token

The intersection of AI, PHI & non-human identity security

Learn how Token Security helped an online mental health provider achieve non-human identity security to protect personal health information (PHI) for its more than 5 million online therapy clients.

Overview

A provider of online-based mental health services recognized that agentic AI could play a pivotal role across the organization. However, for an organization noted for creating safe spaces for users to explore their mental health with licensed therapists, even a single data breach could be catastrophic. Additionally, incorporating agentic AI and related non-human identities within the organization created additional security concerns that overlapped with their need to remain compliant in its heavily regulated industry. For example, shadow AI—auto-enabled AI features in tools that keeps reappearing—was a big concern. Enter Token Security, the only non-human identity (NHI) security platform purpose-built for AI agents.

Beyond IAM: The emerging security challenges of AI agent proliferation

Enterprises deploying AI face challenges that Identity Access Management (IAM) and Privileged Access Management (PAM) cannot solve. AI agents and Model Context Protocol (MCP) servers can be spun up and decommissioned rapidly, creating vast unmanaged identity inventories known as Agent & Identity Sprawl.

About Customer

A leading online mental health provider was founded over a decade ago to remove traditional barriers to therapy to make mental health more accessible to all. Today, they are providing professional, affordable, and personalized therapy in a convenient online format. Their network of licensed therapists has helped millions of people take ownership of their mental health and work toward their personal goals.

aws PARTNER

Continuous autonomous operation can lead to unpredictable behavior of AI agents—the system takes on a life of its own—complicating anomaly detection and monitoring. There can be privilege overreach where determining the correct level of access for non-deterministic agents is difficult, leading to over-provisioning. The compromise of one AI agent can ripple across interconnected systems to increase the blast radius of security events. All the while, static API keys and tokens remain invisible to SSO, MFA, and traditional IAM enforcement as organizations struggle to extend zero trust and compliance frameworks to agentic AI ecosystems.

This provider's online platform is running on Amazon Web Services (AWS) infrastructure that is extremely sensitive when it comes to protecting user data. At the same time, they wanted to adopt agentic AI across the organization to support innovation, efficiency, and the user experience. The company believed it had a fairly good lock on employee access into customer data, but when they completed a threat assessment, they recognized two sets of vulnerabilities: third party access to their environment and privileged workloads that could access all the platform's data. In particular, interconnectedness of their development, staging, and production environments allowed too much cross-account access. Additionally, the company relied almost entirely on default IAM tools which could not achieve their specialized NHI security needs.

Token Security: Managing autonomous AI identities before they start to wander

After a period of search and due diligence for a robust solution, the online mental health provider selected Token Security because it offers the only NHI security platform purpose-built for AI agents. Token Security offers contextual awareness via insights into the interconnectedness of agents, identities, secrets, and services. End-to-end identity lifecycle control means full management over discovery, ownership, and retirement of AI agents and identities. Context decisioning to safely remediate issues without breaking workloads or exposing vulnerabilities allows for intelligent remediation at scale. The platform also extends enforcement of strict least-privilege models for AI agents and other non-human identities as a governance asset while automated, policy-driven threat detection that neutralizes compromised or misbehaving AI agents in seconds delivers real-time detection/response capabilities.

> **"Token Security gave me instant visibility into all NHIs in just seconds, but more importantly, it allowed me to quickly resolve issues and automate remediation effortlessly."**
>
> VP & Head of Cybersecurity

Moreover, Token Security works across the AI agent identity layer to mitigate shadow AI via continuous discovery and contextual inventory of all AI agents, custom GPTs, and servers. The system ensures assigning of clear ownership of NHIs while also enforcing credential rotation and managing decommissioning. Access control and right sizing are established via enforced least privilege and intent-based permission access with continuous evaluation. The platform also helps companies like the online mental health provider in heavily regulated industries engage comprehensive activity logging to provide traceability across multi-agent ecosystems for audit, compliance, and incident response. As but one example of the value Token Security brought to this provider, the platform almost instantly eliminated more than 25% of the company's NHI identity vulnerabilities. Many of these are created and accumulate over years of engineers and other teams creating projects that after resolution of the project the identities were not decommissioned.

Additionally, only Token Security has one leg inside AWS monitoring (identities, activities, entitlements, etc.) and another monitoring the AI agents to provide governance, deep observability, and that helps build the correct policy. What's more, by integrating data from AI coding platforms such as Cursor, Cloud Code, or GitHub Copilot into data captured in AWS, Token Security is able to layer on top of basic AWS identity management to provide comprehensive, enhanced security. This capability speaks to the importance of Token Security's partnership with AWS. Deep integration with AWS security services helps Token Security extend zero trust and identity governance to AI agents for security and compliance alignment. More than that, Amazon Bedrock provides AI capabilities customers rely on while the NHI security platform secures the identities those workloads use. Amazon Web Services global scale supports rapid discovery and remediation across massive, dynamic ecosystems to deliver elastic scalability.

28%

of identity vulnerabilities immediately eliminated

Continuous compliance

with evolving AI security regulations

Reduced attack surface

and minimized blast radius for compromised agents

Secure integration

of AI-driven innovation at enterprise scale

The outcome: AI adoption with holistic NHI security

With AWS, Token Security helps enterprises like this online mental health provider accelerate AI adoption securely to reduce the time to value while addressing risk and maintaining compliance. Companies will neutralize existent AI-driven NHI threats in seconds rather than weeks or months. Meanwhile, continuous compliance is achieved by automating auditability and AI agent traceability across cloud and AI environments. The Token Security platform also supports cloud transformations and M&A by extending governance seamlessly across hybrid AWS environments. Zero trust frameworks extend to non-human identities, governance evolves with ever adapting AI regulations, the attack surface is reduced, and blast radius of compromised agents is minimized. In all, Token Security helps companies with unique NHI security concerns integrate AI-driven innovation at enterprise scale.

About AWS Partner Token Security

Token Security—based in Tel-Aviv, Israel—is a NHI (Non-Human Identity) security platform accelerating secure enterprise adoption of agentic AI by discovering, managing, and governing every AI agent and non-human identity across an organization. From continuous visibility to least-privilege enforcement and lifecycle management, Token Security provides complete control over AI and machine identities, eliminating blind spots, reducing risk, and ensuring compliance at scale. Token Security enables enterprises to protect the invisible and rapidly growing layer of AI agents and non-human identities to ensure AI operates with zero trust security boundaries and compliance frameworks.

To learn more, visit token.security