Censinet Announces New Portfolio Management Capabilities to Accelerate Cyber Risk Management and Incident Response

Major Product Update Uniquely Delivers Automated Support for NIST Risk Assessment Best Practices; Reduces Reassessment Completion Time by 95%

Censinet logo

BOSTON, MA, USA, December 21, 2022 /EINPresswire.com/ -- Censinet, the leading provider of healthcare risk management solutions, today announced a powerful set of new portfolio management capabilities that significantly accelerate third party risk management and incident response. Building upon the release of Censinet RiskOps 5.0 in September 2022, this release introduces several new innovations for comprehensive automated support for NIST Special Publication (SP) 800-30, Guide for Conducting Risk Assessments, including risk tiering and automated reassessment scheduling, delta-based reassessments, and tier-based corrective action plan (CAP) generation. This release also introduces breach and ransomware vendor monitoring to accelerate incident response and recovery.

> Censinet helps us identify third party vendors that represent the highest potential risk. Censinet continues to reduce costs and improve inefficiencies in risk management processes."
>
> *Matt Christensen, Director, GRC, Intermountain Healthcare*

NIST SP 800-30 states: "Risk assessments are not simply one-time activities....Rather, organizations employ risk assessments on an ongoing basis throughout the system development lifecycle and across all of the tiers in the risk management hierarchy—with the frequency of the risk assessments and the resources applied during the assessments commensurate with the expressly defined purpose and scope of the assessments."

This product release transforms NIST 800-30 best practices into automated risk workflows to ensure the highest-risk vendors and products are automatically reassessed more frequently across the entire contract lifecycle. For organizations that have yet to establish a reassessment policy, Censinet provides out-of-the-box, default settings for tier-based reassessment scheduling. With new delta-based reassessment capabilities, organizations can dramatically reduce

reassessment completion times by 95% – delivering unparalleled productivity gains and demonstrable cost savings for third party risk management programs over many years.

“Censinet portfolio management capabilities set a new standard for total automation in third-party risk management,” said Paul Russell, Chief Product Officer at Censinet. “Working with leading healthcare organizations to automate key workflows for tiering, reassessments, and NIST best practices, Censinet widens the aperture on third-party portfolio risk visibility and delivers unparalleled efficiency gains, continuous risk reduction, and enduring cost savings.”

Also in this release, Censinet’s built-in, automated correct action plans (CAP) now dynamically adjust findings and corrective actions based on tier levels for each vendor and product. Powered by Censinet’s curated findings and corrective actions, this new capability produces an automated CAP that is better calibrated to the specific risks that a vendor or product represents to the organization. What’s more, organizations can now define, customize, and automate their own tier-based findings and corrective actions based on organizational tier policy or risk appetite. Organizations automatically set these customized tier-based corrective actions to be included in contractual language for specific vendor/product tiers going forward.

“With these new portfolio management capabilities, Censinet continues to reduce costs and improve inefficiencies in risk management processes,” said Matt Christensen, director, governance, risk and compliance at Intermountain Healthcare. “The Censinet platform helps us identify third party vendors that represent the highest potential risk. These new Censinet capabilities will better enable us to enforce cyber risk policies through automation, and drive continuous, tier-appropriate risk assessment, reassessment, corrective action plan generation, and remediation.”

Also included in this product update, Censinet provides daily monitoring of vendor breaches and ransomware attacks. While Censinet helps organizations identify and reduce the risk of a third party incident through its actionable insight, it strengthens this capability with information about breaches and ransomware attacks related to vendors in an organization’s third-party portfolio. Third-party vendor breach and ransomware events are continually monitored and updated, and Censinet users are automatically notified when an incident or event is detected. This unified view provides a new dimension of risk visibility across the third-party portfolio and speeds up response and recovery upon incident.

Availability
All of these capabilities are available now and included in the Censinet RiskOps platform. To learn more about this product update, please contact us at info@censinet.com or to request a demo, please visit www.censinet.com/riskops-demo-request/.

About Censinet
Censinet®, based in Boston, MA, takes the risk out of healthcare with Censinet RiskOps, the industry’s first and only cloud-based risk exchange of healthcare organizations working together

to manage and mitigate cyber risk. Purpose-built for healthcare, Censinet RiskOpsTM delivers total automation across all third party and enterprise risk management workflows and best practices. Censinet transforms cyber risk management by leveraging network scale and efficiencies, providing actionable insight, and improving overall operational effectiveness while eliminating risks to patient safety, data, and care delivery. Censinet is an American Hospital Association (AHA) Preferred Cybersecurity Provider. Find out more about Censinet and its RiskOps platform at censinet.com.

Justyn Thompson
Censinet
+1 617-221-6875
email us here