
Keeping Secrets Under Control and Secure with Idira and AWS



Contents

Too Many Secrets and Vaults, Not Enough Visibility and Control	3
The Hidden Cost of Vault Sprawl.....	3
Untangling the Tangle.....	4
How Palo Alto Networks and AWS Solve This Challenge	4
Secrets by the Numbers.....	4
One View, Total Control	5
Designed with Developers in Mind	6
Keep Developers in Their Flow	6
No Friction, Just Forward Momentum	6
Built for Real-World Developer Experience	6

Centralized Security and Compliance	7
Delivering Visibility and Consistency	7
Align, Boost, Simplify, and Support Secrets Management	9
Aligned Security and Developers.....	10
Simplified Mergers and Acquisitions	10
Boosted Operational Efficiency.....	10
Find, Unify, and Control Secrets Today and Tomorrow	11
About Palo Alto Networks	12

Too Many Secrets and Vaults, Not Enough Visibility and Control

Your teams and workloads have scaled rapidly in the cloud. Today, machine identities now outnumber humans 82 to 1, with each identity generating or consuming secrets across applications, pipelines, services, and dynamic cloud workloads.¹ To keep up, teams often spin up their own AWS Secrets Manager vaults for each new environment or account.

Over time, this leads to vault sprawl. Secrets are scattered across isolated vaults tied to specific workloads, cloud accounts or teams, and they are often unmanaged, duplicated, or misconfigured. Without centralized visibility and control, security teams must contend with blind spots, inconsistent policies, and security silos that increase operational and compliance risk.

Audit readiness becomes harder. Policy enforcement breaks down. And the attack surface quietly expands across the very cloud environments meant to drive speed and agility.



1. 2025 *Identity Security Landscape*, CyberArk, May 2025.

2. Marks, Melinda and Jon Oltsik, *Research Report: Cloud Detection and Response*, Enterprise Strategy Group, December 15, 2023.

The Hidden Cost of Vault Sprawl

Vault sprawl disrupts security policy, slows down development teams, and increases risk across every stage of the software lifecycle. With 85% of organizations releasing to production at least once a week, secrets are continuously being created and used by dynamic workloads across CI/CD pipelines, containers, serverless functions, and other cloud-native environments.² But when secrets are spread across isolated vaults and each is managed differently by separate teams or accounts, security and compliance become fragmented.

In many organizations, this vault sprawl leads to shadow vaults that developers or platform teams spin up without security oversight. These vaults often fall outside the scope of centralized controls and might not comply with internal policies for access, encryption, or rotation.



Overpermissioned workloads from inconsistent provisioning



Missed rotation schedules leading to compliance gaps



Slow incident response due to compromised credentials

Without a unified view of which workloads use which secrets and how they are secured, enforcing least privilege becomes nearly impossible, as does detecting risk early or demonstrating compliance efficiently.

Untangling the Tangle

To protect identities and secure workloads, you need to bring visibility, consistency, and control to the vaults already in use across the cloud. Instead of expecting developers to rearchitect their workflows, security teams should be able to regain control without disrupting delivery. They need to manage secrets centrally across AWS environments, automating rotation, standardizing policy enforcement, and detecting noncompliant values, all while developers continue working the way they always have.

How Palo Alto Networks and AWS Solve This Challenge

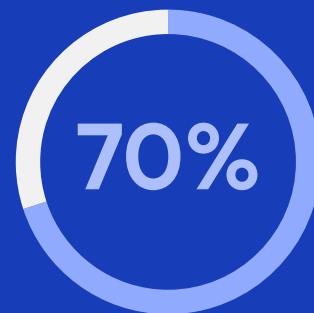
The Palo Alto Networks Idira™ and AWS solution balances enterprise-grade security with cloud-native agility. Developers keep their existing AWS-native workflows and secrets, and security leaders get a centralized control plane to discover, rotate, and enforce policies across their AWS organization, which can be multiple accounts.

Because organizations are focused on visibility and unifying secrets, they can rein in vault sprawl, secure machine identities, and eliminate blind spots, all without slowing down innovation.

Secrets by the Numbers

23.77 million

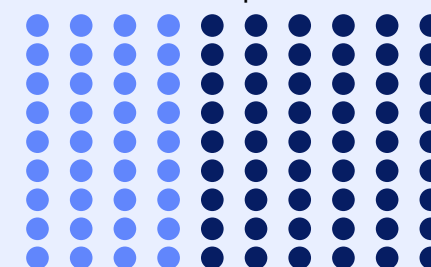
new secrets leaked on GitHub in 2024.³



of secrets first detected in public repositories in 2022 are still active.⁴

40%

higher incidence rate of secret leaks in AI assistant repositories.⁵



3-5. *The State of Secrets Sprawl 2025*, GitGuardian, March 2025.

One View, Total Control

Idira Secrets Hub, a Palo Alto Networks SaaS solution, is purpose-built for organizations that already use AWS Secrets Manager and other cloud-native secrets stores. Idira Secrets Hub consolidates governance, not infrastructure. Security teams can automatically discover secrets vaults across all AWS accounts in their organization, including unmanaged or shadow vaults, providing a complete picture of where secrets live and how they're used.



AWS Secrets Manager

AWS Secrets Manager enables teams to manage, retrieve, and rotate database credentials, application credentials, OAuth tokens, API keys, and other secrets throughout their lifecycles. It helps developers remove hard-coded credentials from application code, improving security by reducing accidental exposure.



A Single Pane of Glass for Secrets Vaults

Idira Secrets Hub seamlessly integrates with native AWS APIs and connects existing secrets vaults to Idira Identity Security Platform, creating a single pane of glass for secrets vault visibility and governance. Developers can continue using their native secrets managers, like AWS Secrets Manager, while security teams apply centralized policies across multiple accounts, tools, and cloud environments. Governance is consolidated across distributed vaults without requiring any rearchitecture.



One Place to Manage All Secrets

Whether secrets are stored in AWS Secrets Manager or across hybrid environments, Idira Secrets Hub gives security teams a clean, unified view of all vaults and workloads without requiring consolidation. From a single console, they can apply consistent policies, automate rotation, and detect unmanaged or noncompliant vaults. Idira Secrets Hub offers AWS organization-level scanning, which helps eliminate shadow vaults, reduce risk, and accelerate audit readiness, resulting in fewer silos, surprises, and security gaps.

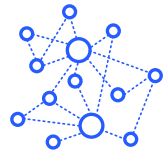


Less Manual Work, More Secure by Default

Idira Secrets Hub supports automatic rotation and vault consolidation so secrets don't sit unchanged or multiply in unmanaged silos. It reduces human error, streamlines policy enforcement, and increases overall security posture. Machine identities and workloads are automatically granted access at scale.

With Idira Secrets Hub, security teams get automation, centralized visibility, and consistent security policy enforcement, all without disrupting developer workflows.

Designed with Developers in Mind



Keep Developers in Their Flow

Developers continue using AWS Secrets Manager, without code rewrites, tool swaps, or worrying about new interfaces. Idira Secrets Hub automatically synchronizes secrets from native stores to the Idira centralized control plane behind the scenes so developers get governance and visibility that doesn't interrupt development workflows.



No Friction, Just Forward Momentum

Idira Secrets Hub removes the need for new tools or process changes, working seamlessly with what's already in place, including code, tools, and CI/CD workflows. It eliminates the tension that often arises between security and developer speed, enabling developers to stay productive and deliver at pace.



Built for Real-World Developer Experience

Whether developers have already built out apps using AWS Secrets Manager or inherited environments through a merger, Idira Secrets Hub fits right in. Without stalling progress, it secures secrets behind the scenes, with enterprise-grade controls applied invisibly across vaults, workloads, and environments. Adoption sticks because developers get security without slowdown.



Automated for Security, While Invisible to Developers

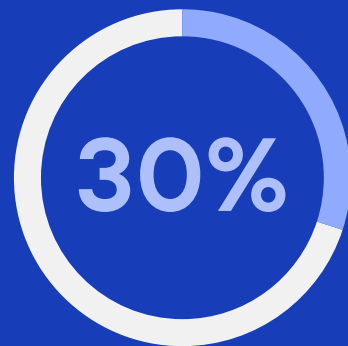
A global insurance company used Idira Secrets Hub and AWS Secrets Manager to create a flow that worked for both security and developers. The company created a policy that developers must store all secrets in Idira and then push them to AWS. By automating this policy, the company now saves every new secret into Idira automatically.

The result is that developers have zero slowdowns and gain enterprise-wide governance for security.

Centralized Security and Compliance

Like developers, security teams also need an easy-to-use solution that works with current workflows or processes. Changing security operations (SecOps) tools can compete for attention with other urgent tasks, cause delays, demand more training and expert skills, and increase security risks. Idira Secrets Hub offers centralized, scalable secrets management across AWS accounts and environments. It ensures that all secrets are protected, reduces complexity, and improves control without imposing added burdens on security teams.

What You Can't See Can Hurt You



A global investment company used Idira Secrets Hub to scan 350 AWS accounts. They uncovered more than 2,000 secrets, of which 600 hadn't been used in over three months. Many of them were idle, forgotten, or unknown to the security team.

Within weeks, they cleaned up unused credentials, tightened rotation policies, and improved audit readiness—without affecting production workloads.

Delivering Visibility and Consistency

By using Idira Secrets Hub, SecOps teams use one console to see, manage, and consistently apply policies to all secrets in the organization. SecOps teams gain visibility across all distributed secrets vaults and achieve full discovery of AWS Secrets Manager instances throughout an AWS organization, including those created outside of provisioning processes. This easy-to-use solution is simple to configure so security teams can quickly and effectively manage secrets without imposing changes to existing code.

The screenshot shows the 'Secret stores' page in the Idira Secrets Hub console. It features a table with 14 items, each representing a secret store. The table columns are: STATUS, PLATFORM, WORKSPACE, SECRET STORE NAME, NUMBER OF SECR..., SYNC POLICIES, and LAST SCAN DATE. The interface includes a search bar, a filter for 'Platform' (set to 'All'), and an 'Add secret store' button.

STATUS	PLATFORM	WORKSPACE	SECRET STORE NAME	NUMBER OF SECR...	SYNC POLICIES	LAST SCAN DATE
<input type="checkbox"/>	AWS	o-0fgerd04sl	COM-NP-Int-M-CloudSec...	56	-	04 Aug 2025, 11:38 AM
<input type="checkbox"/>	AWS	o-0fgerd04sl	COM-NP-Int-M-CloudSec...	66	-	04 Aug 2025, 11:38 AM
<input type="checkbox"/>	AWS	o-0fgerd04sl	COM-NP-Int-M-CloudSec...	-	-	24 Jul 2025, 01:24 PM
<input type="checkbox"/>	AWS	o-0fgerd04sl	723129436356 - us-east-1	15	-	24 Jul 2025, 01:25 PM
<input type="checkbox"/>	AWS	o-0fgerd04sl	COM-NP-Int-M-CloudSec...	53	-	24 Jul 2025, 01:27 PM
<input type="checkbox"/>	AWS	o-0fgerd04sl	COM-NP-Int-M-CloudSec...	106	-	24 Jul 2025, 11:38 AM
<input type="checkbox"/>	AWS	o-0fgerd04sl	723129436356 - ap-sout...	-	-	14 Apr 2025, 01:11 PM
<input type="checkbox"/>	AWS	o-0fgerd04sl	COM-NP-Int-M-CloudSec...	-	-	23 Apr 2025, 11:34 AM
<input type="checkbox"/>	AWS	o-0fgerd04sl	COM-NP-Int-M-CloudSec...	-	-	23 Apr 2025, 11:34 AM
<input type="checkbox"/>	AWS	o-0fgerd04sl	COM-NP-Int-M-CloudSec...	1	-	23 Apr 2025, 11:34 AM
<input type="checkbox"/>	Azure	31ac5fe4-da4a-4605-bd0...	hzur-test	-	-	04 Aug 2025, 11:38 AM
<input type="checkbox"/>	AWS	-	shub-dev - Europe (Fran...	23	-	04 Aug 2025, 11:38 AM
<input type="checkbox"/>	-	-	jenkinshashivaultresourc...	-	-	-
<input type="checkbox"/>	AWS	-	shub-dev - US East (N. Vi...	2791	2	04 Aug 2025, 11:38 AM



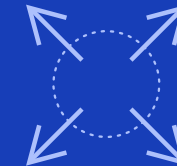
Automating Secrets Rotation

Idira Secrets Hub supports automated rotation of secrets by using AWS Secrets Manager and other cloud-native services. It enables security teams to uphold corporate policies and standards across all AWS-based applications and eliminate manual processes that can be hampered by human errors. Rotation policies are enforced consistently behind the scenes without needing to involve development.



Reducing Vault Sprawl

With Idira Secrets Hub, security teams and organizations can consolidate multiple instances of AWS Secrets Manager into one managed view with the same number of secret stores, reducing vault sprawl and improving efficiency. It helps them identify and unify shadow vaults that development teams might have created independently, giving back the oversight security needs. Security teams can control access to secrets in applications by using AWS Secrets Manager. They can also enforce the principle of least privilege, giving development teams, applications, and CI/CD pipelines access to only the secrets they need.



Scaling with Resiliency

Idira Secrets Hub scales to support large secrets management efforts. Because it's highly resilient, production applications that depend on AWS Secrets Manager aren't impacted. Idira Secrets Hub is architected for cloud scale and integrates directly with AWS native services, providing secure, reliable operations without introducing latency. Idira product-level security can meet stringent enterprise and regulatory requirements, making it trusted by some of the world's most security-conscious organizations.

Align, Boost, Simplify, and Support Secrets Management

Modern environments are a mix of cloud-native speed and legacy complexity. Machine identities, workloads, and even AI agents all demand secure, scalable access to secrets. Idira Secrets Hub brings order to the chaos, supporting everything from AI agents to acquisition rollups without forcing teams to slow down or start over. The benefits and use cases are many and varied.



Why Idira Secrets Hub



Keep using what works

Teams stick with the cloud-native vaults they already know, without disruption or rework.



Cut the clutter

Idira Secrets Hub syncs across Palo Alto Networks and cloud-native vaults to reduce sprawl and simplify operations.



Secure at scale

Policies are enforced centrally, even across hybrid environments so nothing slips through the cracks.



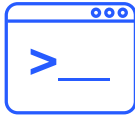
Stay audit-ready

Built-in rotation and access controls help meet compliance standards, with clear trails for every secret.



No slowdown for developers

Native integration with existing tools means developers can keep building without changing how they work.



Aligned Security and Developers

Recent media coverage of security incidents caused by moving laterally from cloud development environments to production has put organizations on high alert. Security teams are expected to make sure that these development vulnerabilities disappear. However, developers can resent these security measures because they believe they can affect their fast release cycles. Idira Secrets Hub helps bridge that gap by creating a shared foundation where security teams enforce policy while developers keep working in native AWS environments. Teams and their organizations experience fewer workarounds, less risk, and smoother collaboration.



Simplified Mergers and Acquisitions

M&A is rarely smooth, especially when reconciling infrastructure. Different teams bring different tools, often with entrenched practices around how secrets are managed. Idira Secrets Hub simplifies this by connecting AWS-native secrets workflows with broader enterprise policies. No new tools or sudden changes are needed. Newly acquired teams can keep working in the AWS environments they know without pausing innovation. Security teams gain the oversight and policy consistency they need. Alignment is accelerated across all environments.



Boosted Operational Efficiency

Manual secrets management is a drag on speed and consistency. Idira Secrets Hub helps teams move faster by automating routine tasks such as syncing secrets across systems, removing guesswork from the process. It also simplifies onboarding. When new applications or teams come online, including through an M&A, Idira Secrets Hub can discover and connect their secrets without delay. There's no need for hand-holding or custom workflows. Rollouts are faster with less overhead, and your teams can spend more time on building and much less time on backtracking.



Supported Post-Quantum Readiness

Quantum computing isn't here yet, but it's close enough that modern systems need to plan for it. Idira Secrets Hub supports TLS connections that use post-quantum cryptographic standards by securing how secrets are transmitted and where they live. It pairs seamlessly with AWS cryptography services and ensures you're prepared for what's next without needing to retool later.

From accelerating today's workflows to preparing for tomorrow's threats, Idira and AWS are helping organizations secure secrets without slowing down. You're ready to meet today's moments while building a stronger foundation for what's next.

Find, Unify, and Control Secrets Today and Tomorrow

Idira Secrets Hub was built in direct response to what customers have asked for—a solution that secures secrets without slowing down development. It's simple to adopt and works with what teams already use, delivering immediate impact without disruption.

By connecting native AWS secrets with Idira's centralized tools, Idira Secrets Hub brings everything into one place. Security teams get single-pane-of-glass visibility and policy control to secure their vaults, machine identities, and workloads. And, developers get to keep their tools, APIs, and workflows intact. Idira Secrets Hub unifies secrets management across environments, clouds, and teams without adding complexity.

As automation and AI reshape how software gets built, Idira Secrets Hub provides a future-ready foundation to help manage secrets at scale.

To explore all the ways Idira can secure the machine identities across your organization, visit www.paloaltonetworks.com/idira/machine.



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 70,000 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.



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

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
idira_eb_keeping-secrets-under-control_043026