October 2026 Cybersecurity Highlights



Key Developments

AI security moves from governance to runtime control

- 15 October: Palo Alto Networks introduced Prisma AIRS enhancements for Claude Enterprise, agent skills and MCP tool traffic, extending security controls into active AI workflows. [1]
- 21 October: SentinelOne unveiled Singularity Agentic Detection and Response to discover, monitor and constrain AI agents in real time. It launched in early access. [2]

Zero Trust expands to AI-agent identities

- 7 October: RSA announced Agent ID to register, govern and apply identity-based access controls to AI agents, including deployment options for regulated organisations. [3]
- 19 October: Microsoft expanded its agent-security approach with broader agent discovery, distinct Entra agent identities and risk-adaptive access controls. [4]

Data and AI protection become one platform priority

On 15 October, Proofpoint announced an agreement to acquire Varonis for approximately $6.3 billion, combining human, collaboration, data and AI security capabilities. The deal was announced, not completed. [5]

Agentic security operations mature into practical workflows

Cloudflare described an evidence-grounded, multi-agent investigation system inside Managed Defense on 7 October, combining alert context and human review. Tanium relaunched Security Operations on 6 October around behaviour-led detection, investigation and response at scale. [6, 7]

Human-risk protection shifts from training to adaptation

On 27 October, Proofpoint introduced a roadmap for User Risk Agents: one to profile, protect and coach high-risk users, and another to test exposure continuously. The first agent is planned for Q1 2027, rather than already generally available. [8]

Post-quantum security becomes an enterprise migration programme

On 27 October, NIST released its transition roadmap for post-quantum cryptography, while IBM announced its Quantum Safe suite for discovery, assessment and migration planning. The UK NCSC updated its post-quantum TLS guidance on 15 October. [9-11]

Path Forward

Cybersecurity is shifting from:

Standalone defence tools and static access rules →

Continuous, identity-led control across people, agents, data and cryptography.

Strategic priorities: Establish an AI-agent inventory and ownership model; test policy enforcement at runtime; retain evidence and human oversight in AI-assisted security operations; and begin cryptographic discovery for quantum readiness.

Selected October sources (click to open)

[1] Palo Alto Networks | 15 Oct

[2] SentinelOne | 21 Oct

[3] RSA | 7 Oct

[4] Microsoft Security | 19 Oct

[5] Proofpoint | 15 Oct

[6] Cloudflare | 7 Oct

[7] Tanium | 6 Oct

[8] Proofpoint | 27 Oct

[9] NIST | 27 Oct

[10] IBM | 27 Oct

[11] UK NCSC | 15 Oct