Meet KAIRO

Breach Modeling for Attack Surface Management

AI-Powered Defense to neutralizes AI-discovered vulnerabilities and zero-days before they are weaponized

Defending the Enterprise in the Post-Mythos Era

An exposed workload. A harvestable credential. An over-privileged identity. Alone, routine risk. Chained together, a reachable breach path. Kairo is Tuskira's breach-path disruption capability, built from a live digital twin of your environment. It maps those paths, validates where controls fail, and identifies the actions that break the chain before attackers can use it.

The Inflection Point

Frontier AI Model Attacks

Frontier AI models like Anthropic's Mythos can discover zero-day weaknesses, chain lower-severity issues into working exploits, and generate functional exploit code at machine speed. Kairo shows whether newly disclosed or AI-discovered zero-days create a reachable breach path in your environment, then identifies the control action needed to break the chain.

Weeks → Minutes

Disclosure-to-weaponization window for AI-discovered exploits

How KAIRO Finds and Breaks Breach Paths...*Continuously*

1. **Unify**
   Normalize identity, cloud, workload & network signals into the Tuskira Security Context Mesh.
2. **Model**
   Build a live Security Context Graph of reachability, privilege, and exploitability, grounded in business context and modeled as a digital twin of your environment.
3. **Map**
   Enumerate every traversable path to crown-jewel assets, ranked by exploitability and blast radius.
4. **Identify Residual**
   Surfaces the paths existing controls don't block, and existing detections don't see.
5. **Disrupt**
   Orchestrate targeted control actions at the highest-leverage control point through existing controls and analyst approval where policy requires it.
6. **Resolve**
   Track closure with evidence and status; reachability is re-validated as the environment changes.

Tuskira™

"2026 is the year cyber defenses are seeing the shift from AI-assisted attacks to AI-enabled attacks, and defenders need to adapt. That's why Intrado partnered with Tuskira."

Charles Gifford | **CISO, Intrado**

Common Breach Paths KAIRO Detects

Other tools find risk. KAIRO finds the attacker's path before they take it. That is preemptive security.

Breach path	Kill Chain	What Tuskira detects	How Tuskira Breaks the Path
Identity → Lateral Movement	Phished credential → MFA bypass → admin escalation → DC access → Golden Ticket	The privilege chain across identity and endpoint — not just the individual events	Removes privilege escalation paths before domain compromise.
Endpoint → Ransomware Staging	Macro execution → Cobalt Strike → LSASS dump → SMB spread → shadow deletion	The staging sequence — not just the ransomware payload at the end	Contains ransomware staging before encryption begins.
Multi-Cloud Pivot	Azure AD compromise → federated trust to AWS → cross-account role → RDS data access	The cross-cloud identity path — a blind spot in every single-cloud detection model	Breaks cross-cloud trust paths before sensitive data access.
On-Prem → Cloud Pivot (single CVE-anchored example)	Exposed appliance (e.g., Ivanti CVE-2024-21887) → in-memory token theft → cached AWS SSO token → cross-account assume-role → RDS snapshot export	The residual path from a known weakness through cached cloud credentials and federated trust into production data	Collapses CVE-to-cloud access paths before exfiltration.

Paths mapped to MITRE ATT&CK and correlated across endpoint, identity, cloud, network, and hybrid environments, including east-west movement, cross-cloud pivots, identity abuse, and insider-driven data movement.

Why KAIRO is Different

CNAPPs show cloud exposure. BAS tools simulate attacks. Exposure tools prioritize findings. Kairo connects them into the attacker's path, showing which risks are actually reachable and which control action breaks the chain.

98%
Findings de-prioritized as unreachable.

Minutes
From environment change to updated path map.

One graph
Identity, cloud, workload & network unified.

One action
Closes multiple paths through a shared control point.

See KAIRO in Action

Map reachable, exploitable paths in days. Break them through the controls you already own, and move from finding counts to breach resilience.

Request a Kairo demo: tuskira.ai/demo | Lorin@tuskira.ai

Tuskira™
Full Stack Agentic SecOps