JOINT SOLUTION BRIEF

Censys + Cyware: Turning Attack Surface Visibility into Proactive Threat Response

Summary

Organizations are dealing with a rapidly expanding attack surface driven by cloud adoption, distributed infrastructure, and increasingly capable adversaries targeting exposed assets. Many security teams lack a clear, real-time view of what's exposed externally and struggle to turn threat intelligence into consistent, scalable action.

Censys and Cyware address this gap by combining continuous external asset intelligence with automated security operations. Cyware, a unified threat intelligence platform, brings the orchestration and automation layer that turns that intelligence into consistent, scalable action. Together, they help organizations reduce exposure risk, respond faster to threats, and improve SOC efficiency by minimizing manual investigation and enrichment efforts.

Customer Challenges

Organizations moving quickly to the cloud are finding it harder to keep track of what they actually have exposed to the internet. Hybrid environments and constantly changing infrastructure make it easy for assets to slip through the cracks, leading to blind spots in security coverage. At the same time, threat intelligence often lives in separate tools and teams, which makes it difficult to use effectively in day-to-day security operations or to support a more proactive approach.

On the operational side, security teams are dealing with limited visibility into external assets and often don't discover exposures or misconfigurations until it's too late. Investigations take longer because enrichment and analysis are still largely manual, and alerts come in without enough context to prioritize them properly. Add in too many disconnected tools and inconsistent asset data, and teams end up spending more time piecing things together than actually reducing risk.

Joint Solution Overview

The Censys and Cyware integration connects external asset intelligence directly into security operations workflows. Censys continuously discovers and analyzes internet-facing assets, providing detailed context on exposures, services, and certificates. Cyware ingests this data into its orchestration and threat intelligence platform, where it can be enriched, correlated, and acted on through automated playbooks.

This integration allows teams to trigger Censys queries from within Cyware, automatically enrich alerts with external context, and initiate response actions such as ticketing or remediation. The result is a more streamlined workflow where external visibility feeds directly into investigation and response, without requiring manual handoffs between tools.

Key Business Outcomes

- **Reduced Risk Exposure:** Continuous discovery and validation of internet-facing assets reduces blind spots and attack surface risk
- **Faster Detection and Response:** Automated enrichment and playbook execution accelerate incident triage and remediation
- **Improved Intelligence Utilization:** Contextualized external asset intelligence enhances threat prioritization and decision-making
- **Operational Efficiency Gains:** Automation reduces manual workflows, lowering SOC workload and improving scalability

Use Cases

External Asset Exposure Monitoring

Security teams don't always have a clear, current picture of what's exposed to the internet, which makes it easy for misconfigurations or risky assets to slip by unnoticed. With Censys and Cyware working together, Censys continuously finds those external assets and exposures, and sends that data into Cyware, where playbooks take over validating the risk, adding context, and kicking off remediation steps so teams can reduce exposure quickly without a lot of manual work.

Automated Threat Intelligence Enrichment

Threat intelligence often comes fragmented and without enough context to be truly useful. With Censys integrated into Cyware Threat Intel Exchange, indicators are automatically enriched with real-world asset data like IP and service details, giving teams clearer insight into what matters and helping them prioritize and respond more effectively.

Incident Response Acceleration

When incidents involve external assets, teams often lose time digging for context and piecing things together manually. With Censys integrated into Cyware, playbooks can automatically pull in asset details, enrich alerts, and kick off response actions like creating tickets or blocking activity so teams can respond faster without the usual back-and-forth.

Attack Surface Reduction

Security teams often have a hard time keeping up with exposed services and making sure they're actually addressed. With Censys and Cyware working together, Censys flags those exposures as they appear, and Cyware helps take it from there to validate the risk, identify ownership, and drive remediation through automated workflows so issues don't just sit unresolved.

Proactive Threat Hunting

Many organizations don't have an easy way to proactively identify risky assets or uncover adversary infrastructure before it becomes a problem. With Cyware and Censys integrated, analysts can run and automate Censys queries directly through Cyware, using aggregated results to spot patterns, surface potential threats earlier, and take action before they escalate.

Why This Joint Solution Matters

Security teams don't just need more visibility, they need a way to consistently act on it. The Censys and Cyware integration closes that gap by connecting external asset intelligence directly into day-to-day security workflows, so insights don't sit idle or require manual follow-up. It helps teams stay ahead of exposures, respond with better context, and reduce the friction between discovery and action. Instead of stitching together multiple tools, organizations get a more streamlined approach that supports how modern SOCs need to operate - faster, more coordinated, and better aligned to managing an evolving attack surface.

Get Started

Contact Censys for more information on how Censys and Cyware integrate external attack surface intelligence and security orchestration for proactive threat 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.