

September 2026 Cybersecurity Highlights



Cybersecurity - September 2026 Highlights

Key Developments

Runtime protection becomes central to AI agent security

- Security platforms are moving beyond AI inventory and governance toward runtime visibility and enforcement where agents actually execute.
- Emerging controls inspect agent behavior, tool calls, network activity, sensitive-data access, and downstream actions.

Zero Trust extends to agent traffic

Traditional user-and-device controls are expanding to on-behalf-of agent activity.

Organizations increasingly require:

- Discoverable agent identities
- Least-privilege access and workload identity
- Continuous policy enforcement
- Data-loss controls for agent-driven traffic

AI coding agents expand the endpoint attack surface

Coding agents can interact directly with:

- Source repositories and local files
- Terminals and command shells
- Credentials and API keys
- MCP tools, browsers, and external services

Agentic SOC moves into production

Security operations are increasingly combining human analysts with AI agents for investigation and response.

The focus is shifting toward:

- Unified telemetry across endpoint, identity, cloud, SaaS, and network
- Runtime guardrails and explainable agent actions
- Faster investigation and machine-speed containment

AI-assisted identity and phishing attacks remain high-impact

September research highlighted AI-assisted executive impersonation, device-code phishing, token theft, and cloud attacks using compromised service principals. Identity telemetry and session protection are increasingly important alongside endpoint controls.

Path Forward

Cybersecurity is shifting from:

Governing AI access →

Enforcing security continuously at agent runtime