SOLUTION BRIEF

Integrated Internet Intelligence Enrichment for Faster Threat Triage and Exposure Response with Censys and Dataminr

Summary

Organizations face accelerating cloud and Internet-facing sprawl, where threat activity and exposure evolve faster than manual investigation can keep up. Security teams need immediate context on IPs and other indicators to distinguish benign infrastructure from active risk—and to understand whether an exposed service is part of their own external attack surface. Censys delivers an authoritative view of Internet assets and exposure through its Internet Intelligence and Attack Surface Management (ASM) capabilities, while Dataminr operationalizes threat intelligence through its Dataminr Agentic Thread Intelligence (TI) Platform and workflow automation.

Together, Dataminr Agentic TI Platform and Dataminr Investigation Insights bring Censys context directly into analyst workflows and playbooks: enriched IOC investigations, faster pivoting, and risk-driven prioritization based on observed services, ownership, and location. The joint solution reduces time spent on manual enrichment, improves triage and response consistency, and strengthens exposure management with high-fidelity, externally observed evidence.

Customer Challenges

Rapid digital transformation, cloud adoption, and hybrid work models are expanding the number of Internet-exposed services, third-party dependencies, and distributed tools in use. This growing complexity makes it increasingly difficult for security teams to apply consistent, actionable intelligence across fragmented environments.

Incomplete external visibility creates significant challenges in accurately attributing infrastructure, confirming ownership, and identifying newly exposed services. This lack of context contributes to delayed detection, weak prioritization, and slower response to active threats, increasing overall risk exposure. At the same time, the inability to maintain an accurate and current inventory of Internet-facing assets introduces compliance and governance gaps, making it difficult to enforce consistent security controls.

Operational inefficiencies arise from manual enrichment workflows that require analysts to perform multiple lookups across disparate tools, slowing investigations and contributing to fatigue. High volumes of alerts and indicators create significant noise, while tool sprawl makes it difficult to standardize triage workflows and ensure consistent decision-making. At the same time, inaccurate or incomplete asset inventories increase the risk of overlooking exposed or unmanaged services, further complicating response efforts and elevating organizational risk.

Joint Solution Overview

The Censys' Internet Intelligence and Attack Surface Management (ASM) capabilities with the Dataminr Agentic TI Platform deliver continuous external visibility and operationalized threat intelligence. Censys provides persistent discovery and monitoring of Internet-facing assets along with rich enrichment for IPs and related entities, including open ports and services, ownership and ASN data, geolocation, and operating system or product fingerprints. On the Dataminr side, the Agentic TI Platform centralizes intelligence management while applying native automation and workflow orchestration, and Dataminr Investigation Insights enhances analyst productivity by delivering a "context anywhere" overlay that enables instant enrichment without requiring tool switching.

Together, the integration enables Dataminr playbooks and Investigation Insights overlays to invoke Censys search and enrichment functions in real time, injecting high-fidelity external context directly into investigations, cases, and response workflows. This unified approach combines indicator-centric intelligence with externally observed asset evidence, allowing security teams to improve infrastructure attribution, prioritize risk more effectively, and accelerate exposure validation and response.

Key Business Outcomes

- **Faster time-to-triage** by enriching observables with authoritative Internet context at the point of investigation.
- **Improved decision quality** by correlating indicators with observed services, ownership, and geolocation to reduce false positives and prioritize real risk.
- **Reduced exposure risk** by validating suspicious infrastructure against known external assets and identifying unmanaged or newly exposed services.
- **Lower operational overhead** through automated enrichment in Dataminr Agentic TI Platform playbooks and consistent context overlays in Dataminr Investigation Insights.
- **More consistent reporting** by capturing enrichment results directly in cases, tickets, and intelligence objects.

User and Buyer Personas

CISOs

SOC/IR leadership

CTI director/manager

Threat hunters

Vulnerability and exposure management leads

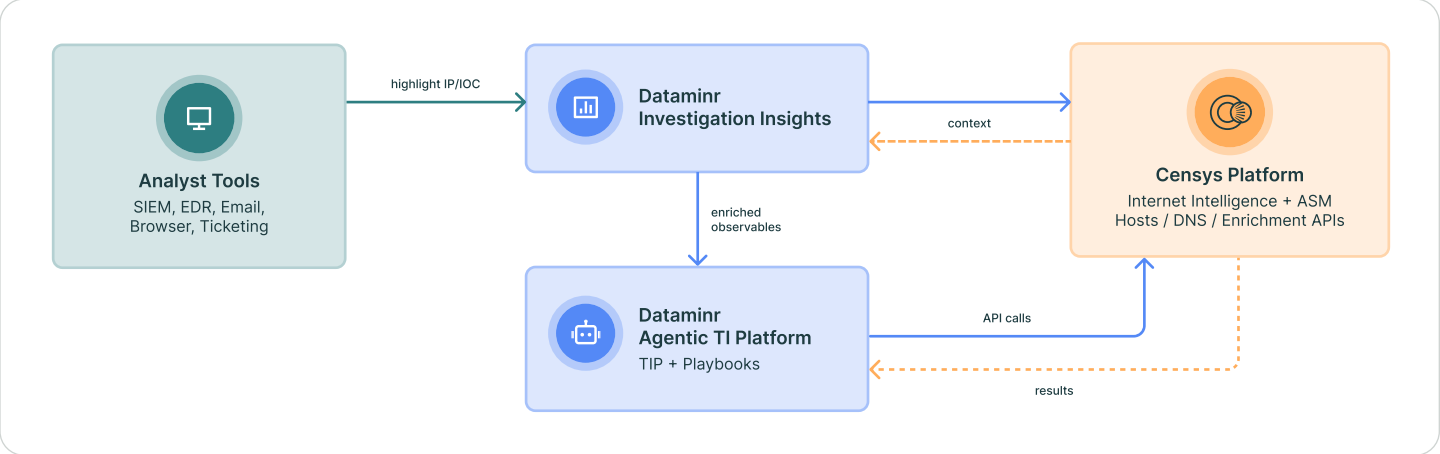

Fig. 1 Data flows: indicators → Censys enrichment → context overlays and automated playbooks

Use Cases

Indicator enrichment during alert triage

During alert triage, high volumes of IP-based alerts often lack immediate attribution and service context, slowing analysis and decision-making. By integrating Censys enrichment into the Dataminr Agentic TI Platform, alerts are automatically enriched with external intelligence such as ownership, services, and geolocation—at ingestion. This enriched context is attached directly to the case or observable, enabling faster, more informed triage decisions and supporting automated routing or escalation based on the intelligence.

"Context anywhere" for investigations with Dataminr Investigation Insights

During investigations, analysts often lose time switching between tools to gather context on indicators like IPs. Dataminr Investigation Insights addresses this with a "context anywhere" capability that delivers instant, in-line enrichment via Censys without leaving the current workflow. When an IP is highlighted in a SIEM, EDR, email, or ticketing tool, it triggers a Censys lookup that returns a structured context card with key intelligence such as ownership, ASN, geolocation, OS details, and services/ports enabling faster assessment and seamless pivoting or enrichment within the Dataminr Agentic TI Platform.

Exposure validation and scoping

Security teams must quickly determine whether suspicious infrastructure belongs to their own environment or a third party to avoid delayed response and increased risk. By integrating Censys enrichment into the Dataminr Agentic TI Platform, infrastructure indicators (IPs/domains) within a case are automatically enriched with ownership and service exposure data via playbooks or Investigation Insights. Teams can then compare this external evidence against internal inventories to validate exposure and take action such as containment, notification, or remediation with workflows assigning tasks or opening tickets that include Censys-derived context.

Prioritize vulnerabilities and risky services with external evidence

Rapidly changing exposure and incomplete asset inventories make it difficult to effectively prioritize vulnerabilities and risky services. By integrating Censys enrichment into the Dataminr Agentic TI Platform, analysts can validate externally exposed services and obtain detailed product fingerprints for relevant IPs identified during investigations. This intelligence feeds directly into response workflows informing case severity, assignments, and SLAs so teams can prioritize remediation of high-risk, Internet-facing services first, improving both efficiency and overall risk reduction.

Why This Joint Solution Matters

Dataminr and Censys combine intel-driven operations with authoritative Internet intelligence to help teams move from indicator overload to confident, risk-informed action. By embedding Censys enrichment directly into Dataminr Agentic TI Platform workflows and Dataminr Investigation Insights context overlay, organizations gain faster triage, stronger attribution, and clearer exposure understanding without adding more tool switching. The result is a more efficient SOC/CTI function and a more defensible external exposure posture.

Request a Demo

Contact Censys to see how Censys and Dataminr together provide faster threat triage and exposure response.

censys

VISIT
censys.com

CONTACT
hello@censys.com

Censys is the authority for Internet intelligence and insights. Delivering the most complete, accurate, and up-to-date global map of Internet infrastructure, Censys provides industry leading solutions for attack surface management, threat hunting, and proactive incident response. Global governments, Fortune 500 companies, and security providers around the world trust Censys to uncover risks faster, respond more effectively, and prevent breaches before they happen.