Palo Alto Networks and Orchid Security

Close the Privileged Access Gap by Finding Accounts Beyond PAM Reach

Key Benefits

- Discovers privileged accounts across application-native and local identity stores.
- Reports the identified high-risk accounts to Palo Alto Networks Idira® for privileged access management (PAM) review.
- Gives administrators source context to prioritize onboarding decisions.
- Keeps vaulting and rotation decisions under Idira administrator control.
- Tracks the status of reported, onboarded, or rejected accounts that Orchid Security surfaces.

The Challenge

Privileged access often extends beyond centralized identity and PAM programs. Applications can store local administrator accounts, service accounts, orphaned users, and other application-native identities that are difficult to inventory and prioritize. When these accounts remain outside the PAM onboarding pipeline, security teams have limited visibility into who can perform sensitive actions, which accounts require review, and where privileged access remains unmanaged. These limitations create coverage gaps, slow remediation, and make it difficult to demonstrate control over privileged accounts during audits.

The Solution

A discovery-driven workflow helps security teams find privileged accounts where they exist, enrich them with application and ownership context, and route them to the team responsible for PAM review. It surfaces accounts that require action by providing sufficient context for administrators to assess risk, decide whether to onboard them, and track the outcome. This approach extends privileged account visibility across the application estate, while keeping onboarding and vault-management decisions within the PAM team.

Orchid Security Identity Control Plane

The Orchid Security identity control plane platform discovers accounts across applications and identifies privileged access that might not be visible in centralized identity or PAM tools. Orchid analyzes application-native identities, local accounts, service accounts, and ownership signals across homegrown, commercial, and SaaS applications. In the joint solution, Orchid identifies accounts to be reviewed for PAM and reports them with source context—enabling PAM teams to investigate and act through their standard workflow.

Palo Alto Networks Idira

Palo Alto Networks Idira is a next-generation identity security platform built on its PAM foundation. It extends zero standing privilege controls to every identity, including external vendors and technicians who need access to distributed energy OT sites. For third-party and vendor access, Idira eliminates VPN and bastion dependencies by replacing standing credentials with browser-based, just-in-time access scoped to a specific task. Every session is isolated and fully recorded for audit and compliance.

Palo Alto Networks and Orchid Security

Together, Palo Alto Networks Idira and Orchid Security help customers close privileged access coverage gaps across applications. Orchid discovers and analyzes application-native accounts, identifies accounts with privileged access, and reports them to the Idira discovered accounts queue. Idira administrators can then review those accounts, decide whether to onboard them, and manage them through the organization's existing PAM workflow. The integration gives

security teams broader coverage into unmanaged privileged accounts without changing vault ownership or bypassing existing approval processes.

Use Case 1: Find Privileged Accounts Outside PAM Coverage

Challenge

Security teams might not know which local, application-native, service, or orphaned accounts have privileged access inside applications. Without reliable discovery, these accounts can remain unmanaged and outside PAM review.

Solution

Orchid Security discovers accounts across the application estate and identifies accounts with privileged access. The integration reports those accounts to the accounts Idira discovered with source context and Orchid tagging. Idira administrators can filter for accounts reported by Orchid, review each account, and decide how to onboard and manage it.

Use Case 2: Add Context to Accelerate Account Review

Challenge

PAM teams often receive incomplete account inventories and must manually determine which accounts need action. Limited context slows review and can delay the onboarding of privileged accounts.

Solution

Orchid Security adds application and discovery context to reported accounts, enabling administrators to understand where each account was found and why it was identified for privileged access review. Idira remains the operational system for review, onboarding, vaulting, rotation, and enforcement.

About Orchid Security

Orchid Security is identity infrastructure for the AI era. Orchid analyzes application binaries to deliver the industry's first identity control plane—continuously discovering enterprise applications, analyzing their native authentication and authorization flows, and surfacing the identities operating at execution time, across human, nonhuman, and agentic AI accounts. By exposing what's actually running inside applications, Orchid helps enterprises close identity coverage gaps and bring unmanaged access under control, at scale. For more information, visit www.orchid.security.

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 75,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.

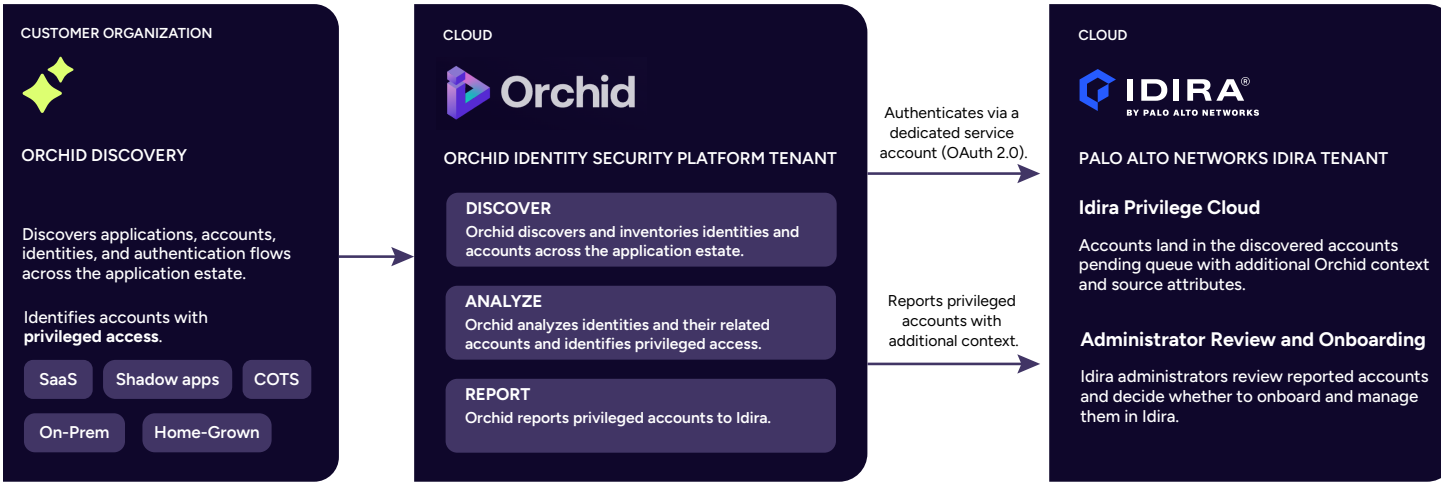

Figure 1. The Orchid to Idira privileged account discovery and onboarding flow

paloalto NETWORKS | Orchid

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

parent_pb_orchid-security_091026