AI threats are prompting a shift in thinking in cybersecurity — one that focuses on interactions. Enterprises are realizing that approaching security as a way of protecting set assets in fixed places is no longer sufficient. They need to apply protections to all interactions between their workforce, their applications and APIs, and their infrastructure. What's more they need to maintain those protections as work moves through the organization. It requires a coordinated, layered approach.

The redefined threat: How AI accelerates lateral movement

With traditional cyberattacks, lateral movement required patience. An attacker compromised an endpoint, established persistence, and carefully issued commands to map the surrounding network without raising red flags.

AI-driven tactics have compressed this timeline down to seconds.

Traditional lateral movement flow

Initial compromise → Manual reconnaissance (weeks/months) → Probe RDP/SMB → Exfiltrate data

AI-accelerated lateral movement flow

Initial compromise → Automated LLM reconnaissance (seconds) → Exploit identities/agents

The 29-minute breakout window

According to the CrowdStrike 2026 Global Threat Report[3], the average global "breakout time" — the window between initial system access and lateral movement into adjacent workloads — has plummeted to just 29 minutes, with the fastest observed breakout occurring in a mere 27 seconds.

Attackers no longer rely on noisy, custom malware that triggers endpoint detection and response (EDR) agents. Instead, 82% of observed intrusions are malware-free. Adversaries harvest valid credentials and exploit native administrative protocols — such as remote desktop protocol (RDP), server message block (SMB), and secure shell (SSH) — to traverse flat internal networks.

The financial stakes of uncontained breaches

When internal systems implicitly trust one another, a single compromised laptop in an enterprise network can provide an attacker with direct pathways into core databases, Active Directory, and operational technology (OT) networks.

[3] *CrowdStrike 2026 Global Threat Report*