ISS Identity Lifecycle Management (ILM)

Secrets

Secure, Centralized Secrets Management for Modern Enterprise and Cloud Environments

ISS ILM – Secrets is a service-based secrets management solution that securely stores, controls, distributes, rotates, and audits secrets across enterprise, cloud, DevOps, and hybrid environments. It enables organizations to manage passwords, application secrets, tokens, and machine credentials as governed lifecycle assets - reducing risk, operational overhead, and credential sprawl.

The Problem

Secrets underpin nearly every modern digital interaction - applications, APIs, CI/CD pipelines, cloud services, and machine-to-machine communication. Yet they remain one of the most common sources of security incidents. **39% of data breaches involve stolen or compromised credentials,** and credential-based breaches take longer to detect and cost more to remediate. In fact, **compromised credentials are the leading initial access vector, responsible for up to 75% of investigated breaches.**

Secrets sprawl is accelerating. **16 billion compromised credentials** are circulating globally, hard-coded secrets in public repositories continue to rise, and cloud and SaaS adoption multiplies exposure points.

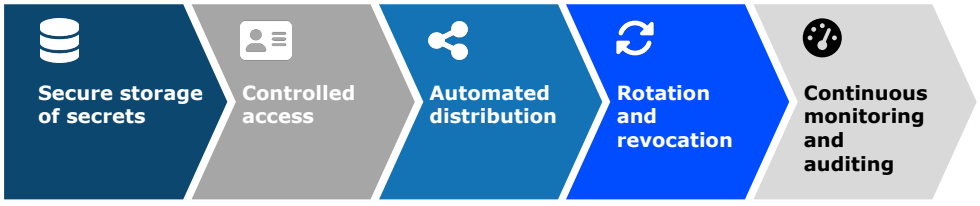
Despite their critical role, secrets are often scattered across tools and environments, hard-coded or long-lived, manually managed, and locked into vendor-specific platforms, leaving organizations without centralized visibility or control. As automation and cloud-native architectures scale, unmanaged secrets become a major **security, compliance, and operational risk.**

OUR SOLUTION – ILM Secrets

ISS ILM Secrets provides a centralized, policy-driven approach to secrets lifecycle management. It abstracts secrets handling into reusable services that enable secure access without exposing credentials, while maintaining strong governance and auditability. By treating secrets as lifecycle-managed trust assets, not static configuration data - ILM Secrets enables organizations to:

- Securely store and protect secrets using modern encryption
- Control and enforce least-privilege access
- Automate secret distribution to applications and services
- Rotate and revoke secrets without service disruption
- Continuously monitor and audit secret usage

The result is reduced operational friction, improved security posture, and consistent secrets governance across environments.



What Are Secrets?

ILM Secrets manages confidential values whose exposure would grant unauthorized access or capability, including:

- Application and API credentials
- Service account passwords
- Database passwords
- Cloud access keys
- OAuth client secrets and tokens
- CI/CD pipeline secrets
- Service-to-service authentication secrets

Passwords and management of the explosion of **non-human, machine, and application secrets** are covered.

DISCOVER

Identify where secrets exist across applications, pipelines, and systems to understand usage and exposure.

PLAN

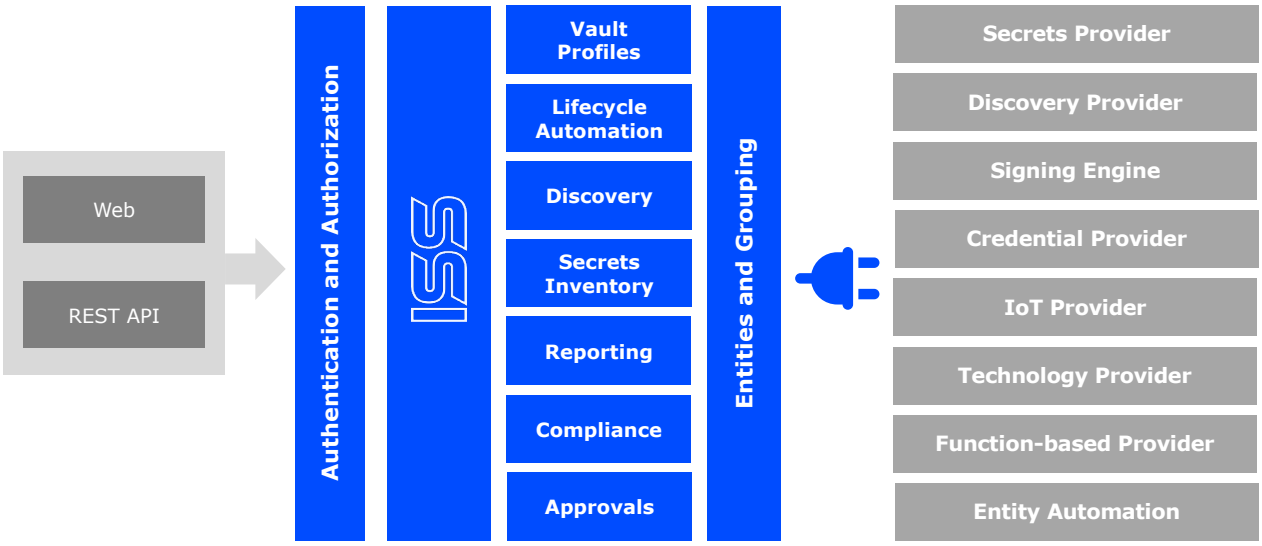
Define policies, access controls, and rotation requirements based on risk, compliance, and operational needs.

IMPLEMENT

Securely store secrets, automate distribution, and integrate secrets into applications and workflows.

MONITOR

Continuously audit access, usage, rotation status, and compliance through centralized monitoring and reporting.



KEY BENEFITS

- **Security** – Protect sensitive credentials with centralized control and strong encryption
- **Control** – Enforce least-privilege access and separation of duties
- **Automation** – Reduce manual handling with automated distribution and rotation
- **Reliability** – Prevent outages caused by expired or mismanaged secrets
- **Visibility** – Gain centralized insight into where secrets are used and by whom
- **Compliance** – Support audit and regulatory requirements with full traceability
- **Flexibility** – Avoid vendor lock-in with an open, service-based architecture

Deployment Flexibility: Open, Vendor-Agnostic Architecture - ILM Secrets integrates across cloud, on-premises, and hybrid environments without vendor lock-in. Its API-first design enables seamless integration with existing security, DevOps, and platform tools, ensuring secrets are managed consistently as infrastructure and applications evolve.