JOINT SOLUTION BRIEF

Accelerate Attack Surface Discovery, Investigation, and Response with BlinkOps and Censys

Summary

Organizations today face an expanding external attack surface driven by cloud adoption, mergers and acquisitions, shadow IT, and rapidly changing internet-facing infrastructure. Security teams need continuous visibility into exposed assets and the ability to rapidly investigate and remediate risks before attackers can exploit them.

Censys provides industry-leading Internet intelligence, attack surface management, and threat hunting capabilities, helping organizations continuously discover and monitor internet-facing assets and exposures. Censys delivers comprehensive visibility into external infrastructure, certificates, web properties, and attack surface risks.

BlinkOps is an Agentic Security Operations Platform that deploys AI agents to ingest that intelligence, investigate findings end to end, reason about risk and asset context, and execute response actions across the security stack without waiting for analyst involvement. Together, BlinkOps and Censys close the gap between exposure discovered and exposure resolved.

Joint Solution Overview

Discover and Investigate External Exposures

Censys Platform gives BlinkOps agents on-demand access to the most comprehensive map of the global Internet — AI-driven scanning across all 65,535 ports, daily refresh on over 5 billion running services, and the world's largest X.509 certificate repository with over 17 billion certificates. Agents can execute structured queries across hosts, services, certificates, and web properties, and tap historical data to understand how an asset's exposure has changed over time. Censys ASM adds the organizational layer: continuous, first-party scanning that maps each customer's specific attack surface, detects exposure drift in near real time, and surfaces unknown or unmanaged infrastructure before attackers find it. BlinkOps connects natively to both, giving agents an attacker-accurate, high-fidelity intelligence feed they can act on immediately with no manual query handoff, no stale data.

Agents handle the full investigation workflow:

- Query Censys Platform to identify exposed hosts, services, technologies, and certificates across the global Internet
- Execute structured or natural language queries across 1,000+ parsed and indexed fields to detect threats and understand exposure patterns
- Pull ASM host records with open ports, running services, and associated risk findings for assets within the monitored surface
- Detect newly surfaced assets and exposure drift as they occur, triggering automated triage
- Retrieve certificate intelligence: issuer, validity, revocation status, and subject alternative names, at individual or portfolio scale
- Assess internet-facing web properties for detected technologies, hidden endpoints, misconfigurations, and risk indicators
- Flag unmanaged or unknown infrastructure for owner identification and remediation routing

© Censys, 2026. All rights reserved.

Execute Remediation Across the Security Stack

Once a BlinkOps agent has investigated and scored a finding, it drives remediation without waiting for analyst handoff. Agents act across connected systems based on the severity and context of each exposure.

Remediation actions include:

- Create ServiceNow remediation tickets with structured finding data
- Notify asset owners through Slack or Microsoft Teams
- Open Jira tasks for infrastructure and cloud teams
- Trigger cloud remediation workflows directly
- Update CMDB records to reflect current asset state
- Escalate critical findings to incident response teams
- Track remediation progress and SLA compliance

The result is a consistent, traceable response process applied to every finding at the speed and scale that manual workflows cannot match.

Key Business Outcomes

Together, BlinkOps and Censys give security teams the means to:

- **Discover external risks and act on them within the same workflow**
- **Reduce the investigation burden on analysts**
- **Shorten remediation timelines without adding headcount**
- **Maintain consistent response quality across all finding types**
- **Scale security operations to match the pace of exposure growth**

Common Use Cases

Attack Surface Monitoring

Censys ASM continuously scans across all 65,535 ports, including nonstandard ports and self-signed certificate hosts that other tools miss, and alerts on meaningful deltas the moment the surface changes. When unknown infrastructure surfaces or an existing asset's exposure profile shifts, the BlinkOps agent identifies the owning team, checks the asset against the approved register, and initiates escalation or remediation based on policy.

Certificate Risk Management

Agents identify expiring, misconfigured, or unauthorized certificates across the external surface. When a certificate issue is detected, the agent initiates renewal or revocation workflows and notifies relevant teams before expiry creates a service disruption or trust failure.

External Asset Inventory Validation

Agents compare Censys-discovered assets against the internal CMDB. Assets that appear in Censys but not in the approved inventory are flagged as shadow IT. The agent triggers an owner identification workflow and routes findings to the appropriate remediation queue.

Threat Hunting

Agents execute structured Censys searches to identify exposed technologies, legacy services, or indicators associated with active threat campaigns. Findings route directly into investigation workflows. No manual query handoff required.

Vulnerability Prioritization

Agents enrich Censys findings with cloud infrastructure context, vulnerability scan data, and asset criticality scores. High-business-impact exposures are escalated first. Lower-severity findings are queued with full context attached, so analysts work prioritized backlogs rather than raw finding lists.

Incident Response

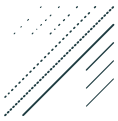
When an incident opens, a BlinkOps agent immediately queries Censys for the external footprint of involved assets. It retrieves exposure history, identifies ownership, maps connectivity context, and surfaces the complete picture to the responding analyst before they ask for it.

© Censys, 2026. All rights reserved.

Why This Joint Solution Matters

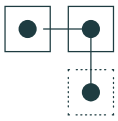
Intelligence without action is a backlog.

Censys surfaces what is exposed. BlinkOps agents work the findings end to end, from investigation through remediation execution. The combination closes the loop that every SOC struggles to close at scale.



Agents work in parallel, at machine speed.

Most ASM programs generate findings faster than teams can manually triage them. BlinkOps agents apply consistent logic to every finding simultaneously, regardless of volume. Coverage does not degrade as findings increase.



Native integration, no custom scripting.

BlinkOps connects to both Censys Platform and Censys ASM out of the box. Agents can be deployed against live Censys data in hours.

Attacker-accurate visibility, not inferred inventory.

Censys ASM is built on first-party Internet scanning across all 65,535 ports, not DNS inference or third-party feeds. BlinkOps agents operate from the same picture an attacker would have, so investigation and response is grounded in what's actually reachable.

Full auditability.

Every agent action is logged and traceable. Security teams get consistent processes applied to every finding, with a complete record of what was investigated, what decision was made, and what action was taken.

Learn More

Contact Censys to see how Censys and Dataminr together accelerate attack surface discovery, investigation, and 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.