Dataminr

Dataminr for Cyber Defense & Silent Push

Know and Anticipate the Adversary

The Challenges

The cybersecurity industry only tracks about 2% of threat actor infrastructure. This creates blind spots for threat intel and security operations teams responsible for tracking, understanding, preventing, and responding to threat actors and attacks.

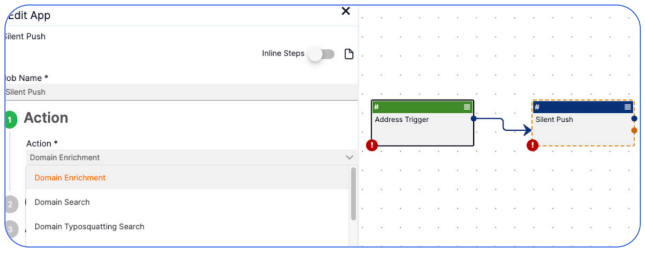
Why Dataminr for Cyber Defense & Silent Push

Silent Push generates first-party data across the IPv4 space and produces Indicators of Future Attack (IOFA) enabling intel teams to track adversary infrastructure before it's weaponized and used against an organization. The integration of Dataminr for Cyber Defense enables CTI and SecOps analysts to easily enhance the data in their Threat Library with the rich context from Silent Push to provide even more value to their accumulated threat intel and internal knowledge.

Get Results with Dataminr for Cyber Defense & Silent Push

The Silent Push Playbook App makes it easy to automate context enrichment on the intel in your Threat Library and search Silent Push's intel with almost two dozen out-of-the-box actions. The combination of Dataminr and Silent Push enables use cases like:

- **Enrich Threat Intelligence:** Automated contextualization of your threat intelligence to improve its accuracy and fidelity, enabling better and faster analysis and actions.
- **Threat Detection and Prevention:** Improve the threat detection capabilities of your SIEM and security analytics tools, endpoint, network, and cloud security solutions. Proactively block adversary infrastructure before it's used in attacks against your organization.
- **Threat Hunting:** Leverage Silent Push to hunt for indicators associated with attacker infrastructure and reduce attacker dwell time.



Key Benefits

Highly enriched threat intel with complete, timely, and accurate context of global internetfacing infrastructure

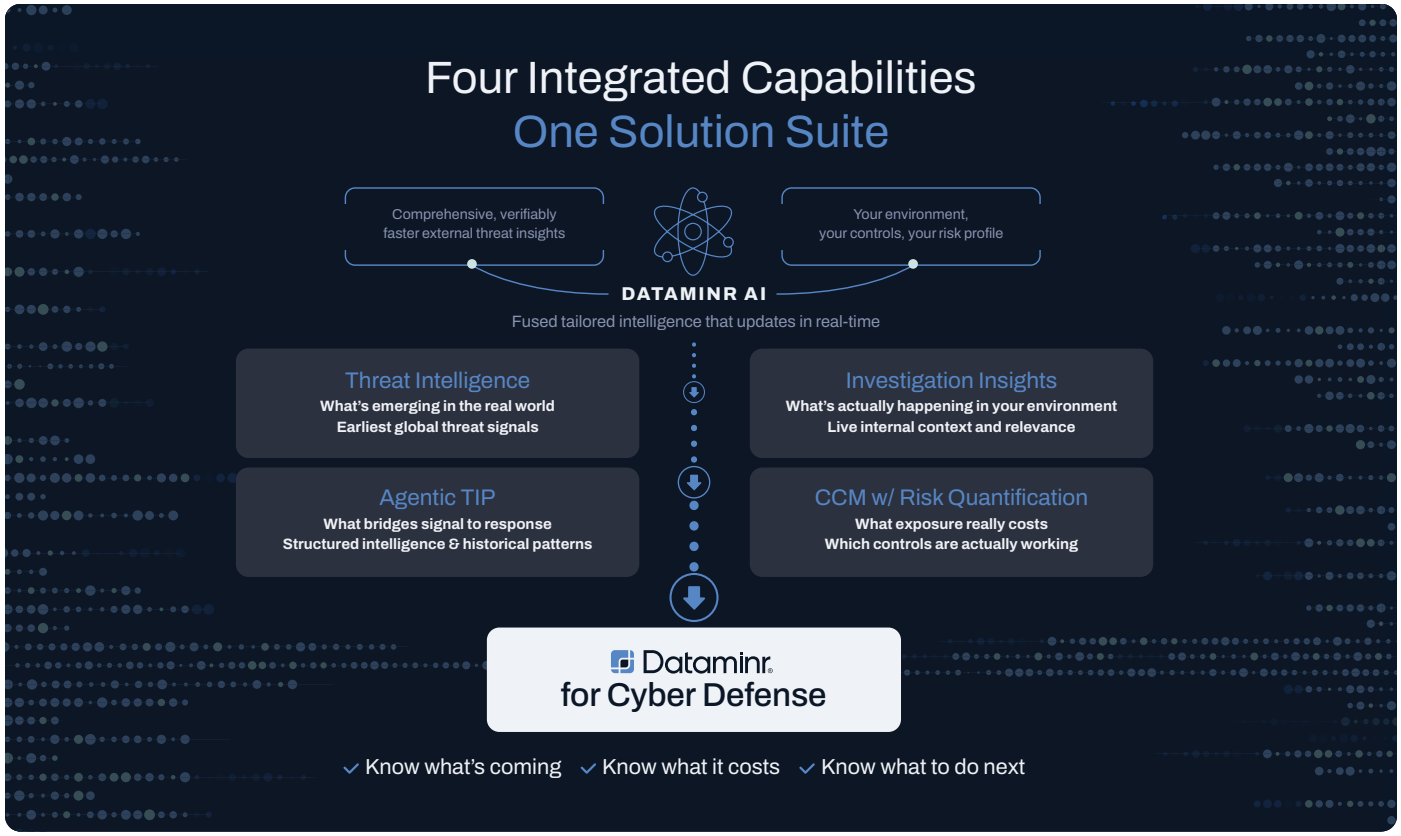
Better anticipate threat actor activity and take action

Proactively block threat actor infrastructure to improve threat defense

How to Get Started

Request a demo on our website. To learn more about this particular integration, contact sales@dataminr.com. If you're an existing customer, please reach out to your customer success manager.

Four Integrated Capabilities
One Solution Suite



Client-Tailored
Threat Intelligence (CTTI)

Real-Time Threat Insights, Full-Stack Context

Detect emerging threats and exploits from the earliest signal with Dataminr Client-Tailored Threat Intelligence (CTTI), and instantly search across your security stack without pivoting.

- **Early-Signal Threat Detection**
- **Agentic AI Adversary Intel**
- **Cross-Stack Security Search**
- **No Syntax, No Context Switching**

Agentic TI Ops

From First Signal to Finished Intelligence — Automatically

Instantly discover emerging vulnerabilities, exploits, and zero-day attacks with detailed context on trending CVEs, CVSS/EPSS scores, and threat actor TTPs.

- **Embedded Dataminr CTTI Tooling**
- **Intel-First Playbooks & Automation**
- **Unified Threat Library & Reporting**
- **Intel Hub with 125+ Integrations**

Predictive Threat
Exposure Management (PTEM)

Exposure Prioritized by Risk, Quantified by Impact

Proactively prioritize vulnerabilities with continuous rationalization of high-efficacy exploit signals, attack surface context, compensating controls, and financially quantified risk.

- **Intel-Driven Risk Prioritization**
- **Automated Attack Path Modeling**
- **MITRE-Level Financial Modeling**
- **Continuous Control Monitoring (CCM)**

Dataminr for Cyber Defense

Activate a Unified, Multi-Modal Cyber Defense Fabric

Extend, tailor, and fuse cyber risk insights and context across Dataminr solutions for a shared, continuously adapting view of security, threat, and exposure priorities to drive agentic, threat-informed defense.

Threat Intelligence | Investigation Insights | Agentic TIP | CCM w/ Risk Quantification

Power the Future of Cyber Defense with Dataminr

dataminr.com