snare

Extensive Dynamic Affordable

Security, integrity and resilience drive everything we do at Snare

Five reasons snare is the event logging software of choice

1 > Reduced noise

Snare's smart filtering works out of the box with preconfigured settings or you can calibrate to your own environment so you only get the log information you need.

2 > Rapid deployment

The Snare toolset is ready to go from the box. Deployment, even in complex environments, can be deployed and active in minutes — not days or weeks.

3 > Complete log archiving

Reducing noise doesn't mean we're discarding logs. Quite the opposite. Every event is still logged and available for detailed searching.

4 > Plays well with others

Snare connects with nearly every SIEM and MSSP solution on the planet. Changing your SIEM? No problem. Your Snare solution will plug straight into your new platform and continue logging as before.

5 > Support for IT security standards

Snare supports all major IT security standards including HIPAA, PCI DSS, Sarbanes Oxley, (SOX), USA Patriot Act, EU General Data Protection Regulation (GDPR).

Snare Agents are installed in millions of devices across thousands of organisations in sectors ranging from government, healthcare, and automotive to banking and finance, aerospace and manufacturing.

snaresolutions.com

More than 2,000 companies and government agencies around the world rely on the Snare suite of logging tools every day.

That means we can't afford to miss a single critical event, even when it's buried in millions of logs generated by thousands of devices.

That's why the entire Snare suite is built from the ground up to:

- run straight out of the box, no matter how complex your environment
- cut noise by filtering less important events so you can respond to threats and problems faster
- efficiently archive every log for regulatory compliance
- plug in to nearly every SIEM and MSSP solution in the world
- be very light on memory and processing resources

In addition, the logs that Snare Agent generate can be compressed up to 50:1 when storing them on the Snare Central system, saving on storage and communication costs, and helping keep datacentre charges down.

Snare also captures, stores and communicates logs in real-time, which shortens MTTD and MTTR.

In fact, Snare is so fast at generating important event information that it can transmit logs before event logging is disabled on compromised devices, making it harder for intruders to remain undetected.

Snare Central offers the features required by the most demanding IT environments combined with low costs to license, install, maintain, run and retain data.

Introducing the Snare suite

The Snare product suite incorporates everything from a fully-functional, enterprise-grade SIEM through to endpoint solutions that augment your existing network and security infrastructure

Snare Central is our enterprise solution which combines key Snare products into a single, interoperable suite.

Snare Server

Snare Server is a Security Information and Event Management Solution (SIEM), developed in the security labs of the defense industry. It coordinates critical logging functions for even the most complex environments and stores logs, supports forensic searching and ensures IT security standards compliance. It is also the central control point for log forwarding to other applications or nodes and is where reporting and analytics are driven from.

Snare Agent Management Console

The Agent Management Console (AMC) enables remote management of Snare Agents through a workbench interface. The AMC enables administrators to set up automatic audits of the configuration of Agents within their site.

The results of these audits helps administrators identify if the configurations of any Agents have been unexpectedly modified. Using the AMC you can create as many policies and schedules as you need.

Snare Reflector

Having multiple offices in different locations can pose a logging conundrum, but the Snare Reflector can cache, filter, and forward those logs to centralized systems regardless of their format or final destination. Importantly you can use filters to decide what information and how much of it (truncation) needs to be sent. Snare Reflector will cache logs locally if network connections are temporarily lost to the destination, transmitting as soon as the network connections are re-established. This keeps log histories contiguous and ensures compliance requirements are met.

Snare Agent Manager

Snare Agent Manager (SAM) delivers advanced license management for Snare Agents. It is also a central console that includes binary distribution, meaning all Windows 5.1 and later agent upgrades can be managed from one location.

Snare Agents

Snare agents are available for every IT environment. They have a small resource footprint and, importantly, can be installed on Windows endpoints where most breaches, vulnerabilities and transactions are generated.

Operating system agents

Whether you are pulling from servers or endpoints, Snare's agents can find, filter and forward the log data you need. Agents are available for Windows, LINUX, Solaris and OSX.

Database agents

Snare captures and processes logs from MSSQL to monitor critical database functions and allow full database log auditing.

The Snare SQL agent allows the security team to capture critical activity for any or all privileged users on the MSSQL databases and filter out unwanted noisy events. Our intelligent Snare SQL agent installer is also fully cluster aware allowing the admins to deploy the Snare SQL agent across many types of Microsoft SQL clusters with minimal effort.

Epilog agents

Snare's epilog agents collect, process and manage text-based logs across Windows and Linux environments such as Apache, Microsoft IIS, DNS and DHCP among others.

Server/Desktop Windows agents

Snare recognises that Microsoft Windows-based endpoint devices are often the most likely vectors of cyberattack on a network. For that reason Snare offers agents to log activity on desktops and laptops to capture events down to the user level. This is particularly important for ensuring PCI DSS compliance as well as improving overall network security.

Snare Windows Agents also include File Integrity Monitoring (FIM) to ensure compliance with standards such as PCI DSS and ISO-27001. In addition, Snare Windows Agents V5.1 and later are CA Veracode verified, the leading independent application security validation certification.

ca technologies VERACODE VERIFIED STANDARD

> Snare gives you total network visibility. We filter, log and store every event you want to see from desktops to switches, routers, databases and applications. And we tread lightly with an incredibly small footprint, highly compressed log storage and near real-time log transmission.

Contact us

Toll Free US: 1 (800) 834 1060
Denver Office: 1 (303) 771 2666
Asia Pacific: +61 8 8213 1200
UK/Europe: +44 (797) 090 5011

US Headquarters

8480 E Orchard Rd. Suite 4350
Greenwood Village, CO 80111

Corporate Headquarters

Level 1, 76 Waymouth Street
Adelaide, South Australia 5000, Australia

ABN: 84 151 743 976

IT Security standards supported by Snare include, but are not limited to:

C2 / CAPP, California Senate Bill 1386/AB 1950, Danish Standard DS-484:2005, DCID 6/3, DDS-2600-5502-87 Chapter 4, DIAM 50-4, GLBA (Gramm-Leach-Bliley Act), HIPAA, ISO 27001/2, Massachusetts 201 CMR 17.00, NISPOM Chapter 8, PCI DSS, PSPF/ISM, Sarbanes Oxley, (SOX), USA Patriot Act, EU General Data Protection Regulation (GDPR)

ca technologies VERACODE VERIFIED STANDARD

Snare Agent Management Console V1.0 and later and Snare Windows Agent V5.1 and later are CA Veracode Verified at the Standard Status level. As part of this program and the policy we are using we have been able to demonstrate that we have no medium, high or very high coding security vulnerabilities as based on the OWASP top 10 and SANS top 25 coding vulnerabilities. As part of this program and others we have a commitment to provide the best security we can for our customers. The Veracode Verified program independently validates secure software development processes.