

Three Critical Use Cases for Enterprise Secrets Management

Securing Secrets Across Cloud, DevOps, and
Legacy Infrastructure

The number of machine identities in modern enterprises is growing dramatically—often outnumbering human users by more than 109 to 1.¹ These nonhuman identities, used by applications, automation tools, containers, bots, and services, rely on secrets like API keys, credentials, and tokens to function. As organizations scale their use of DevOps, multicloud, and AI-driven workloads, the volume and importance of these machine secrets continue to rise.

This rapid growth brings new risks. Unmanaged and hard-coded secrets, vault sprawl, inconsistent rotation, and limited visibility create security gaps that attackers are increasingly targeting. While Palo Alto Networks predicts the number of machine identities will continue increasing, many organizations aren't prepared to secure them.

To manage machine secrets effectively, security and development teams must work together. But collaboration can't come at the expense of speed. The secrets management strategy needs to strengthen security and support modern development workflows across hybrid, multicloud, and on-premises environments.

This whitepaper explores three core use cases for enterprise secrets management, each mapped to a specific Palo Alto Networks Idira™ product that helps secure dynamic, cloud-native applications and CI/CD pipelines:

- **Idira Secrets Manager**, which helps gain centralized visibility and control over cloud-native secrets vaults.
- **Idira Secrets Hub**, which protects static or hard-to-refactor applications that require secrets at runtime.
- **Idira Credential Providers**, which delivers a centralized, policy-based solution to secure secrets in static, long-lived, and on-premises environments.

Each use case highlights the challenges it addresses, when to apply it, and the security and operational benefits organizations can expect. While products can be deployed individually, they are designed to work together as part of a unified platform—enabling centralized policy, identity-based access, and consistent audit across the entire infrastructure.

Best Practices for Machine Secrets Management

The most successful organizations adopt a strategy that combines strong security principles with operational efficiency. Key machine secrets management best practices include:

- **Discover and inventory secrets** across environments to close visibility gaps.
- **Eliminate vault sprawl** by consolidating secrets under centralized governance.
- **Automate rotation and enforce least privilege** to reduce exposure windows.
- **Use dynamic secrets** for just-in-time (JIT) access in cloud-native environments.
- **Avoid hard-coded credentials** in code, pipelines, and configuration files.
- **Support developer workflows** with APIs, native integrations, and low-friction tooling.
- **Audit and log all access** to maintain compliance and support incident response.

Whether you're securing CI/CD pipelines, integrating with Amazon Web Services (AWS) or Microsoft Azure, or protecting established enterprise systems, Idira's flexible secrets management solutions can help you enforce security best practices without slowing innovation.

1. *2026 Identity Security Landscape*, Palo Alto Networks, May 11, 2026.

Use Case 1:

Standardize Secrets Management Across Hybrid and Multicloud Environments

Many organizations operate in hybrid environments, with applications running both on-premises and across multiple cloud platforms. This fragmentation often leads to security silos, where different teams use inconsistent tools and processes to manage secrets. As a result, organizations struggle with secrets sprawl, hard-coded credentials, and limited visibility—making it difficult to enforce consistent security controls and increasing the risk of exposure.

Idira Secrets Manager provides centralized secrets management for hybrid and multicloud environments. It secures application credentials, service accounts, and other sensitive secrets wherever they reside. Whether running in Kubernetes, virtual machines, or PaaS environments, Idira Secrets Manager enforces strong authentication, automates rotation, and provides full auditing and policy control.

For developers, Idira Secrets Manager offers a consistent REST API interface and integration with DevOps tools, making it easier to write portable, infrastructure-independent application code. Teams can standardize how they access secrets across environments—without rewriting code for each cloud platform or on-premises deployment.

By unifying secrets management across hybrid infrastructure, Idira Secrets Manager helps organizations eliminate silos, reduce operational complexity, and maintain centralized control over their most sensitive credentials.

Use Case 2:

Unify Secrets Governance and Visibility Across Native Cloud Vaults

Most cloud platforms offer their own secrets management tools. Managing secrets across multiple providers, however, often leads to vault sprawl and security silos, especially when teams need to manage application secrets that live outside the cloud provider's ecosystem, such as on another cloud platform or on-premises.

These silos result in fragmented visibility, inconsistent security policies, and limited auditability. Native tools often lack the centralized control and lifecycle automation needed to meet enterprise security and compliance standards. Developers, meanwhile, are burdened with managing secrets across disparate tools, slowing workflows, and increasing the risk of misconfiguration or hard-coded secrets.

Idira Secrets Hub helps organizations gain centralized governance and control over secrets stored in cloud-native vaults like AWS Secrets Manager—without disrupting developer workflows. It integrates directly with native cloud provider APIs to enable centralized discovery, rotation, and auditing of secrets, while allowing developers to continue using the tools they already know and prefer.

In addition to centralized management, Idira Secrets Hub includes built-in cloud-native secrets scanning and discovery capabilities to identify unmanaged, orphaned, or misconfigured secrets across their cloud environments—closing security gaps that native tools often miss. With Idira Secrets Hub, you can:

- **Discover and assess secrets-related risk** across cloud-native vaults and services.
- **Reduce vault sprawl** by syncing secrets into a centralized control plane.
- **Unify policies and enforce automated rotation** across multicloud and hybrid environments.
- **Improve compliance** with centralized audit trails and policy enforcement.
- **Preserve developer velocity** by working seamlessly with native secrets tools and APIs.

Security teams readily adopt Idira Secrets Hub to gain centralized oversight while enabling developers to maintain their preferred workflows.

Use case 3:

Secure Secrets for COTS and Traditional Applications at Scale

Many organizations still rely on a mix of on-premises applications, commercial off-the-shelf (COTS) tools, and long-lived, internally developed systems—including vulnerability scanners, IT automation platforms, RPA tools, and mainframes. These applications often form the backbone of enterprise infrastructure, supporting critical operations that are difficult to be rearchitected or moved to the cloud.

Yet, these environments are often overlooked when it comes to secrets management. Hard-coded credentials, manual processes, and inconsistent policies create persistent security gaps—leaving privileged access unmanaged and difficult to audit.

Idira Credential Providers offer a centralized, policy-based solution to secure secrets in static, long-lived, and on-premises environments. They eliminate hard-coded credentials by brokering secure, JIT access to secrets stored in Idira—all without requiring changes to application code or workflows.

With support for a wide range of COTS integrations; operating systems including Windows, Linux or UNIX, and z/OS; and enterprise dev stacks including Java and .NET, Idira Credential Providers are purpose-built for environments that demand stability, scalability, and control. With Idira Credential Providers, organizations can:

- **Eliminate hard-coded credentials** in traditional and on-premises applications.
- **Secure privileged access** for COTS tools without relying on vendor-native secrets managers.
- **Automate credential rotation** without disrupting critical systems.
- **Improve compliance and reduce audit risk** through centralized policy enforcement and visibility.
- **Support critical infrastructure** across hybrid IT with proven, enterprise-grade integrations.

Idira Credential Providers help secure the systems that keep your business running—giving you the control and consistency needed to protect high-value infrastructure at enterprise scale.

A Unified Approach to Secrets Management

Idira's secrets management products—Idira Secrets Manager, Idira Secrets Hub, and Idira Credential Providers—are part of the broader Idira Identity Security Platform. While each product addresses a specific challenge, they are most powerful when used together to secure secrets across the entire application landscape.

Many organizations use more than one Idira solution to support hybrid environments. For example, a team might use:

- **Idira Secrets Manager** to secure dynamic cloud-native workloads.
- **Idira Secrets Hub** to extend visibility into AWS or Azure secrets.
- **Idira Credential Providers** to protect applications that cannot easily be refactored.

These tools are built to work together—sharing identity context, enforcing consistent policies, and consolidating audit trails.

John Walsh, Idira senior product marketing manager, explains this collaborative philosophy, "I think for us, the challenge is when customers hear about our multiple products. We like to explain how this becomes the solution because it will never be either/or, but rather a mix of solutions depending on what fits your organization's particular environment and specific needs."

“Customers often assume they need to choose a single solution, but in practice, the strongest security outcomes come from using a combination.”

—John Walsh, Idira Senior Product Marketing Manager, Palo Alto Networks

Getting Started

Where you begin depends on your current environment, architecture, and operational maturity—not your industry. “Product selection is definitely not industry-dependent, as it’s really about the maturity of your business rather than what particular industry you’re in,” explains Walsh.

Organizations with modern DevOps pipelines and cloud-first strategies might prioritize Idira Secrets Manager and Idira Secrets Hub. Others with established systems that rely on manual credential handling may see immediate value from starting with Idira Credential Providers.

Many organizations start with one or two products and expand over time as their security strategy evolves. Idira’s modular approach makes it easy to scale without rearchitecting your environment.

Conclusion

Secrets are everywhere—across cloud-native apps, on-premises workloads, CI/CD pipelines, and third-party tools. Managing them securely, consistently, and at scale requires more than a one-size-fits-all solution.

Idira delivers a unified approach to secrets management that grows with your organization. By aligning developers and security teams around flexible, purpose-built tools, Idira helps secure machine identities across any environment—without disrupting how teams build and deploy.

Explore all the ways Idira can secure the identities across your organization. [Request a demo.](#)

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_wp_three-critical-use-cases-for-enterprise-secrets-mgmt_050126