

Active Threat Assessment (ATA)

From Illumio & IBM

Evaluate your readiness against agentic-enabled threats
Stop Hiding. Start Hunting.

The New Threat Landscape

Organizations today must not only defend against a broad spectrum of cybersecurity threats, but also contend with a new generation of attackers using frontier AI models. These models represent a step change in offensive capability, which can dramatically lower the time, cost, and expertise required to carry out sophisticated attacks and push organizations toward continuous business disruption.

As attacks move at machine speed, security programs built on fragmented tools and manual processes are increasingly outmatched. Defending against agentic adversaries will require security programs that are autonomous and coordinated at scale.

In today's landscape, it's not a matter of *if*, but *when*. Standard security tools often miss sophisticated, AI-driven attacks or misconfigurations that provide easy entry for bad actors. In an agentic threat environment, defensive advantage no longer comes from individual tools, but from how quickly and coherently security programs can act.

How We Can Help

Together, Illumio and IBM are committed to helping organizations prepare for this critical inflection point in cybersecurity where resilience must match machine speed.

Leveraging Illumio's best-in-class segmentation platform and IBM's award-winning X-Force global Incident Response team, we use a data-driven approach to map your entire attack surface to identify:

- **Hidden Compromises:** We identify malware, unauthorized access, and persistent mechanisms already in your environment.
- **Ransomware Readiness:** A specialized evaluation of your ability to resist and recover from modern extortion tactics.
- **Vulnerability Mapping:** Identification of high-risk misconfigurations, unpatched systems, and policy gaps.
- **AI Exposure:** Visibility into how your AI models and environments might be exploited by "agentic" attack vectors.

Getting Started

The **Active Threat Assessment** is delivered in a three-phase approach:

1. **Environment Discovery & Scanning:** We deploy proprietary tools to analyze your endpoints, assets, network traffic, and cloud environments without disrupting operations.
2. **Expert Analysis & Threat Hunting:** IBM X-Force hunters analyze the data to distinguish between normal business noise and genuine malicious activity.
3. **The ATA Briefing:** You receive a comprehensive report featuring an executive summary of risk posture, technical details of any discovered threats, and a prioritized remediation "hit list" of exactly what to fix first.

Ready to secure your future?

Don't wait for a breach to find your weaknesses.
Contact IBM@illumio.com to schedule your assessment today.

Fast Facts

- **44% Increase in Exploitation:** A sharp rise in attacks targeting public-facing applications (40% of incidents in 2025).
- **Credential Harvesting:** The top impact from attacks, with 300,000 ChatGPT credentials exposed in 2025.
- **Agentic Threats:** The rise of AI agents that can, once inside a system, move laterally and identify assets with little human intervention.
- **48% of cybersecurity professionals** identify agentic AI as the most dangerous attack vector entering 2026.

Key Components

The **IBM X-Force Active Threat Assessment** identifies vulnerabilities across increasingly complex IT environments, with a particular focus on exposure to AI-driven threats for:

- ✓ **Deep Visibility:** Identifying security gaps, policy weaknesses, and AI-specific exposures.
- ✓ **Exploit Path Mapping:** Pinpointing potential paths attackers could take through the network.
- ✓ **Mitigation Guidance:** Providing prioritized, actionable advice to fix vulnerabilities, including interim safeguards when immediate patches are unavailable.
- ✓ **Automation Focus:** Highlighting opportunities to improve detection and response through better AI-driven automation.

"Frontier models are creating a new category of enterprise threat that is fast moving, systemic and increasingly autonomous"

"Meeting that threat requires a systemic defense. AI powered offense demands AI powered defense. That's what IBM is delivering."

Mark Hughes
Global Managing Partner
of Cybersecurity Services
IBM Consulting

About Illumio



Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments — stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

Copyright © 2026 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.