

When AI Acts Alone, You Need Identity to Maintain Control

Autonomous AI agents are reshaping industries, but their rise demands a new identity-centric approach to cybersecurity.

Agentic AI Adoption Is Accelerating

76%

of financial and software organizations expect to adopt agentic AI within the next 3 years.

Agentic AI builds on generative AI's potential to add **\$2.6–\$4.4 trillion** annually to the global economy.

Autonomy Taxonomy: 6 Emerging Types of AI Agents



KNOWLEDGE & RESEARCH
Provides information and analysis across domains



TASK
Performs simple, discrete actions triggered by workflows



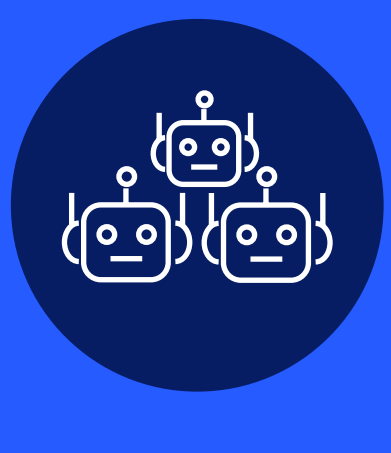
WORKFLOW
Executes multistep operations processes across systems



GOALS & PLANNING
Plans and determines execution paths to meet defined objectives



ORCHESTRATOR
Coordinates multiple agents or systems to optimize execution



PERSONABLE
Acts as virtual teammate with human-like interaction and decision-making

AI Agents Amplify Systemic Risks

Autonomy reshapes risks through decisioning, delegation, and information sharing—turning familiar security challenges into potential enterprise-wide exposures.

66%

of CISOs rank agentic AI among their top 3 cybersecurity risks.

TOP AGENTIC AI RISKS

Cross-agent task escalation (privilege escalation)

Untraceable data leakage (data exfiltration)

Synthetic identity risk (identity spoofing)

Chained vulnerabilities (supply chain flaws)

Propagation of corrupted data (data corruption)

Identity Is the Emerging Foundation for Securing AI Agents

As AI agents take on more enterprise tasks, identity will represent **nearly 25% of cybersecurity spend** within 3 years—more than network and application security combined.

10%

have deployed critical controls like agent registries and dynamic authorization at scale.

Mission-critical identity security controls include:

- ✓ Agent registries for tracking and credentialing
- ✓ Dynamic, just-in-time access permissions
- ✓ Continuous activity logs for traceability
- ✓ Built-in kill switches for containment

Who's in Charge of Agentic AI Security

CENTRALIZED (Chief AI Officer or AI Risk Committee)	FUNCTIONAL (CISO, CRO, CLO-Led)	FEDERATED (Business-Unit Led)
✓ Consistent standards and regulatory alignment	✓ Faster adoption aligned with established processes	✓ Flexibility where AI risks vary
✗ Slower execution due to review layers	✗ Gaps across data, tech, and ops boundaries	✗ Inconsistent standards and limited enterprise-wide visibility

Before your AI agents can operate safely, anchor autonomy to identity.