snare
A PROPHECY SOLUTION

Snare Central on Oracle Cloud Infrastructure (OCI)

Best-of-breed corporate logging, compliance and cyberattack prevention

Snare Central cloud log management on Oracle Cloud Infrastructure (OCI) empowers security teams to monitor, process, analyse, and visualise logs in an easy and manageable way from one central location.

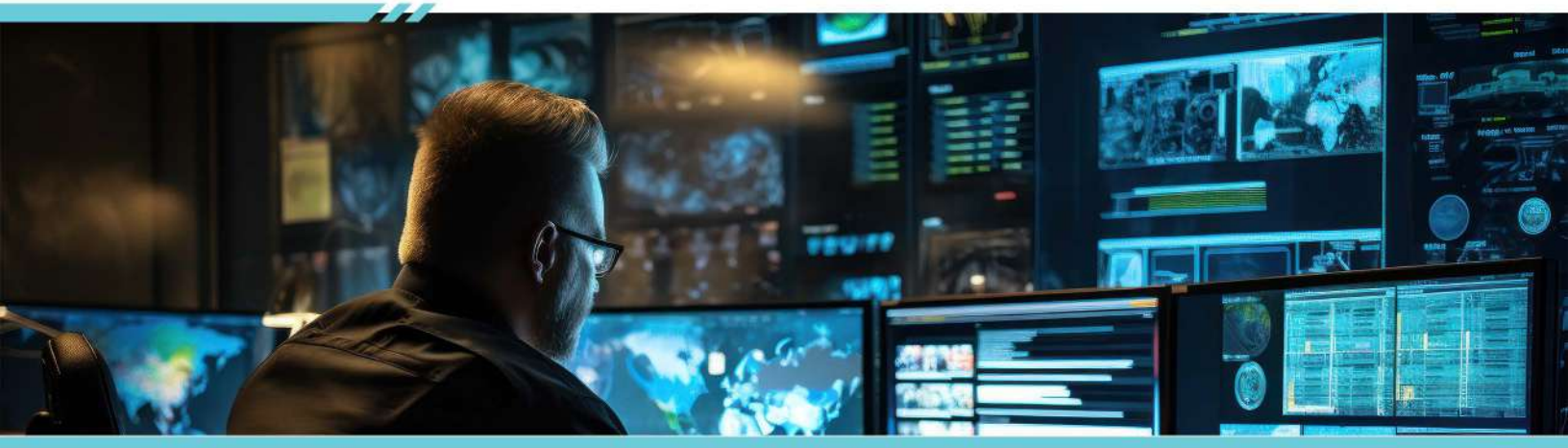
Provides organisations with the ability to meet minimum audit compliance requirements.

Significantly reduces the costs of compliance reporting for cyber.

Assists organisations under ingestion stress to reduce their spend.

Reduce risk while saving time and money

Managing log events with cloud computing services can be complex. Cloud computing environments have a large volume of log data and multiple applications all operating within one single organisation, which can make identifying the source of logging events or data forensics challenging.



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

snare
A PROPHECY SOLUTION

Organisations need a cloud log management solution that is:

FLEXIBLE

Snare Central is the only solution that gives you total control of your logs, empowering you to collect any log from anywhere, while managing what data goes where and to how many places.

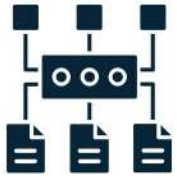
SIMPLE TO USE

Cloud logging services streamline management by offering an interface for routing your logs, making it easier to organise, search, and analyse for standardised reporting and insights.

SCALABLE

Cloud storage simplifies saving historical system logs for future reference, offering scalable capacity that can easily grow with the business.

Snare Central's cloud log management solution is quick –to deploy and simple to scale, in addition to working seamlessly with any security information and event management (SIEM) – consistent with our mantra of reducing risk while saving customers time and money.



Log monitoring system capacity remains independent of your main network, so it should not be slowed by any errors or failures.

Keeping your logs separate and away from the systems that generate the logs is important for forensics, security, and compliance.

Key features and benefits

Snare Centralised Log Management Server
Store and manage logs

Snare Central is responsible for archiving logs, remotely managing agents, routing logs to multiple destinations including managed security service providers (MSSPs), security operations centres (SOCs), and other third-party solutions, as well as Snare applications.

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

snare
A PROPHECY SOLUTION

A Snare Central server can help with the ability to store and manage logs:

- alerts and thresholds focus on possible indicators of compromise (IoC) events
- store events on local storage with automatic retention rules applied
- up to 50:1 compression for long-term historical forensic storage of the security picture
- generate and schedule report distribution
- health checker “heartbeat” to monitor system health
- real-time dashboards for instant data visualisation.

Snare Collector/Parser
Ingest logs from anywhere

Once logged, data needs to be normalised in order to analyse it. Unstructured data means additional work sifting through noise rather than spending time on intelligence.
With the Snare Collector/Parser, you can:

Ingest logs from a variety of sources and formats.

Parse data into a useable format.

Intelligently translate datainto “desired formats”.

Eliminate vendor lock-in.

Filter, truncate, transform and enrich data in log collection pipelines.

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

snare
A PROPHECY SOLUTION

The Snare Collector/Parser lets you ingest logs from anywhere and normalise data from disparate systems and formats:

- server and desktop systems
- network devices (firewalls, routers, switches, and any syslog source)
- Internet information services (IIS), Apache, and other “flat file” sources.

Snare Reflector
Flexible data handling

Collecting and analysing logging information from across disparate systems can be complex. The Snare Reflector can filter, truncate, transform and enrich data in log collection piplines that can forward logs to multiple systems regardless of their format .
The Snare Reflector is used to:

Regain control of log data. Collect once and deliver anywhere in just a few clicks.

Implement a mature & proven enterprise logging architecture. Protecting critical infrastructure and national assets globally.

Tune data and log collection pipelines with unmatched precision.

The Reflector can send data in real-time to one or more destinations, using user datagram protocol (UDP) or transmission control protocol (TCP) with transport layer security (TLS) encryption enabled. We send logs in any of the major formats, including both syslog types 3164 and 5424.

With the Snare Reflector, you will be able to:

- send only high priority logs to analysis engine(s)
- divert holistic overview logs to long-term local storage
- data masking (PCI DSS data, personally identifiable information (PII) data, credit card numbers, social security number (SSN), etc.), limiting and reducing risk
- provide an application-level secure tunnel for events (e.g., receive syslog, transport over TLS, then convert back to syslog on the other end), increasing your security
- multi-tier: complex environments are handled with ease
- consolidate, correlate, send to concurrent stakeholders throughout the business
- feed multiple destinations at once, while tailoring what is sent.

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

snare
A PROPHECY SOLUTION

Asset Management Console
Know what you have and that it is connected and reporting

With Snare's Asset Management Console (AMC/SAM), you will be able to know that your agents are connected and reporting. The AMC/SAM empowers your team to:

Centrally configure and deploy endpoint policies with ease.

Quickly upgrade thousands of agents on endpoints from a central console.

Leverage simple and clear updates to ensure all agents and associated policies are current.

Snare's full Asset Management Console includes full AMC/SAM for managing agents on endpoints:

- manage agent configurations for endpoints
- centralised configuration of endpoint policies
- tailor policies by groups
- perform asset agent upgrades centrally (SAM) – (currently for Windows Enterprise and Windows Desktop agents).

Report Pack
Easily pull reports for compliance

Managing and, importantly, analysing, log data is crucial to staying in front of evolving regulations regardless of what industry you operate in. Event logging and forensic analysis make it easy to comply with these regulations. If an incident occurs, being able to pinpoint exactly what happened is essential to be able to prevent a similar incident from occurring again in the future. A full account of what happened may also be required by the relevant authorities.

Snare Central on Oracle Cloud Infrastructure (OCI)

OCI is the next-generation cloud designed to run any application faster and more securely, for less. Snare Central runs on OCI with on-premise secure agents and provides organisations with the ability to meet minimum audit compliance requirements, significantly reducing the costs of compliance reporting for cyber and assisting organisations under ingestion stress to reduce their spend.

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

snare
A PROPHECY SOLUTION