

Salt Security Introduces the Industry's Largest Policy Library for Agentic AI Governance

Industry-first milestone includes policies purpose-built for AI agent security, MCP, agent authorization, and corporate agentic-specific threat patterns

PALO ALTO, CA, UNITED STATES, July 20, 2026 /EINPresswire.com/ -- [Salt Security](#), the leader in

“

The board question CISOs are being asked right now is not whether we have AI governance. It is whether we can prove it.”

*Aner Gelman, VP of Products,
Salt Security*

API and Agentic Security, today announced that the Salt Policy Hub has reached 100 pre-built policies, creating what is effectively the industry's first app store for agentic security governance. As enterprises race to deploy [AI agents](#) across their organizations, the Policy Hub provides security teams with an immediately deployable library of governance policies spanning APIs, MCP servers, agent permissions, authentication, compliance and runtime behavior.

The milestone comes at a critical moment. Every AI agent depends on APIs to access data, invoke tools and take actions across enterprise systems. The infrastructure organizations have spent years securing for APIs has become the execution layer for agentic AI. As a result, API governance has become synonymous with agent governance, creating a need for security policies that extend across the entire agentic ecosystem rather than protecting individual components in isolation.

Rather than forcing organizations to build that governance framework from scratch, the Salt Policy Hub provides a library of enterprise-ready policies that can be activated immediately and customized to suit each organization's environment. Much like an app store provides trusted applications, the Policy Hub gives security teams access to proven governance policies covering the technologies that power modern AI agents, helping organizations adopt autonomous AI with confidence while maintaining security and compliance.

By the Numbers

- 100 pre-built policies covering data security, access control, OAuth, API architecture, MCP configuration, third-party risk and agentic security
- 61 policies activate automatically out of the box, providing immediate protection without configuration

- 12+ policies purpose-built for AI and agentic security, covering MCP server configuration, agent authorization and autonomous agent behavior
- Eight compliance frameworks mapped across the Policy Hub, including PCI DSS, FedRAMP, SOC 2, GDPR, HIPAA, ISO 27001, CMMC and HITECH
- Unlimited custom policies allowing organizations to extend governance with their own requirements
- Single-click activation for the remaining policies with no complex configuration required

The Policy Hub is a component of the Salt Agentic Security [Platform](#), which gives enterprises full visibility and governance across the Agentic Security Graph: the connected layers of LLMs, MCP servers, APIs, and integrated enterprise systems through which AI agents take action. The 100-policy milestone extends that governance framework from runtime protection into proactive posture management across the full agentic stack.

“When we launched the Policy Hub in 2024, the most common thing we heard from CISOs was: we know we need posture governance, but we have no idea where to start. That question was killing governance programs before they launched. 100 policies means that question now has a concrete answer. Security teams can walk in on day one with meaningful protection already active, and extend it from there without limit.”

Michael Callahan, VP of Strategy and CMO, Salt Security
Built for the Agentic Era

AI agents do not operate in isolation. They rely on APIs, MCP servers, identity systems and enterprise applications to gather information and perform actions. Securing AI therefore requires more than protecting models or prompts. It requires governing everything an agent can access and everything it is authorized to do.

Many of the policies within the Policy Hub were originally developed for API posture governance because APIs remain the foundation of every agentic workflow. As organizations adopt AI agents, those same controls naturally become part of a broader governance framework for the entire agentic ecosystem. Salt has continued to expand the Policy Hub alongside the rapid growth of agentic AI, adding policies that address MCP server misconfigurations, over-privileged agents, unauthorized agent actions and other emerging risks unique to autonomous systems. When Salt Security introduced MCP server discovery in September 2025, identifying and classifying MCP servers across enterprise environments, corresponding governance policies were developed in parallel. The Policy Hub continues to expand alongside the technologies that underpin agentic AI, ensuring organizations can govern new capabilities as quickly as they adopt them.

Salt Code, launched in June 2026, extends the same Posture Governance Engine into the software development lifecycle, applying governance policies to AI-generated code as it is created. This provides organizations with a consistent policy model spanning AI-generated software, APIs, agents and runtime behavior across the entire application lifecycle.

“The board question CISOs are being asked right now is not whether we have AI governance. It is whether we can prove it. 100 policies in active deployment is a concrete, operational answer to that question. Not a roadmap. Not a strategy. An active governance layer running today.”

Aner Gelman, VP of Products, Salt Security

Availability

The Salt Policy Hub is available to all Salt Security customers as part of the Salt Agentic Security Platform. All 100 pre-built policies are available today. Custom policy creation is available without limit. Organizations interested in evaluating the Salt Agentic Security Platform can request a demo at salt.security.

About Salt Security

Salt Security is the leading API and Agentic Security company, protecting the world’s most innovative enterprises from API and AI agent attacks. The Salt Security Agentic Security Platform secures the full agentic ecosystem, discovering all APIs, agents, and MCP connections, stopping attacks in real time, and eliminating vulnerabilities before they reach production. Salt Security was founded in 2016 and is backed by Sequoia Capital, S Capital, Tenaya Capital, Salesforce Ventures, Advent International, and other leading investors. For more information, visit www.saltsecurity.com.

Media Contact

Dr. Karl Bateson
karlb@salt.security

Karl T Bateson
DigitalPulse365
+ +1 6173066275
karl@digitalpulse365.com

This press release can be viewed online at: <https://www.einpresswire.com/article/928014854>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.