Cloud is purpose-built to directly solve the challenges of managing permissions across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Prisma Cloud automatically calculates users' effective permissions across cloud service providers, detects overly permissive access, and suggests corrections to reach least privilege entitlements. Out-of-the-box policies help you govern IAM best practices. User and entity behavior analytics capabilities provide clarity by monitoring activities that could signal account compromises.

Prisma Cloud CIEM Capabilities

Visibility into Net-Effective Permissions

Prisma Cloud analyzes entitlements granted to identities across multiple cloud providers, including those identities managed in identity providers (IdPs) and calculates the net-effective permissions, normalizing the data into a table or graph view that offers instant visibility into exactly who or what has access to which resources and what they can do.

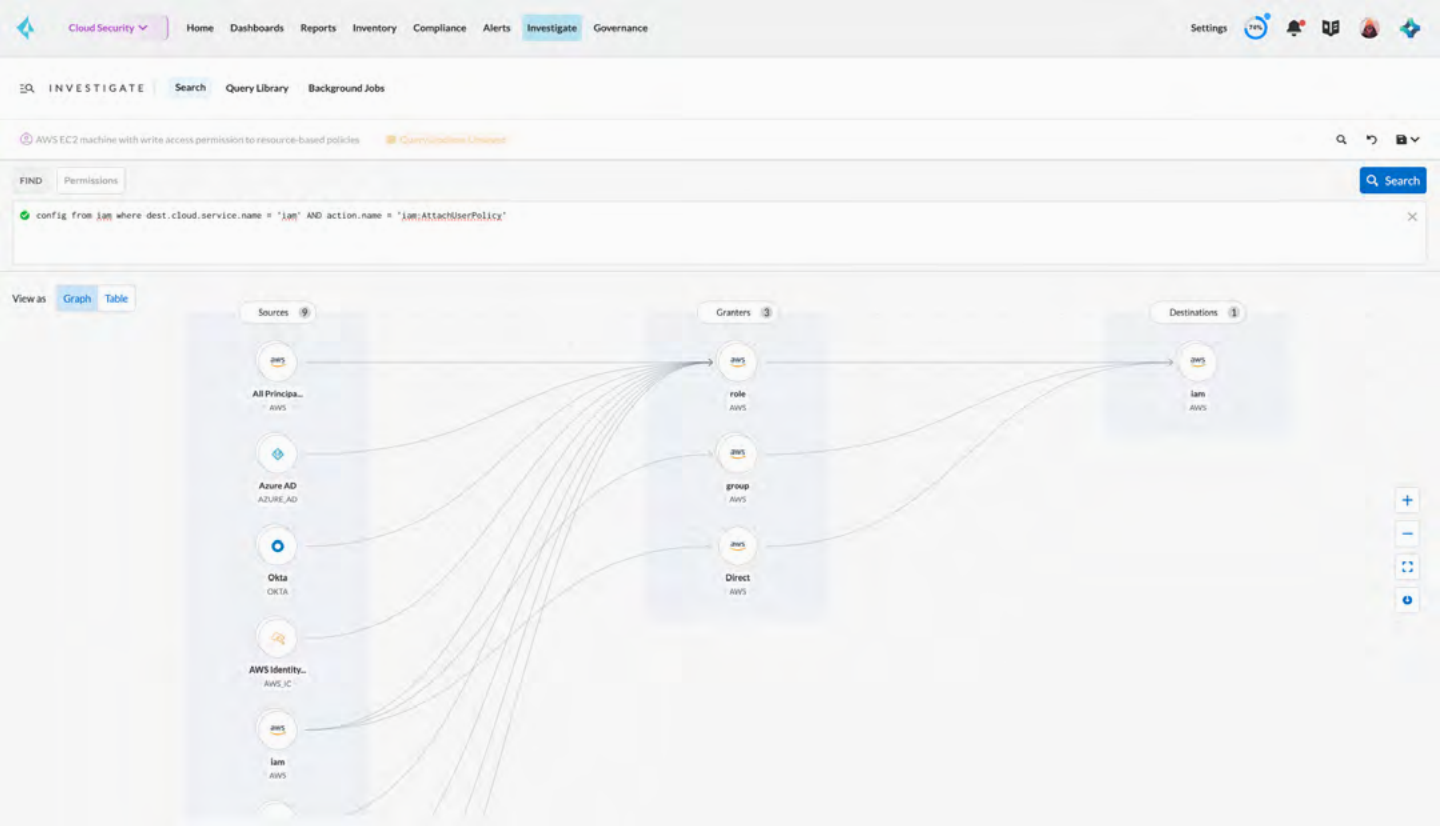

Figure 2: Comprehensive visibility into resource permissions

Out-of-the-Box Policies and Rightsizing Permissions

Use out-of-the-box policies to detect public exposure, wildcards, risky permissions, and more. Prisma Cloud helps remove unnecessary access to cloud resources by automatically detecting overly permissive access policies and then offering suggestions to rightsize them to achieve least privilege entitlements.

IAM Entitlement Investigation

Use Prisma Cloud Resource Query Language (RQL) to query all relevant IAM entities, including all the relationships among different entities and their effective permissions across cloud environments. You can answer questions such as:

- Which users have access to resource X?
- What accounts, services, and resources do the user name@domain.com have access to?
- Can any users outside of group C access resources in region D?

IdP Integration

Prisma Cloud integrates with IdP services such as Okta, Azure Active Directory (Azure AD), and AWS IAM Identity Center to ingest single sign-on (SSO) data. It then correlates this data with cloud identities such as IAM users and machine identities, enabling you to view a user's effective permissions or detect overly permissive roles.

User and Entity Behavior Analytics (UEBA)

Prisma Cloud applies UEBA to millions of audit events using machine learning to detect anomalous activities that could signal account compromises, insider threats, stolen access keys, and other potentially malicious user activities.

Automated Remediation

Prisma Cloud can automatically suggest or make permissions adjustments, helping you continuously ensure least-privileged access.

Just-In-Time (JIT) Access

Provides a Zero Trust approach to permission management by limiting access to resources based on specific, time-limited permissions. Users and machine identities are granted access only when they need it and for a limited amount of time, reducing the overall attack surface and exposure of critical resources to potential threats.

- **Utilize zero standing privileges**: Allow identities to request temporary access to resources on an as-needed basis, reducing the risk of having long-lasting unused permissions.
- **Automate or manually approve access**: Enable both automatic and manual approval based on the organization configurations.
- **Active monitoring**: Gain visibility into active sessions with the ability to kill unwanted sessions in real time.

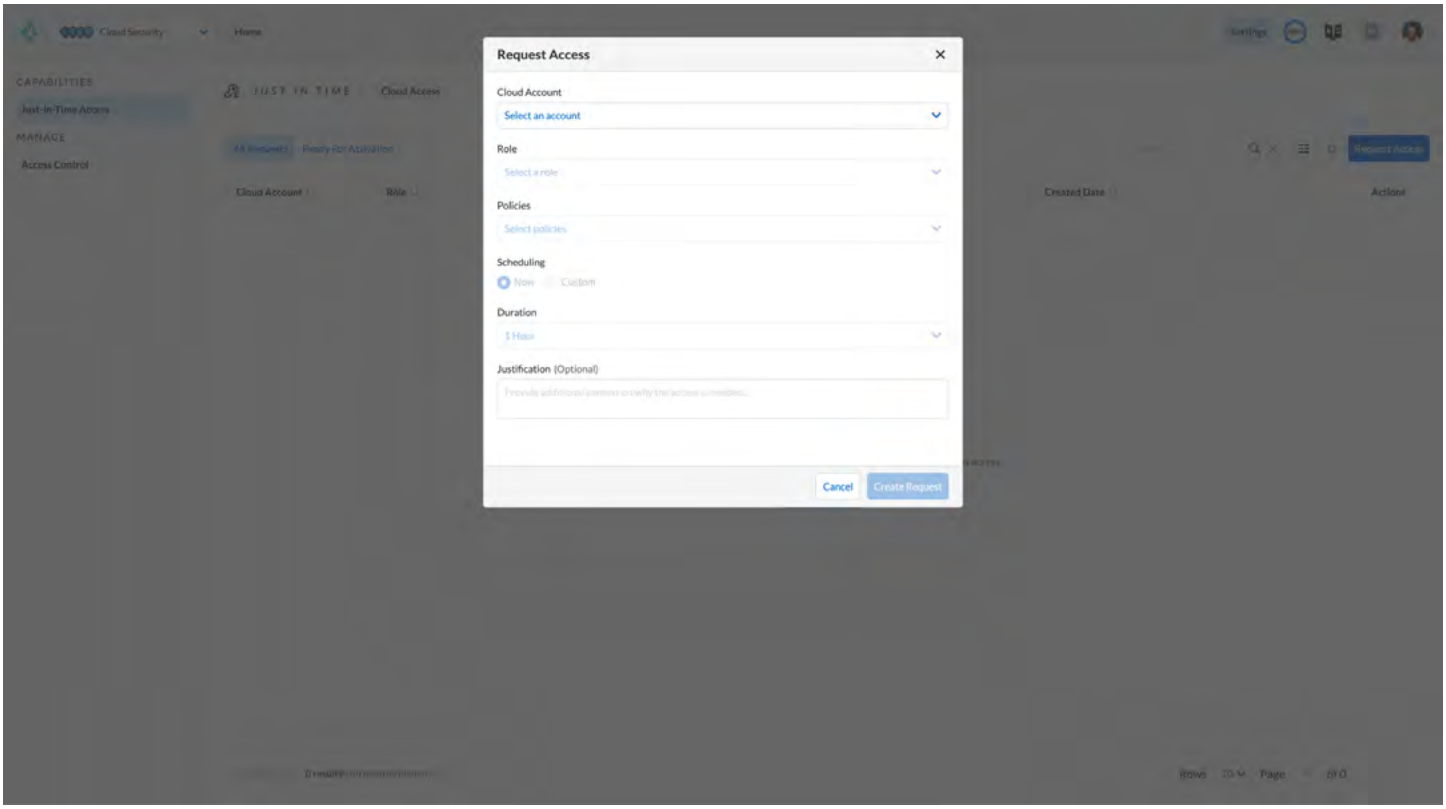

Figure 3: Developer requesting JIT access

Extending Beyond CIEM

The Prisma Cloud platform provides value that standalone CIEM tools cannot. Best-of-breed CIEM capabilities are integrated into a single-vendor cloud-native application protection platform (CNAPP), providing additional value.

Correlate Findings to Prioritize and Understand Critical Risks

A misconfigured or overly permissive identity by itself does not always represent application risk. Prisma Cloud analyzes misconfigurations, vulnerabilities, public exposures, excessive permissions, exposed secrets, sensitive data, incidents, and more to identify interrelated issues that present critical risks.

Visualize Attack Paths to Accelerate Investigations

Prisma Cloud visualizes interconnected risks, helping security teams understand how several configuration mistakes form attack paths. By combining multiple risk factors across identities and cloud assets, Prisma Cloud can help you prioritize interconnected alerts.

Remediate Risk Efficiently

Prisma Cloud provides several options to address risks such as opening tickets with application owners, automatically remediating misconfigurations. Security professionals can communicate risk context and remediation steps to help reduce any developer friction.

> **"We wanted a consistent, holistic approach to cybersecurity, using modern technologies like AI and automation to efficiently safeguard the organization."**
>
> – Liran Sheinbox, Head of Cyber Security, Playtika

Read the full case study.

About Prisma Cloud

Prisma® Cloud is the industry's most comprehensive cloud-native application protection platform (CNAPP) with the broadest security and compliance coverage—for applications, data, and the entire cloud-native technology stack—throughout the development lifecycle and across multicloud and hybrid environments. Our integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate secure cloud-native application development. To learn more, visit us online.

To learn more, visit us online or watch a demo now.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com