PLEASE REGISTER AT THE FRONT: AGENT REGISTRIES AND AGENTIC AI AS GARANTIR'S FIFTH PILLAR OF DIGITAL TRUST

Garantir's recent Agentic Artificial Intelligence (AI) announcement demonstrates the critical role of cryptographic service providers in the burgeoning agentic security market, but also indicates how agent registries, alone, remain only a first step in securing control and governance.

NEWS

GARANTIR ANNOUNCES AGENTIC AI SECURITY AS THE FIFTH PILLAR OF DIGITAL TRUST WITHIN THE GARATRUST PLATFORM

Breakout star in digital trust, Garantir, provides myriad cryptographic services within its broader GaraTrust platform, including, as of July 2026, security for Artificial Intelligence (AI) agents. Each of GaraTrust's cryptographic offerings corresponds to one of (now) five pillars: data security, passwordless authentication, certificate management and Public Key Infrastructure (PKI), software supply chain security, and agentic security. In terms of cryptographic functionality, the announcement does not represent the launch of a new point solution, new capabilities, or radical departure from Garantir's brand positioning, instead amounting to a strategic proclamation of the applicability of Garantir's existing cryptographic portfolio to Agentic AI.

In its approach to agentic security, using delegated key and certificate access, Garantir will enable agents to perform cryptographic operations such as authentication and encryption, and will support agent registration as a Non-Human Identity (NHI) through dynamic enrollment and ephemeral attestation, backed by signed, Security Information and Event Management (SIEM)-verifiable records that contextualize agents based on users and scope. Meanwhile, GaraTrust enables Hardware Security Module (HSM) signing of agentic actions via a Model Context Protocol (MCP) wrapper, relying on Just-in-Time (JIT) access, Multi-Factor Authentication (MFA), or quorum-based access to delegate agent access, supporting short-lived credentials per session. These same step-up controls also support a human-in-the-loop model, inserting a required human approval at the point of key access before higher-risk agentic actions can proceed.

The announcement coincides with a flurry of activity across the cryptographic services, identity and NHI, and broader digital security markets, as well as within leading standardization bodies and national governments. Of particular note are the recent statements from the Estonian government regarding the establishment of an AI agent registry, coupling registered agents with official government ID numbers. Strategic Outcomes for Garantir and the Broader Cryptographic Services Market

IMPACT

STRATEGIC OUTCOMES FOR GARANTIR AND THE BROADER CRYPTOGRAPHIC SERVICES MARKET

By translating its expertise in delegated key and certificate access, Garantir is explicitly extending its suite of cryptographic services to the agentic realm, flagging the synergies between traditional cryptographic operations such as code or digital signing of cryptographic objects to governance of agentic parameters via signing, cryptographic binding, and tokenization. This pivot in market positioning to encompass agentic security is a strategic decision that reflects a constructive new market position for Garantir. Agentic security is a fast-growing segment with lucrative prospects for vendors across security subsegments.

Garantir's recent announcement not only sets the stage for its continued expansion but supports a healthy demand trajectory as it pertains to long-term revenue opportunities. By tying this new fifth pillar to its standing capabilities, Garantir offers agentic security without the need for customers to integrate those capabilities separately or purchase new products, rather this process is simplified to augmenting existing GaraTrust deployments with additional licensable modules. The ease of integration here and absence of any rip-and-replace or agent code changes is set to accelerate uptake; a positive indicator for future earnings and sustained growth for Garantir.

Some of Garantir's core differentiators that are favorable for long-term prospects include how it built its solution from the ground up on cryptographic primitives rather than limiting it to Secure Shell (SSH) solutions. Further, Garantir operates below the application layer, which is significant in the agentic context where agents operate as the application itself, securing agents from the same attacks that OAuth-based defenses and gateways are vulnerable to. In this way, Garantir's offering is a step ahead of much of its peers in agentic security in two ways. First, by operating below the application layer, Garantir's is aligned with increasing customer migration to application-level encryption rather than storage level. Second, in the context of the budding agentic security marketplace, Garantir's offering moves beyond the vogue around AI agent registries, conjoining the notion of an agentic registry with the cryptographic governance demanded to meaningfully complete the access control and comprehensive security story for agents. This move is key in signaling the importance of the visibility provided by agent registries, but equally the importance of going beyond the inventory stage.

RECOMMENDATION

BEYOND REGISTRIES: CONTROL OF AI AGENTS EXTENDS BEYOND INVENTORY AND VISIBILITY

Agent registry offerings are rife with emerging standards and protocols pertaining to agent inventory (e.g., Google's Agent2Agent (A2A) protocol and Registry, IETF's Agent Name Service (ANS) proposal) and orchestration (e.g., MCP and Agent Communication Protocol (ACP)). Further, the Estonian government's June 16 announcement about registering agents coupled with national IDs demonstrates the pronounced emphasis on registries in agentic security. Yet, Garantir's approach goes a step further by providing registration coupled with actualized control of agent access and behavior, lifting the veil on the illusion of security that agent registries accord organizations while demonstrating to the wider industry that agent registries initiatives must be fused with corresponding access control mechanisms going forward. Learning from the work of Garantir and in the context of the emerging agentic security market, considerations and takeaways for market players existing in this space or moving into it include the following:

- Look to Existing Feature-Sets Before Reinventing the Wheel: While there are certainly technology-specific elements to agentic security, as shown by Garantir, pre-existing security methods and capabilities remain relevant and should not be discounted. Understanding and appreciating that agentic security remains just as much as a new marketing and security messaging journey as a technological pursuit is key to building streamlined solutions that integrate with existing security estates, while catering to the tech-specific challenges posed by AI agents. Vendors would be remiss in not taking their core functions and cross applying those to Agentic AI given the opportunities that brings for expansion and unlocking new revenue streams. Adaptability can win out innovation in set use cases. Yet, at the same time, concepts such as multi-hop delegation demand special attention, particularly given the issues they pose for agent registries. While current OAuth can handle single-hop delegation via On-Behalf-Of (OBO) tokens, where agents can subsequently create their own agents, multi-hop delegation issues rear their heads. Garantir is innovating in this space with OIDC On-Behalf-Of Flow to track agent delegation flows back to the original agent creator and configurations on the Large Language Model (LLM) itself to secure justifications for given actions (e.g., using a certain tool for a given prompt). Dynamic agent registration is another agent-specific issue, with static registries like MCP servers insufficient in terms of scale and cross-trust functionalities.

- Focus on Collaboration and Partnerships to Capitalize on the Emerging Agentic Security Market: Agentic security is in its infancy and, given the large prospective capital opportunities, faces a coalescence of vendors from various security backgrounds seeking to nab a piece of the pie. On the hardware-side, confidential computing and Trusted Execution Environments (TEEs) present interesting partnership opportunities for software-based enabling platforms, while the multi-faceted nature of agents themselves—sitting between human and machine workloads—presents prospects for Identity Access Management (IAM) providers, as well as cryptographic service providers like Garantir.
- Prioritize Standards Interoperability in Solution Development and Deployment: The landscape of inter-agent communication and agent orchestration protocols is dynamically evolving; thus, successful offerings should ensure integration of and interoperability with emerging standards. The most important standards underpinning agentic security include OAuth 2.0/2.1, OpenID Connect, SPIFFE/SPIRE, SCIM, NGAC, and MCP, although there are others. For cryptographic service providers, homing in on MCP first is key given its relevance in terms of delegated cryptography. Then, looking at A2A in the context of dynamically generated agents and runtime crypto identities will be important.
- Maximize Alignment with Ongoing Regulatory Efforts Where Possible: Agentic AI invites a hoard of legal issues that remain unclarified or underexplored, including liability issues under regimes such as the new Estonian proposal. Documentation of AI systems and their risk classifications as a whole is key under the AI Act and DORA, and while the EU AI Act has gone some of the way in prescribing liability to those who put "high risk" AI systems on the market, neither Act contains explicit delimitations for AI agents specifically. Given the documentation requirements and August 2026 deadline for compliance, AI agent inventories or registries remain the key first step. Yet, where registries are static and cannot keep pace with the dynamism of the agentic world, they are likely to fall below the Act's documentation benchmarks regarding AI system runtime. Thus, agentic security cannot stop at the registry.
- Monitor New Guidelines and Best Practices on a Global, Rather Than Strictly National Basis: Given the nascency of the agentic security space, best practices, guidelines, and standards regimes are in a state of fragmentation; emerging in different forms and with differing remits across regions and agencies. For example, while countries in Europe like the United Kingdom and Estonia have released guidelines on agent registries and signed agents, other national agencies have gone a step further, e.g., Australia's Digital Transformation Agency's Agentic AI Addendum—published June 4—mandating governing agent-to-agent data exchanges with authentication and encryption protocols, access controls such as least-privilege access, and continuous monitoring. Other agencies like the National Institute of Standards and Technology (NIST), while U.S.-based, tend to have an internationalized scope with regard to their influence. Closely monitoring the work of the NIST AI Agent Standards Initiative will be necessary to stay at the edge of market innovation.

Above all, ensuring that inventory-taking or agent registration happens in tandem with actionable ways of governing and controlling the actions and behaviors of those registered agents is critical. Agents may soon be required to register at the front desk, but watching their behavior within the building is equally important.