snare
A PROPHECY SOLUTION

Complying with ISO27001

Whitepaper

Preparing your business with Snare

The technical controls imposed by ISO (International Organisation for Standardization) Standard 27001 cover a wide range of security features from physical and environmental asset management, to human resources, development, communications and operations management, system monitoring, incident management, business recovery, compliance and policy. This standard is widely considered a best practice guideline for improving Information Security Management Systems, given the wide coverage and multi-faceted approach to security management that it requires. Ultimately, many of the controls mandated by ISO 27001 are replicated in many other information security standards. Adequate collection, management, and analysis of both log data and system events are integral to meeting the ISO 27001 guidelines. Many IT environments consist of heterogeneous devices, systems, and applications; all of which generate log data. The log data that is generated must be captured and analysed, in order to produce actionable insights. Thus, given that millions of individual log entries can be generated daily, or even hourly, the task of organizing the information can be overwhelming without a reliable and efficient system in place. IT teams that attempt to deploy manual or home-grown solutions, often are overwhelmed by the amount of data that needs to be processed.

HOW CAN SNARE HELP WITH YOUR ISO 27001 MANAGEMENT?

Snare enables businesses to automate log collection on their services, servers and workstations by deploying Snare Agents, and can forward log data to an array of third-party SIEM solutions. Snare Agents when used in conjunction with Snare Central deliver log collection, archive and recovery capabilities across your entire IT infrastructure. Further, the system can generate advanced log analysis and reports through a comprehensive list of flexible objective report protocols. Log data is categorized, identified, and filtered for

ease of analysis and reporting. With the click of a mouse or simply by using the included automated scheduler, Snare can help you meet your reporting needs for ISO

Ultimately, Snare Agents flexible collection and filtering abilities, when combined with the powerful reporting and alerting functionality of Snare Central, provides an organisation with the capability to meet corporate security goals by detecting critical issues, providing timely notifications, and empowering the security team and data owners to conduct forensic investigations.

THE 'NITTY-GRITTY' OF HOW SNARE CAN HELP YOU:

Monitoring and Detection (A.10.10)

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.10.10.1	**Audit Logging** Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	Collect audit logs - which record user activities, exceptions and other information security events.	Collects and retains event logs from a wide variety of source systems, applications and network devices. Archiving logs in compressed files - for cost effective, easy to-manage, long-term storage. Archives can quickly and efficiently be restored.	*Status \ General Statistics* *System \ Data Back-up and Data Restore*
A.10.10.2	**Monitoring System Use** Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	Collect the system data which can be sent to Snare Central or a third-party system.	Analysis, archiving, alerting, auditing, and reporting capabilities provide for continuous monitoring of access points across the IT security perimeter(s), and within the core of the organization.	*Operating System Objective Reports* *Network Objective Reports* *Application Objective Audit Report*
A.10.10.3	**Protection of Log Information** Logging facilities and log information shall be protected against tampering and unauthorized access.	Send logs from systems in near real time - prevents tampering of the audit trail on the system that is generating the logs, and minimizes the chance that logs can be deleted or tampered with before being sent to the destination SIEM system.	Small attack surface, access controls to prevent tampering Control access of users Storing file checksums, to help verify that data has not been tampered with	*Operating System \ Login Activity \ Login Failures* *Snare Server Objective Reports*
A.10.10.4	**Administrator and Operator Logs** System administrator and system operator activities shall be logged.	Capture activities of privileged users. Can be deployed across a range of platforms: Windows, Linux, Solaris and Mac OSX platforms, as well as MS SQL Server, web server logs, firewall logs, DNS, DHCP and application logs.	Capture logs from any syslog-capable devices - facilitates log analysis of administrator activity on devices such as firewalls or routers, that cannot run a Snare agents restored.	*Operating Systems \ Administrative Activity* *Operating Systems \ Login Activity*

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.10.10.5	**Fault Logging** Faults shall be logged, analyzed, and appropriate action taken.	Collect system fault logs from the local event subsystem and/or log files on the host, and send the data to Snare Central or another SIEM system. Snare Agents can send logs to Snare Central continuously and on a near real-time basis.	Many objectives to assist in detecting and resolving system faults, and in detecting inappropriate actions being performed on systems. The logs are filtered, analyzed and presented in the Snare Central Dashboard for review. Alarms are activated on critical events that will cause immediate and direct notification to the administration staff.	Reports and investigations for compliance are available at all times. *Application \ Windows Log Data \ Corrupt Events Logs* *System Health Checker*
A.10.10.6	**Clock Synchronization** The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	While the clock synchronization at the host level will need to be performed by the customer, the Snare agents will use the time of the local system for all events that are sent.	The Snare Central system can have its clock set using NTP to any authorized and trusted time source in the customers network. We always recommend that customers have an accurate and trusted time source for all systems as it is critical for any system forensics to have accurate time so that the order of events is logged correctly.	

Human resource security (A.8)

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.8.3.3	**Removal of Access rights** The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Snare Agents can collect all account management activities. Snare reports provide easy and standard review of all account management activity.		*Operating System \ Administrative Activity \ Windows * Accounts Added and Removed Group Changes Groups added or Removed

Communications and operations management (A.10)

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.10.1.2	**Change Management** Changes to information processing facilities and systems shall be controlled.	File activity/integrity monitoring can be used to detect additions, modifications, deletions, and permission changes to the file system of a host system.	Analysis & reporting capabilities can be used to monitor configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations or system activity.	*File and Resource Access \ Sensitive Files* *UNIX Hosts Configuration Change* *Windows Hosts Configuration and Policy Changes*
A.10.3.1	**Capacity Management** The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	Snare Central provides central, secure, and independent audit log storage. When combined with an extensible storage backbone, it provides a level of confidence that capacity will not be exceeded. Snare Central can collect logs from hosts, network devices, IDS/IPS systems, A/V systems, firewalls, and other security devices. Providing central analysis and monitoring of network and host activity across the IT infrastructure. The Snare Central real-time alerting capability can be used to independently detect and alert on threshold violations.		*Health checker reports on Log Volume (By Log Source)* *Systems and agents that stop reporting* *System Critical And Error Conditions* *UNIX Hosts Critical Events and Errors* *Windows Hosts Critical Events And Errors*
A.10.3.2	**System Acceptance** Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to	Snare Central can track and report on patch installation, showing which systems have been patched within the past month, or any other time frame as dictated by organizational policy. For example the Windows Update log can be monitored using a Snare Epilog agent and can send the contents to Snare Central for reporting.		

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.10.4.1	**Controls Against Malicious Code** Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	Snare agents along with Snare Central can detect and provide alerts on a range of malicious activities. Information can be retrieved directly from anti-virus application log files by Snare Epilog agents, which can assist in the process of identifying malware infection inside the environment, and provide administratively useful indications of service disruption and signature update. Such data can supplement AV console functionality, and validate service effectiveness.		
A.10.5.1	**Information Backup** Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	Snare can track and report on when backups are performed within the past month, or any other time frame as dictated by organizational policy.		
A.10.6.1	**Network Controls** Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	Snare Central can collect logs from hosts, network devices, IDS / IPS systems, A/V systems, firewalls, and other security devices. Snare Central provides a central location for the analysis and monitoring of network and host activity across the IT infrastructure. Snare Central can correlate activity across user, origin host, impacted host, application and more. Snare Central can be configured to identify known bad hosts and networks, can verify network firewall controls, and can provide network vulnerability assessment capabilities. Snare Centrals' alarm functionality can be used to independently detect and alert on network and host-based anomalies via sophisticated filtering, correlation and threshold violations.		*Operating System\ Administrative Activity* *Operating System\ Process Monitoring* *Operating System\ File and Resource Access* *Network*
A.10.8.4	**Electronic Messaging** Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	Snare agents along with Snare Central can collect and provide a record of all services used and can alarm on the use of unauthorized modification of system settings or data.		

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.10.9.3	**Publicly Available Information** The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.	Snare Agents file access/integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system.	Snare Centrals' analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.	*Operating System\ Administrative Activity* *Operating System\ Process Monitoring* *Operating System\ File and Resource Access* *Network*

Access control (A.11)

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.11.2.1	**User Registration** There shall be a formal user registration and deregistration procedure in place for granting and revoking access to all information systems and services.	Snare agents along with Snare Central Server collects all account management and account usage activity. Changes to accounts, usage of default accounts and the full detail of authorization and permissions related activity are automatically monitored and can be easily alerted on when nefarious unauthorized activity is detected. Packaged reports are provided to supply full account of all account usage and change history. Snare agents, in combination with the Snare Server, can provide snapshots of user access, and group membership, which can be compared against formal registration and deregistration logs.		*Operating System\ Administrative Activity* *Operating System\ Process Monitoring* *Operating System\ File and Resource Access* *Network*
A.11.5.1	**Secure Log-on Procedures** Access to operating systems shall be controlled by a secure log-on procedure.	Snare Agents along with Snare Central collects all account management and account usage activity. Changes to accounts, usage of default accounts and the full range of authorization and permissions related activity are automatically monitored and can be easily alerted on when nefarious unauthorized activity is detected. Packaged reports are provided to supply full account of all account usage and change history.		*Operating System\ Administrative Activity* *Network*

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.11.5.4	**Use of System Utilities** The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Snare Agents combined with the Snare Central file access/integrity monitoring capability can be used to independently detect access and use of utilities.	Snare Central can collect audit logs reporting on the access and use of utilities on hosts for monitoring and reporting.	*Operating System\ Administrative Activity* *Operating System\ Process Monitoring* *Operating System\ File and Resource Access*
A.11.6.1	**Information Access** Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	Snare Central supplies a one stop repository from which to review log data from across the entire IT infrastructure. Reports can be generated and distributed automatically on a daily weekly or monthly basis. Snare Central provides an audit trail of who did what within Snare Central and a report which can be provided to show proof of reports being generated.		

Information Systems Acquisition, Development and Maintenance(A.12)

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.12.4.2	**Protection of System Test Data** Test data shall be selected carefully, and protected and controlled.	File access/integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes.	Real-time alerting can be utilized to detect and notify of changes to specific configurations.	

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.12.4.3	**Access Control to Program Source Code** Access to program source code shall be restricted.	The Snare Agent file access/integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Filtering capabilities at the agent can be configured to closely monitor particular folders that hold source code material. Analysis & reporting capabilities can be used for monitoring configuration changes.	Real-time alerting can be utilized to detect and notify of changes to specific configurations.	
A.12.5.1	**Change Control Procedures** The implementation of changes shall be controlled by the use of formal change control procedures.		Capable of reporting on operations and configuration changes that may jeopardize the security of the system.	*Operating System\ Administrative Activity*
A.12.5.2	**Technical Review of Applications After Operating System Changes** When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.		Capable of reporting on operations and configuration changes that may jeopardize the security of sensitive data.	*Operating System\ Process Monitoring* *Operating System\ File and Resource Access*
A.12.5.3	**Restrictions on Changes to Software Packages** Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.		Capable of reporting on modifications to operating system software packages via file and executable event monitoring. Patch information associated with individual non-operating-system packages can be supported through the ingestion of relevant application-level logs.	

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.12.6.1	**Control of Technical Vulnerabilities** Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk	Vulnerabilities can be detected by real-time examination tools or by using compatible vulnerability scanning systems. Alarms can be configured to inform the custodian(s) if malware is detected inside the environment.		*Active Scanning\Port and Vulnerability Scan* *Application Audit logs*

Information security incident management (A.13)

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.13.1.1	**Reporting Information Security Events** Information security events shall be reported through appropriate management channels as quickly as possible.		Access controls facilitate ownership of particular reports by users outside the traditional security team. Reports can be made available directly via the web-based user interface, or sent to relevant parties via email.	
A.13.1.2	**Reporting Security Weaknesses** All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.		Access controls facilitate ownership of particular reports by users outside the traditional security team, which can potentially include contractors or third party users. Reports can be made available directly via the web-based user interface, or sent to relevant parties via email.	*Active Scanning\Port and Vulnerability Scan* *Application Audit logs* *Operating System\ Administrative Activity* *Operating System\ Process Monitoring* *Operating System\ File and Resource Access*

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.13.2.1	**Responsibilities and Procedures** Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.		Reports can be tailored to provide very specific information relating to particular information security incidents, in order to support rapid response to particular criteria.	*Active Scanning\Port and Vulnerability Scan* *Application Audit logs* *Operating System\ Administrative Activity* *Operating System\ Process Monitoring* *Operating System\ File and Resource Access*
A.13.2.2	**Learning from Information Security Incidents** There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	Snare Central completely automates the process and requirement of collecting and retaining security event logs. Snare Central retains logs in compressed archive files for cost effective, easy to-manage, long-term storage. Log archives can be restored quickly and easily months or years later in support of after-the-fact investigations. Reports generated by Snare Central can generate PDF reports that can be sent via email, and integrated into normal organisational email classification and archival processes in order to facilitate the measurement of incident numbers and frequencies.		*Status\General Statistics* *System Status*
A.13.2.3	**Collection of Evidence** Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	Send logs from systems in near-real-time. This helps to prevent tampering of the audit trail on the system that is generating the logs and sending to the destination SIEM system.	Ensures audit trails are protected from unauthorized modification. A small attack surface and access controls, restrict the ability to tamper or remove log information to authorized administrators only. The web interface can also control which users have access to administrative functions to delete data, and does not allow modification of log data. It can also produce and store file checksums of all the log data, to help verify that log data has not been tampered with.	

Business Continuity Management (A.14)

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.14.1.2	**Business Continuity and Risk Assessment** Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.		Snare Central collects logs continuously and real-time in the organizational IT environment. The logs are filtered, analyzed and presented in the Snare Central Dashboard for real-time review, and can include log sources that indicate application, system, or network problems. Alarms are activated on critical events that will cause immediate and direct notification to the administration team. Reports and investigations for compliance are available at all times.	*Active Scanning\Port and Vulnerability Scan* *Application Audit logs* *Operating System\ Administrative Activity* *Operating System\ Login Activity* *Operating System\ Process Monitoring* *Operating System\File and Resource Access*

Compliance (A.15)

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.15.1.3	**Protection of Organizational Records** Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	File access/integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system.	Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.	*Active Scanning\Port and Vulnerability Scan* *Application Audit logs* *Operating System\ Administrative Activity* *Operating System\ Login Activity* *Operating System\ Process Monitoring* *Operating System\File and Resource Access*

ISO 27001 COMPLIANCE RECOMMENDATION		HOW SNARE SUPPORTS THE GUIDELINE?		
		SNARE AGENTS	SNARE CENTRAL	EXAMPLE REPORTS
A.15.3.2	**Protection of Information Systems Audit Tools** Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	File access/integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Snare agents can detect indications of audit subsystem disruption, and a heartbeat capability is available in Snare agents, which can be used to detect interruptions to log service collection.	Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.	*Active Scanning\Port and Vulnerability Scan* *Application Audit logs* *Operating System\ Administrative Activity* *Operating System\ Login Activity* *Operating System\ Process Monitoring* *Operating System\File and Resource Access*