From Chaos to Clarity
Visualizing and Acting on Your Attack Surface with TruContext

Executive summary

The enterprise perimeter no longer exists. Cloud, mobile, and IoT growth have created a sprawling, dynamic attack surface full of hidden assets and fast-moving threats. Visium TruContext transforms that chaos into operational clarity by combining multi-layer graph modeling, continuous discovery, and agentic Artificial Intelligence ("AI") — not just to show risk, but to act on it. The result: prioritized, context-aware remediation that scales to modern environments and defends against AI-accelerated adversaries.

The problem: visibility without action

Many organizations use disconnected tools and manual processes that produce stale or partial views of assets. That creates blind spots attackers exploit and overwhelms security teams with too many low-value alerts. Visualization alone is necessary but not sufficient: teams need intelligence that reasons across relationships, proposes prioritized actions, and can execute or orchestrate remediation steps where appropriate.

TruContext approach: unified graph plus agentic AI

TruContext builds a continuous, multi-layer graph that maps users, devices, apps, data, cloud instances, identity relationships, and network flows. That contextual backbone lets TruContext do more than surface inventory: it enables threat path analysis, business-impact scoring, and automated, context-aware responses.

- **Persistent multi-layer graph** — captures entities and relationships to reveal lateral movement paths and dependency chains.
- **Continuous discovery and normalization** — keeps the graph current as environments change.
- **Business-impact context** — ties technical findings to critical assets and processes for better prioritization.
- **Agentic AI orchestration** — AI agents analyze graph context to recommend, prioritize, and in some cases execute remediation actions automatically.

For concrete examples of TruContext's agentic AI capabilities — including automated investigative agents, remediation orchestration, and contextual assistant workflows — see the TruContext agent examples and demos.

How agentic AI changes outcomes

Agentic AI extends TruContext from visibility to action in three capability areas:

1. Continuous threat path discovery and prioritization

    - Agents traverse the graph to identify high-probability attack paths and compute business-impact scores so teams fix what matters first.
2. Automated investigation and enrichment
    - Agents consolidate telemetry, risk signals, and identity context, producing concise investigative summaries and recommended next steps that remove manual toil.
3. Remediation orchestration and guided response
    - Where policy allows, agents can trigger containment (isolate a host, revoke credentials), open tickets with prioritized remediation steps, or generate playbook-ready actions for SOC and IT teams.

These agent workflows reduce mean time to detect and remediate, lower analyst workload, and close gaps that humans alone routinely miss.

Real-world scenario: defending against AI-accelerated attacks

Attackers increasingly use automation and AI to scan, probe, and chain exploits at machine speed. Against that threat, TruContext's combined graph + agentic AI advantage is threefold:

- Faster reconnaissance: agents continuously surface emergent attack paths before adversaries can chain them.
- Contextual triage: agents score paths by business impact and exploitability, preventing wasted effort on low-value alerts.
- Rapid containment: agents execute validated containment actions or hand off precise, prioritized playbook steps to human operators.

This reduces the window of opportunity for attackers and converts noisy telemetry into decisive, timely actions.

Implementation and outcomes

Deployment of TruContext delivers measurable operational improvements:

- **Fewer blind spots** — continuous discovery reduces unknown or unmanaged assets.
- **Higher remediation velocity** — prioritized, agent-suggested actions accelerate patching and containment.
- **Lower analyst fatigue** — agents automate enrichment and routine responses, freeing experts for complex investigations.
- **Better executive visibility** — business-aligned risk scoring supplies clear decision-grade summaries for leadership.

Successful rollouts pair TruContext's agentic workflows with existing SIEM, SOAR, IAM, and ticketing systems to preserve investments while increasing automation and effectiveness.

Conclusion

Visibility is the first step, but modern security requires systems that reason, prioritize, and act. Visium TruContext combines a richly contextual graph with agentic AI to turn discovery into defended outcomes — surfacing critical attack paths, automating investigation, and orchestrating remediation at scale. For security teams facing faster, AI-powered adversaries, TruContext delivers the clarity and agency needed to stay ahead