HOW SNARE HELPS WITH FISMA

What is FISMA?

The Federal Information Security Management Act (FISMA) requires that all federal agencies document and implement controls for information technology systems that support their operations and assets.

9 Steps for FISMA Compliance

The National Institute of Standards and Technology (NIST) outlines nine steps for FISMA compliance. In particular, the NIST standard 800-53 covers the updated technical controls for FISMA

- **Categorize the information to be protected**
- **Select minimum base controls**
- **Refine controls using risk-assessment procedures**
- **Document the controls in the system security plan**
- **Implement security controls in the appropriate information systems**
- **Assess the effectiveness of the security controls once they have been implemented**
- **Determine the agency-level risk to the mission or business case**
- **Authorize the information system for processing**
- **Monitor the security controls on a continuous basis**

You can learn more by checking out this NIST publication.

Snare Simplifies FISMA Compliance

Fully automate log collection, archiving and recovery across your agency's entire infrastructure with Snare. You'll have the tools at your fingertips to align your organization's risk assessment with forensic investigations, reporting and prioritization settings. To start, the Snare Central Platform automatically performs the first level of log analysis. Log data is categorized, identified and normalized for easy analysis and reporting. With Snare Central's objective reporting features, you will be able to easily conduct forensic investigations around incident response activity and create near real-time alert reports for key areas of your environment.

Complying with FISMA

The Federal Information Security Management Act (FISMA) requires that all federal agencies document and implement controls for information technology systems that support their operations and assets. Standards and guidelines have been developed and published by the National Institute of Standards and Technology (NIST). These published guidelines cover many areas surrounding access control, audit and accountability, incident response, and system and information integrity. Each agency is responsible for implementing the minimum security requirements as outlined by NIST. Agencies are periodically scored to determine their compliance level and the results are presented to Congress. Poor performance can result in penalties and be an embarrassment to agency management and staff.

The collection, management and analysis of log data are integral to meeting many FISMA requirements. The use of Snare solutions directly meets some requirements and decreases the cost of complying with others. IT environments consist of heterogeneous devices, systems and applications all reporting log data. Millions of individual log entries can be generated daily, if not hourly. The task of organizing this information can be overwhelming in itself. The additional requirements of analyzing and reporting on log data render manual processes or homegrown remedies inadequate and costly. Snare Central can help. Log collection, archive and recovery are fully automated across the entire IT infrastructure. Snare automatically performs the first level of log analysis. Log data is categorized, identified and normalized for easy analysis and reporting. Snare's powerful alerting capability automatically identifies the most critical issues and notifies relevant personnel. With the click of a mouse, Snare Central's out-of-the box reporting packages ensure you meet your reporting requirements. Remember that the reports are customizable so you can match them to your exact needs.

FISMA has 20 security control requirement areas that require organizations to implement and perform procedures to effectively capture, monitor, review, and retain log data. The remainder of this paper lists the applicable FISMA control requirements, as specified in NIST 800-53, that our Snare solutions help address. For each requirement, an explanation of how Snare supports compliance is provided. Learn how Snare's comprehensive log management and analysis solution can help your organization meet or exceed FISMA regulatory requirements.

Access Control

NIST 800-53 Compliance Requirements	How Snare Supports Compliance
AC-2 Account Management The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts.	Snare collects all account management activities. Snare Central reports provide an easy and standard review of all account management activity. Example Reports: • Account added or removed • Group member changes • Groups added or removed • User account changes • User and group snapshots also allow review of accounts not logged in for the last 90 days, last login times, user disabled status and other user flags
AC-3 Access Enforcement The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	Snare collects all access activity. Snare Central reports provide an easy and independent review of access control settings and enforcement. Example Reports: • Successful/failed host login activity • Successful/failed out of hours login • Successful/failed windows incidents with various change reports for audit policy, admin user changes, privilege escalations, running tasks, etc.
AC-5 Separation of Duties The information system enforces separation of duties through assigned access organizations.	Snare collects information from production access control systems to help define role usage requirements, determine attempts to cross role boundaries and changes to configurations that can affect separation of duties: Example Reports: • Various reports for Windows incidents and administrative activity • User login activity • Group member changes • User account changes

AC-6 Least Privilege The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets and individuals.	Snare monitors activities by both users and systems to assist in determining necessary access, frivolous access, and resource needs of production systems. Review of activities such as network connections, application access, and system logons can help identify appropriate and inappropriate use according to policy. Example Reports: • User login activity • Network device user access reports • Group member changes • Groups added or removed
AC-7 Unsuccessful Login Attempts The information system enforces a limit of specific number of consecutive invalid access attempts by a user within a certain time period. The information system automatically locks the account for a specified time period and delays next login prompt after a set time frame has expired.	Snare collects all authentication activity. Snare Central reports provide an easy and standard review of unsuccessful login attempts to systems and applications. Snare Central alerts can detect and report on multiple unsuccessful login attempts. Example Reports: • Failed login attempts by user • Failed logins for locked accounts • Out of hours logins • Interactive and network logins

AC-13
Account Management
 	
The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.
	Snare collects all access activity. Snare Central reports provide an easy and independent review of access control settings and enforcement.
	
	Example Investigations:
	• Administrative activity
	  ○ Accounts added or removed
	  ○ Audit logs cleared
	  ○ Audit policy changes
	  ○ Group changes
	  ○ Groups added or removed
	  ○ User account changes
	• File and resource access
	• Process monitoring
	• Sensitive application tracking
	• File integrity and registry integrity monitoring

AC-17 Remote Access The organization authorizes, monitors, and controls all methods of remote access to the information system.	Snare collects all account management activities. Snare Central reports provide an easy and standard review of all account management activity: Example Reports: • Network device user access reports • System user login activity, both local and remote connections, SSH, type 3 and 10 logins for windows

AC-18 Wireless Access Restrictions The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, and controls wireless access to the information system.	Snare Central can collect all access activity via syslog. Snare Central reports provide an easy and independent review of access control settings and enforcement. Example Reports: • Successful/failed logins to hosts by user • Successful/failed application access by user • Successful/failed file and resource access by user • Process monitoring • Sensitive application tracking • File integrity and registry integrity monitoring
AC-19 Access Control for Portable and Mobile Systems The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.	Snare Central can use geolocation in reporting for firewall, VPN and web server access. That allows for correlation and event monitoring based on location relative to the organizational networks to determine inbound, outbound, and local network traffic. Remote access and usage activities from mobile devices can be monitored by observation of the logs from authentication systems, security systems and production servers.
AC-20 Personally Owned Information Systems/Use of External Information Systems The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.	Snare Central collects remote access activity. Snare Central reports provide easy and independent reviews of external access to information systems. Example Reports: • Remote access activity by user for host-based systems • Remote access activity by network and VPN devices

Audit & Accountability

NIST-800-53 Compliance Requirements	How Snare Supports Compliance
AU-2 Event Logging The organization needs to determine which log types are necessary and coordinate across the business. An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes; failed logons or failed accesses related to systems; security or privacy attribute changes; administrative privilege usage; PIV credential usage; data action changes; query parameters; or external credential usage. In determining the set of event types that require logging, organizations should consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.	Snare Agents help comply with this by collecting the needed logs from the host platforms and providing the flexibility to collect the needed log event types, including host-based audit logs, application logs from web servers, and custom application logs. Many log types may be required for forensic investigations. Examples: • Windows event logs • Linux audit logs • Web server logs • Application logs such as DHCP, DNS, email, Database SQL activity, custom application logs • Network device access • IDS and IPS • Honeypot log feeds
AU-3 Content of Audit Records The contents of the audit logs must provide the needed forensic details.	Snare Agents collect the needed details on the events: what type the event was, when it occurred, where the event occurred, the source of the event, outcome of the event user identity of the event and objects associated with the event, as well as the time details of the event, which are linked backed to a trusted NTP source that the systems use.

AU-4 Audit Log Storage Capacity The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of the capacity being exceeded.	Snare Central provides this. The customer decides how much storage they want to use to keep the logs. We have a disk management option that allows the customer to grow their archive location when they add more disks to the system. Snare Central is also designed to collect the logs away from the system generating the logs. The Central Log Management collection platform is also referred to as a CLM.
AU-5 Response to Audit Logging Process Failures Audit logging process failures include, for example, software and hardware errors; reaching or exceeding audit log storage capacity; and failures in audit log capturing mechanisms. Organization-defined actions include overwriting oldest audit records; shutting down the system; and stopping the generation of audit records.	Where the endpoint system has hardware or auditing failures, the Snare Agents can collect that additional information from the system. If the agents were to go offline then Snare Central will report it in the healthchecker for the last contact time for the agent or other syslog systems reporting to Snare Central. The healthchecker can raise email alerts for any amber or red alert it detects. Snare Central will also report alerts for other various local issues such as storage/ disk space, caching capacity, reflector destination problems, file integrity issues with changes to the OS or data store, and device EPS rate changes either higher or lower than normal. The Agents will also report if they detect audit logs being cleared on Windows platforms as well as system reboots and service resets.

AU-6 Audit Record Review, Analysis and Reporting The organization regularly reviews/ analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.	Snare Central provides the options to perform audit log review analysis and reporting. Snare Central provides dynamic review of the logs in real time using the ad hoc search capabilities as well as scheduled reports for specific areas. Snare has over 300 out-of-the-box reports, covering operating system and network devices. Customers can create custom reports for their specific needs as well as for third party application log analysis. Snare Central provides centralized monitoring, analysis, and reporting of audit activity across the entire IT infrastructure. Snare Central automates the process of identifying high-risk activity and prioritizes based on asset risk. High-risk activity can be monitored in real time or alerted on bases. Snare Central reports provide easy and standard review of inappropriate, unusual, and suspicious activity. Example Reports: • Accounts added and removed • Accounts disabled • Privilege escalation • Local accounts added to Administrators group • Maintenance activity by user • Administrator changes • Group changes • Group member changes • Policy changes • User account changes • Software installation and services being installed • Startup and run task alerting • Login type 3 and 10 remote access

AU-7 Audit Record Reduction and Report Generation The information system provides an audit reduction and report generation capability.	Snare Agents includes an audit log sequence number for all records, along with the date and time so it helps to show the order the events were generated as. The Agents have a filtering option to reduce noise for unwanted events. Snare Central also has reporting options to reduce and filter out unwanted events from the reporting process to allow users to get to the specific events they want to see. The events can be viewed and sorted in various ways including tabular raw data, charts, and heatmaps. None of the audit log raw data is ever alerted in contents. All of the data can be reviewed on demand as needed. Snare Agents' policy-based log processing capabilities provide automatic audit log reduction by reducing the noise of unwanted events. "Interesting" audit logs can be forwarded as events for immediate monitoring and/or alerting. "Uninteresting" audit logs can be filtered out and/or retained at an archive-only level. Snare Central analysis and reporting facilities provide aggregated views of audit data, providing further audit reduction. Snare Central provides extensive report generation capabilities with over 300 out-of-the-box reports.
AU-8 Time Stamps The information system provides time stamps for use in audit record generation.	All audit records contain time stamps using the host time, which should be from a trusted NTP source. Snare automatically and independently synchronizes audit log time stamps to the local system time or an absolute time standard (GMT). This ensures the true time of the occurrence is known for audit log analysis and reporting. When the customer has to collect logs from multiple geographic time zones, the Snare Agents can send logs in GMT time so all logs are one consistent time.

AU-9 Protection of Audit Information The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Snare Central keeps all of the logs in a central location that has restricted access to protect the data. Only administrative users have access to the backend. Designated users can have access to the web UI and be assigned roles based on role-based access controls, seeing only the parts of the systems and functions they are allowed to see and use. As Snare Central is a software appliance, it does not use write once only media; it's using disk drives. It does have the option to backup data to DVD or other write once media when required to export the data for long term. Snare Central runs hashing checks of the operating system and data store to check for any changes. Any changes are reported via the healthchecker which can send a real-time alert to designated email recipients. Split passwords can be used for dual authentication for the administrator accounts in the UI and for the backend root and Snare logins. All of the audit log information in Snare Central is in read-only mode from the UI and users can never change the data.

AU-10
 	
Non-repudiation
 	
The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.
	The logs collected from the end systems using the Snare Agents provide the non-repudiation evidence to show what user actions were on the end systems. All actions within Snare Central also provide local logs for all actions performed on the system, both at the operating system level and from within the web UI. Logs can be sent using TLS encryption to prevent tampering of the logs in transmission. Additional checksum options are also available to validate the logs have not been tampered with. All Snare Agent logs also contain a sequence number to also show if a log was missing. Along with file integrity checks on the Snare Central side, it will also show if logs files were tampered with and raise alerts in the healthchecker.
	
	Snare collects all access activity. Snare Central reports provide easy and independent review of access control settings and enforcement.
	
	Example Investigations:
	
	• Successful/failed logins per host/system access by user
	• Successful/failed application access by user
	• Successful/failed file access by user
	• Incident reporting for Windows platforms
	  ○ Administrative activity
	  ○ File and resource access
	  ○ Process monitoring

AU-11 Audit Record Retention The organization retains audit records for an appropriate time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Audit log retention in Snare Central can be configured to suit the business needs and logs can be purged after specific times and dates on a schedule to comply with the business policies. Snare Central completely automates the process and requirement of collecting and retaining audit 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. Snare Central gets on average between 40:1 and 50:1 compression on the raw logs. Logs can be purged after defined retention times and can be configured to comply with policy needs.

AU-12 Audit Record Generation Audit records can be generated from many different system components. The event types specified in AU-2d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.	Snare Agents can be configured to run in two modes: one to collect the logs as they are set based on the local system or group policies when on Windows; or two (the default) to configure the local audit policies to enforce the generation of the specific log types needed. When the default option is used, if someone tampers with the end system and disables a policy, the Snare Agent will turn it back on while also sending the log of the policy being disabled and then re-enabled. The Snare Agents provide a standard system-wide log format to be sent to Snare Central and other standard syslog formats. Snare Central also has a reflector that can reflect the logs in near real time to other Snare Centrals for high availability/redundancy, as well as other SIEM systems in various standard syslog formats.
AU-14 Session Audit Session audits can include monitoring keystrokes, tracking websites visited, and recording information and/or file transfers.	Snare Agents can collect the various log files from websites using the logs from web servers like IIS and Apache. It does not track key strokes on the system but can monitor all user activities like running commands, access files and network resources. System start-up and reboots are logged.
AU-15 Cross Organizational Audit logging When organizations use systems or services of external organizations, the audit logging capability necessitates a coordinated, cross-organization approach.	Snare Central can reflect the logs it receives to other Snare Centrals or other SIEMs that cross organizational boundaries when configured to do so. These logs can be filtered to only send the needed logs to the other system as well as data masked, if needed, to protect the privacy of some information. All the identity of the original log data is preserved by default.

Certification, Accredidation & Security Assessments

NIST 800-53 Compliance Requirements	How Snare Supports Compliance
CA-2 Security Assessments The organization conducts an assessment of the security controls in the information system periodically to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Snare Central's log analysis and reporting capabilities can be leveraged during a security assessment to help ensure implemented controls are functioning as intended and to potentially identify any weaknesses.
CA-3 Information System Connections The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.	Snare Central can collect network device logs. Snare Central's analysis and reporting capabilities can be used for reviewing network activity to ensure only authorized communications occur. Snare Central alerts can be used for detecting unauthorized communications.

CA-4 Security Certification The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Snare Central's log analysis and reporting capabilities can be leveraged during a security certification to help ensure implemented controls are functioning as intended and to potentially identify any weaknesses.
CA-7 Continuous Monitoring The organization monitors the security controls in the information system on an ongoing basis.	Snare Central's monitoring, analysis, and reporting capabilities provide for continuous monitoring of specific controls across the IT infrastructure. For instance, Snare Central alerts can detect the use of restricted accounts.
CM-4 Monitoring Configuration Changes The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.	Snare Agents file integrity monitoring capability that can be used to detect the following changes to the file system and registry keys: • Additions • Modifications • Deletions • Permissions Snare Central's analysis and reporting capabilities can be used for monitoring configuration changes. Snare Central alerting can be utilized to detect and notify of changes to specific configurations of files or registry keys.
CM-5 Access Restrictions For Change The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.	Snare Central collects all access activity and changes to access controls. Snare Central reports provide easy and independent review of access control settings and enforcement. Example Reports: • Access granted/revoked by user • Access granted/revoked by object • Login failures for locked accounts • Successful/failed file and registry access by user • Successful/failed host and login access by user • Successful/failed application access by user • File integrity and registry monitoring

Incident Response

NIST 800-53 Compliance Requirements	How Snare Supports Compliance
IR-4 Incident Handling The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The logs and reporting in Snare Central can help with the incident management process and forensic analysis of the activity.
IR-6 Incident Reporting The organization promptly reports incident information to appropriate authorities.	Snare Central's notification capabilities can route alerts to the appropriate individual based on email alias, group membership or relationship to the impacted system. Snare Central reports provide summary and detail level reporting of incident-based alerts.
IR-7 Incident Response Assistance The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.	Snare Central's integrated knowledge base provides information useful in responding to and resolving incidents.

Maintenance

NIST 800-53 Compliance Requirements	How Snare Supports Compliance
MA-3 Maintenance Tools The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.	Snare Agents can collect user and application activity on the systems along with process execution activity. Snare Central can report on system application installs and process execution activity on the system to track the usage of maintenance tools and other applications. Example reports: • Successful/failed application access by user • File integrity and registry monitoring • Process monitoring/sensitive applications • File and Resource Access/Sensitive Applications
MA-4 Remote Maintenance The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.	Snare Central can identify maintenance related activity for analysis and/or reporting. Snare Central reports provide easy review of remotely executed maintenance activity. Example Reports: • Maintenance activity by user with user adds and removes • Maintenance activity by host with changes in configuration and policies • Remote access summary by user from network devices and VPN remote access • Remote access by application with collection and review of application logs.

MA-5 Maintenance Personnel The organization allows only authorized personnel to perform maintenance on the information system.	Snare Central can identify maintenance related activity for analysis and/or reporting. Snare Central reports provide easy review of maintenance activity. Example Reports: • Maintenance activity by user • Administrator changes • Group changes • Group member changes • Policy changes • User account changes • Software installation and services being installed • Start-up and run task alerting

Physical & Environmental Protection

NIST 800-53 Compliance Requirements	How Snare Supports Compliance
PE-6 Monitoring Physical Access The organization monitors physical access to the information system to detect and respond to physical security incidents.	Snare Central reports provide easy review of terminated personnel to ensure access rights have been removed. Snare Central alerts can be used to detect usage of should-be terminated user accounts. Example Reports: • Accounts added and removed • Accounts disabled • Privilege escalation • Local accounts added to Administrators group • Maintenance activity by user • Administrator changes • Group changes • Group member changes • Policy changes • User account changes • Software installation and services being installed • Start-up and run task alerting • Login type 3 and 10 remote access

Personal Security

NIST 800-53 Compliance Requirements	How Snare Supports Compliance

PS-4
Personnel Termination
 	
The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.
	Snare Central reports provide easy review of terminated personnel to ensure access rights have been removed. Snare Central alerts can be used to detect usage of should-be terminated user accounts.
	
	Example Reports:
	• Accounts added and removed
	• Accounts disabled
	• Privilege escalation
	• Local accounts added to Administrators group
	• Maintenance activity by user
	• Administrator changes
	• Group changes
	• Group member changes
	• Policy changes
	• User and group snapshots
	  ○ Disabled user account information
	  ○ Account groups
	  ○ Account last login
	  ○ User flags

PS-5
Personnel Transfer
 	
The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.
	Snare Central reports provide an easy review of transferred personnel to ensure access rights have been terminated and/or appropriately modified.
	
	Example Reports:
	• Accounts added and removed
	• Accounts disabled
	• Privilege escalation
	• Local accounts added to Administrators group
	• Maintenance activity by user
	• Administrator changes
	• Group changes
	• Group member changes
	• Policy changes
	• User and group snapshots
	  ○ Disabled user account information
	  ○ Account groups
	  ○ Account last login
	  ○ User flags

Sytems & Communications Protocol

NIST 800-53 Compliance Requirements	How Snare Supports Compliance
SC-7 Boundary Protection The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	Snare Central can collect boundary device logs from routers, firewalls, VPN servers, etc. Snare Central can alert on unauthorized or suspicious activity. Snare Central reports provide a consolidated review of internal/external boundary activity and threats.

SC-8 Transmission Confidentiality and Integrity Protecting the confidentiality and integrity of transmitted information applies to internal and external networks, and any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios.	Snare Agents can transmit the logs over TLS to protect the confidentiality and integrity of the logs over the network. Snare Central can collect logs over TLS and also reflect the logs to other systems that can support TLS protocols.
SC-13 Cryptographic Protection Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information; the provision and implementation of digital signatures; and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals.	Snare Agents and Snare Central can use FIPS based algorithms for hashing and encryption of data while in transit.
SC-15 Collaborative Computing Devices and Applications The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.	Snare Central may be able to identify, report and/or alert on the initiation of specific collaborative computing activity.
SC-18 Mobile Code The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.	Snare Central may be able to identify, report and/or alert on specific mobile code activity.

SC-19 Voice Over Internet Protocol The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.	Snare Central may be able to identify, report and/or alert on specific VoIP activity where network detection devices can send the relevant log data to the system.

Systems & Information Integrity

NIST 800-53 Compliance Requirements	How Snare Supports Compliance
SI-4 System Monitoring The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system.	Snare Central can collect logs from IDS/IPS systems, A/V systems, firewalls, and other security devices. Snare Central provides central analysis and monitoring of intrusion related 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. Snare Central customizable objective dashboards provide customized real-time monitoring of events and alerts.
SI-5 Security Alerts and Advisories The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	Snare Central can alert on specific intrusion related activity. Users can be notified based on department or role.

SI-7 Software and Information Integrity The information system detects and protects against unauthorized changes to software and information.	Snare Agents' file integrity and registry monitoring capability can be used to detect the changes to the file system. Snare Central can be used to report on the changes as reported from the Snare Agents. Activity such as the following can be reported on. • Additions • Modifications • Deletions • Permissions This capability can be used to detect unauthorized changes to software, and configuration settings in the registry on Windows systems and information.