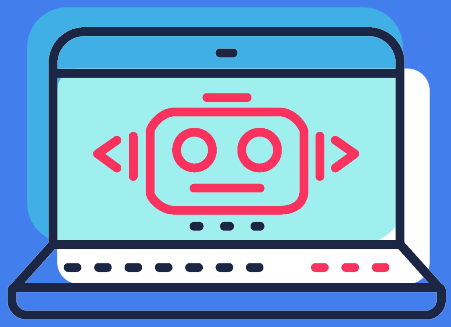
transmit security

SERVICE BRIEF

Secure & Unified Machine Identity Management

Modernize secrets management with a **unified & live view** of machines and **risk-based, actionable workflows.**



The exponential growth of non-human entities with access to sensitive data is a critical security threat. Minimize risk with just-in-time enrollment & unified, trackable machine identities.

Challenge

Diverse non-human entities with critical access outnumber humans 50x
Applications, devices, containers & bots are growing rapidly, with access to business-critical workloads that must be highly secure and resilient.

Static provisioning of machine identities is cumbersome & complex
A proliferation of identities complicates provisioning & management with infrastructure-as-code tools, especially in hybrid & multicloud environments.

Unified identity tracking is non-existent to minimal
Without a single source of truth, it can be difficult to know which identities are assigned to which machines, making it hard to update & revoke credentials.

Lack of control & implementation problems create security vulnerabilities
Low visibility, complexity & poor protection of "secret zero," which uses single-factor authentication to access stored secrets, present growing risks.

Solution

Transmit Security Machine Identity Management replaces static provisioning with dynamic, just-in-time enrollment and provides unified, continuous visibility and control to strengthen security and eliminate blind spots.

- **A single, trackable identity** unifies multiple identities with existing certificates from cloud providers.
- **Secret zero access is limited** to the control plane, restricting the use of persistent identities and preventing attacks on the data plane, which is more frequently targeted and less secured.
- **Out of the box, pre-integrated secrets management** with simple access policies are available as SaaS with platform secrets already in it.
- **Low-to-no-code orchestration** enables risk-based, actionable workflows for all components in the machine identity ecosystem.

Key Benefits

Simplified integration

Short-lived access to tokens for data & compute workloads enables easy integration with existing stacks and security backends.

Enhanced visibility

A single source of truth for monitoring of machine IDs with full visibility into peers, secrets, enrollment tickets & activities.

Reduced complexity

Dynamic, just-in-time enrollment simplifies provisioning while unified access & low-to-no-code orchestration makes it easy to create actionable workflows across services.

Assured compliance

Better control over 3rd party usage with risk, audit & posture advisory enables zero-trust security and ensures compliance with industry regulations.

Stronger security

Limited access to secret zero, strong ID of machines via multiple factors & automatic revocation of compromised machines fortifies security posture.

Use cases

The market has only recently defined machine identity management, and many organizations are still struggling to solve the problems surrounding it. With Transmit Security's Machine Identity Management, businesses can:

1. **Manage identities** by leveraging just-in-time IDs provided by the service or unifying existing identities.
2. **Store & manage secrets** using our standalone secret store or reduce fragmentation by integrating with your existing secrets management tools.
3. **Track usage** of machine identities, secrets, workload runtime information and availability.
4. **Implement authorization policies** that are simple yet expressive to enable role-based access control for multiple stakeholders.
5. **Support & orchestrate workflows** for managing identities and permissions with actionable indicators to detect and mitigate risk in real time across hybrid and multicloud environments.

Fraud detection & response for machine identities

Most machine identity management solutions focus solely on credentialing, basic authorization and authentication, building static policies using basic metadata and only checking periodically for compromised identities. This creates a window in which attackers can use stolen certificates or API keys to access sensitive data or resources, launch malware attacks or hijack overly permissioned identities to move laterally across environments.

Transmit Security's Machine Identity Management reduces these risks by wrapping its services with fraud detection and response that automatically detects compromised identities and revokes authorization before fraudsters have time to exploit stolen credentials.

Key Features

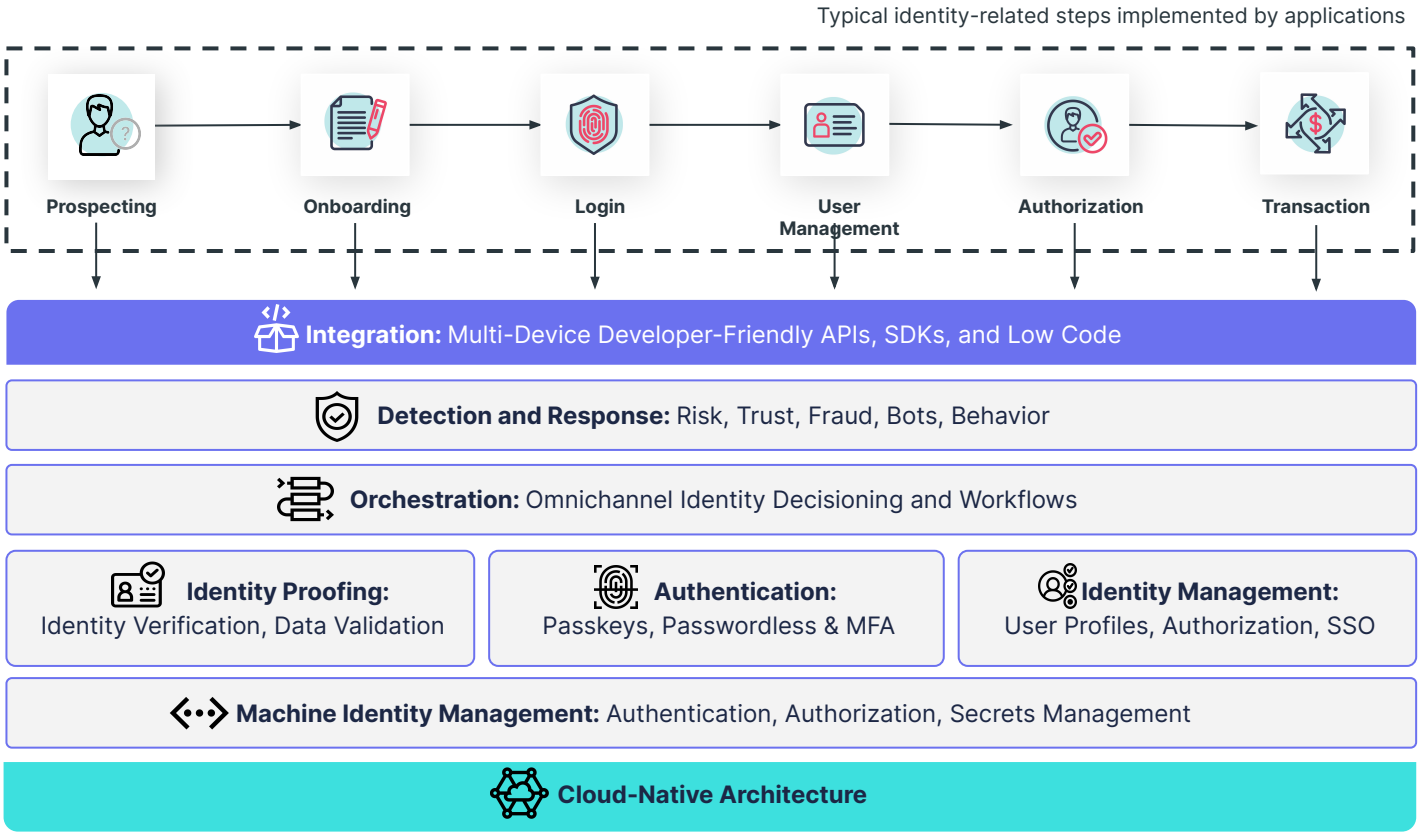
- **Flexible implementation** as a standalone or BYO secret store
- **Single source of truth** for machine identities and roles
- **Just-in-time IDs** and short-lived access to tokens
- **Unified access** across the entire fleet for an enterprise-wide strategy
- **Risk-based workflows** for multiple stakeholders
- **Liveness monitoring** with automatic revocation of unused identities
- **No-code & low-code** workflow orchestration across environments, including hybrid and multicloud
- **Ad-hoc VPN** with multiparty detection automatically revokes compromised machines
- **SaaS platform** is purpose-built to support modern runtime environments and development workflows

kuppingercole ANALYSTS

Transmit Security Named 'Overall Leader'
in three ranking reports: Fraud Reduction Intelligence, Passwordless Authentication and CIAM Platforms.

Native integration with modular, plug-and-play CIAM services

Machine Identity Management provides lifecycle support that is fully integrated into a complete, modular and security-first platform. This enables end-to-end protection with easy access to a full suite of pre-configured identity services, underpinned by orchestration capabilities that are used in production by 8 of the top 10 global banks and proven to scale to 100 million users. Developer-friendly APIs and SDKs make it easy to close security gaps, improve visibility and gain control with a few lines of code.



Secret storing is only one aspect of machine identity.
Maintaining digital trust requires dynamic adaption to risk and trust signals to continuously establish digital identities throughout the entire lifecycle, from enrollment to revocation.

Explore our full CIAM Platform

- Identity Verification
- Detection & Response
- Orchestration
- Identity Management
- Authentication
- Data Validation
- Machine Identity Management

About Transmit Security

Transmit Security gives businesses modern tools to deliver secure and trusted end-to-end identity journeys. The Transmit Security CIAM Platform is security-first, developer-friendly and modern to provide customers with smooth experiences and prevent fraud across all channels and devices. Transmit Security serves many of the world's largest banks, insurers, retailers and other leading brands, collectively responsible for more than $2 trillion in annual commerce. For more information, please visit **www.transmitsecurity.com**.