XM Cyber | SOLUTION BRIEF

Continuous Exposure Management for the AI Attack Surface

Secure AI innovation by unifying AI discovery with your broader Continuous Exposure Management strategy for a holistic view of hybrid risk. Proactively prioritize and sever validated attack paths connecting AI workloads to your critical assets by assessing AI exposures alongside traditional vulnerabilities and identity risks.

The rapid evolution of AI has sparked a global race to innovate, with organizations investing heavily in AI-powered workflows to drive business growth. This breakneck pace of adoption often bypasses traditional security gates, leaving CISOs flying blind to AI usage and scrambling to implement retroactive controls. At the same time, attackers are weaponizing AI to orchestrate sophisticated threat vectors and compress time-to-exploit from days to mere minutes. As regulatory bodies and security leaders struggle to keep pace, the core challenge remains: how to embrace AI innovation without increasing organizational risk.

XM Cyber empowers organizations to embrace AI innovation without compromise. By unifying AI discovery within our broader Continuous Exposure Management platform, we eliminate shadow AI and assess configuration impacts alongside identity risks. Our platform uniquely secures identity-driven orchestration layers, proactively severing attack paths where hijacked, over-privileged roles target your models or data. We ensure AI-enabled attackers cannot exploit these exposures, protecting your most critical assets across the hybrid enterprise.

Visualize the AI Attack Surface:

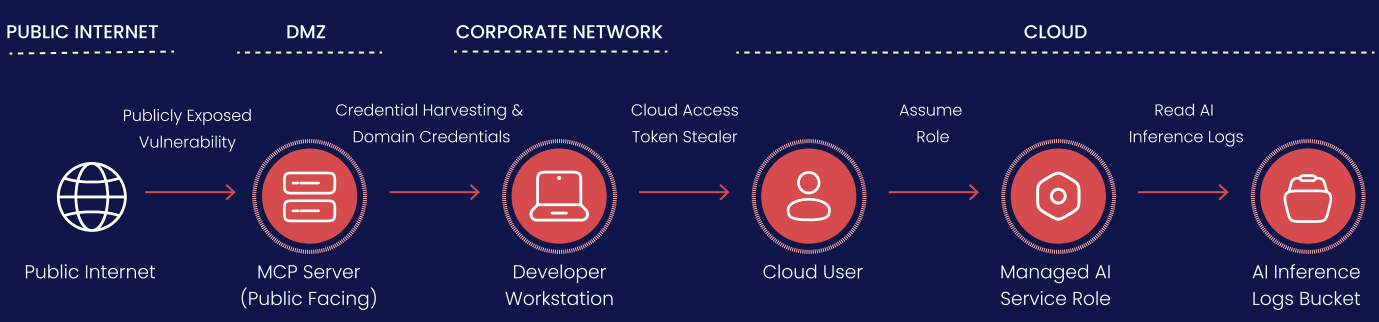
Continuously discover AI workloads and the infrastructure resources that support them.

Validate AI Attack Paths:

Validate and quickly sever attack paths that lead to and traverse AI resources and MCP servers.

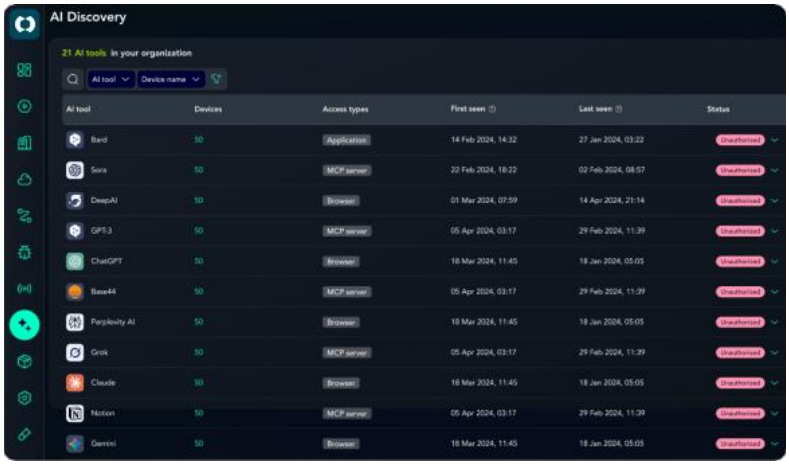
Enforce AI Policies & Compliance:

Ensure AI deployments adhere to security posture controls and predefined AI compliance.



Visualize the AI Attack Surface

ELIMINATE SHADOW AI
Continuously discover AI workloads, SaaS AI tools, and the hidden infrastructure resources supporting them across endpoints and data centers.



MCP INVENTORY
Automatically catalog all configured Model Context Protocol (MCP) servers to remove blind spots in your AI ecosystem.

CLOUD AI VISIBILITY
Gain deep coverage of managed cloud AI services, including AWS Bedrock, Google Vertex, and Azure OpenAI.

Uncover Validated AI Attack Paths

HYBRID ATTACK PATH VISUALIZATION
XM Cyber is the only vendor that visualizes validated attack paths that jump from on-premises workstations to cloud-based AI resources.

STOP AI SECRETS HARVESTING
Scan MCP configurations and environment variables for hardcoded API keys and tokens before they can be weaponized.

IDENTIFY EXPLOITABLE UTILITIES
Proactively flag AI resources configured with exfiltration-ready tools (e.g., curl, wget) or elevated privileges (e.g., sudo, shell interpreters).

Enforce AI Security & Compliance

GOVERNANCE & MONITORING
Ensure all AI deployments adhere to security posture controls and global frameworks, such as the EU AI Act and NIST AI Risk Management.

MUTATION DETECTION
Detect unauthorized configuration shifts or "mutations" in AI server definitions between scans to maintain a hardened state.