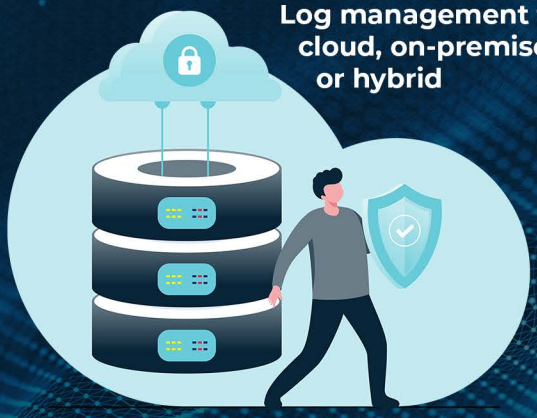
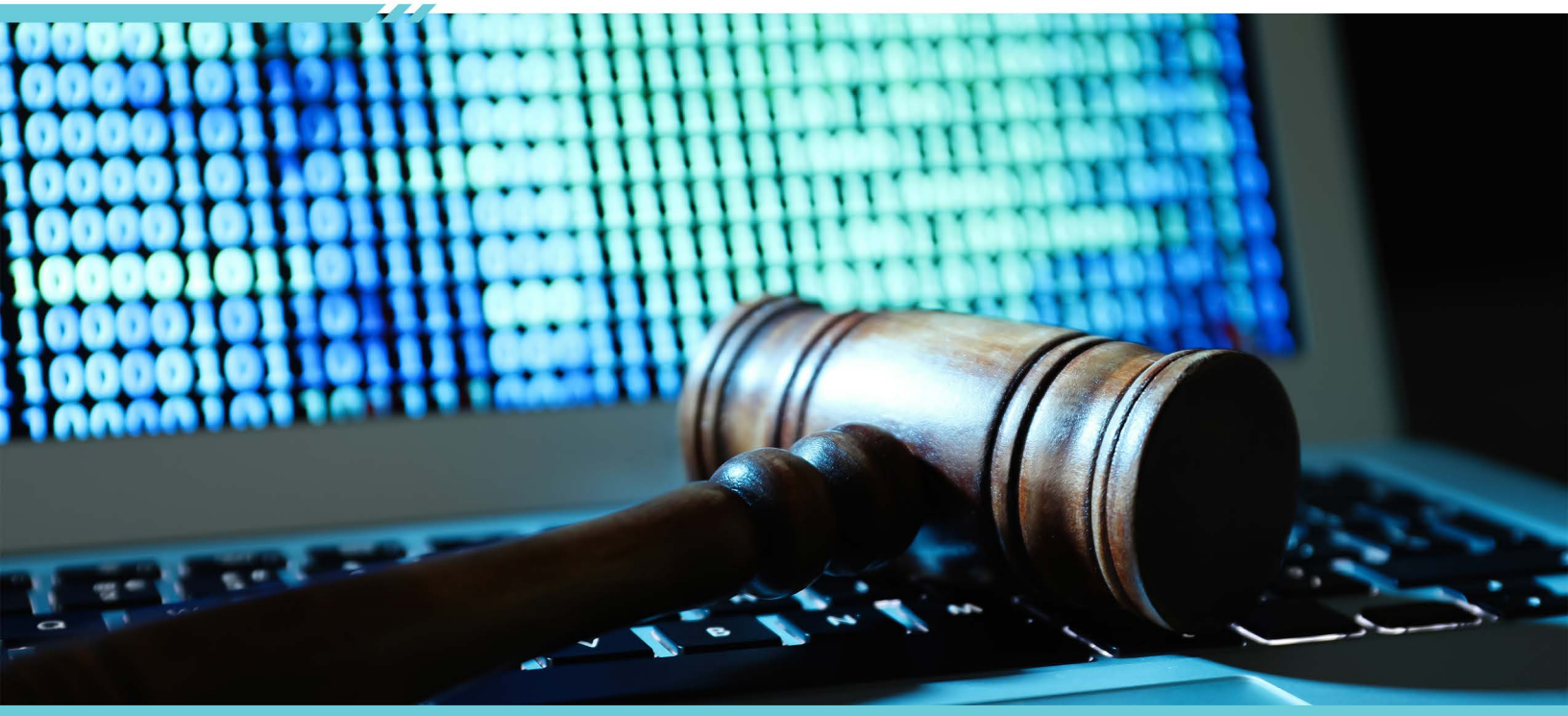
snare
A PROPHECY SOLUTION

How Snare streamlined a global law firm's IT infrastructure to achieve efficient log management and system-wide security compliance



EXECUTIVE SUMMARY

A global law firm faced significant challenges during its transition from AlienVault to QRadar for Security Information and Event Management (SIEM). The firm required a scalable solution for efficient log management across its extensive IT network, which included a wide range of servers and systems, coupled with a complex data retention policy involving cloud platforms and S3 Glacier. To address this, the company deployed Snare Agents for log collection, using Reflectors for dual log transmission to QRadar and S3 Glacier, and establishing a Snare Agent Management Console in each data center. This strategic integration has streamlined the firm's data management, providing a scalable, efficient, and cost-effective log management system that meets its specific security, compliance, and infrastructure needs, while preparing for future changes in SIEM technology without the need for a significant infrastructure redesign.



Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com

CHALLENGE SUMMARY

A global law firm, operating in multiple countries with a substantial team of lawyers, was struggling to find a reliable and scalable platform capable of managing agents for efficient log collection and transmission to QRadar, which emerged during its transition from the AlienVault system to QRadar as part of a security information and event management (SIEM) refresh. The AlienVault system was inherited, and underperforming in event consumption, handling only a fraction of the expected volume..

The firm needed a solution that could efficiently manage and scale log collection across its diverse and extensive IT infrastructure, which comprises a significant number of Windows servers (including some transitioning to Azure), a considerable fleet of Windows Desktops, MacOS systems, and MSSQL servers. The global law firm's move to Office 365 and its requirement to manage data across multiple data centers with a robust retention policy, including several months of online storage before transferring to S3 Glacier, further complicated the situation.

Our objective was to demonstrate how Snare could integrate into the global law firm's existing technology infrastructure to enhance compliance and security, while offering significant cost savings by:

- deploying Snare Agents on endpoints for efficient log collection
- using Reflectors to send logs to both QRadar for analysis and S3 Glacier for storage
- implementing a Snare Agent Management Console (AMC) in each of the four data centers.

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com

OUTCOME SUMMARY

The integration of Snare into the global law firm's technology infrastructure has resulted in a scalable, cost-effective, and efficient system that is well-suited to managing its expansive network. Snare's deployment enhances security and compliance, while its centralized management via AMC and effective log routing through Reflectors to QRadar and S3 Glacier aligns seamlessly with the global law firm's requirements for data retention and legal compliance.

During the transition, the firm placed a high priority on planning for the future by establishing a solid logging foundation. This approach would afford it the ability to be vendor agnostic, avoiding the need for a complete infrastructure redesign should a decision be made to change the SIEM provider in the future. The implementation of Snare alongside the new SIEM was a strategic move that provided this flexibility. Such foresight ensures the firm's readiness for future technological shifts and vendor changes, offering peace of mind and enhanced control over the IT strategy.

The addition of Snare Enterprise Agents and a Snare Agent Management Console to its infrastructure has:

- delivered efficient log collection and transfer to QRadar for streamlined data management and security analysis
- provided centralized control and management of the Snare Agents across the entire infrastructure to enhance oversight and system integrity
- ensured scalability in log consumption without compromising performance
- offered compatibility with a diverse infrastructure, including Windows servers, desktops, MacOS, and MSSQL servers
- supported the transition to cloud platforms like Azure and Office 365
- facilitated a two-year data retention strategy, with provisions for online storage and seamless transfer to S3 Glacier for long-term archiving and cost reductions

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com