



Snare & NIST

Zero Trust Model

Whitepaper



Snare and NIST Zero Trust Model

Introduction

Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. NIST has established this Zero Trust security architecture in order to promote a "deny until verified" approach to resources accessed from inside and outside the organizational network. ZT helps to combat the complexities of modern corporate networks and infrastructure. A modern internet-connected enterprise has multiple remote access methods, allows mobile users, and integrates cloud services; as such, there is no single identifiable perimeter for the enterprise. Managing a network with perimeter-based security models has been shown to be insufficient - once an attacker breaches the perimeter they can often move laterally around the network, unhindered and potentially undetected.

The NIST Zero Trust paper is available from the following location:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800207.pdf>.

Executive backing

On Wednesday May 12, 2021, President Biden signed an [executive order](#) aimed at strengthening U.S. cybersecurity. The order was prompted by a series of sweeping cyberattacks on public companies, companies that supply the U.S. Federal Government, and Federal Government networks over the past year. Examples include the 2020 [SolarWinds attack](#), and the most recent attack on the Colonial Pipeline by the hacker group "DarkSide".

Both attacks are examples of criminal groups and state actors exploiting U.S. cyber vulnerabilities. To help protect the U.S. Government, agencies, and both public and private companies from future attacks, the May 12 Presidential Executive Order calls for the Federal Government and private sector to partner to confront "persistent and increasingly sophisticated malicious cyber campaigns" that threaten U.S. security.

How Snare Can Help

Snare can help organizations meet existing and new cybersecurity requirements laid out by the Executive Order, and improve organizational cyber posture.

- **Central log collection, analysis and reporting** – by collecting all important logs from critical assets in the business, Snare facilitates the identification and monitoring of advanced persistent threats (APT) and can forensically analyse the actions of criminal groups attempting to infiltrate in the network or move laterally through organizational assets. Without effective logs, you are flying blind with no clear awareness that an incident is in progress or has happened in the past.
 - *Government agencies and businesses need to know:*
 - **Who** did the actions. Was it a normal user, or an administrator? Were credentials breached? How much lateral movement was involved?
 - **What** data or systems were affected, how many were there, and which networks were affected? What commands were run on each system? What parameters were used? Were other tools loaded to help the attacker? Was data exfiltrated out of the environment? Have they established a beachhead in the network for future exploitation?
 - **When** the activities occurred. Covering the exact time and dates. Was it small attacks over a wide range of time, or a focused effort over a short period?
 - **Where** the specific actions took place.
 - **How** did they do it? What path was taken? Was it user access breach? Was it zero-day exploit?

Having [Snare Central](#) or [Snare Agents](#) in place can help security teams gather the forensic data required to answer who, what, when, where, and how – and ‘how bad is it’.

Zero Trust Initiative

Snare provides several mechanisms to detect attacker activity. The [Zero Trust](#) initiative indicates that detection is the key to ensuring controls are functioning correctly. If there is nothing to perform analysis on, there can be no validation of technical controls working correctly, and no information for adequate remediation in the event of a problem or incident response.

Section 3(e) states that within 90 days all agencies should implement a logging solution to:

- **Collect logs from as many sources as possible** – all servers, desktops, network devices, everything that can send a syslog event. All devices should have some form of logging or monitoring in place.
- **Use FIM, FAM, RIM and RAM to track and monitor all key files and system configuration.** Know who changed a file, when the files were changed, and what tools were used.
- **Use Database Activity Monitoring (DAM) to track key activity on SQL databases.** Know if admin accounts are being abused and verify that key data has not been tampered with.
 - **Collect evidence** to show the attack mechanism - logs can assist in identifying whether the attack came in via email, USB, a web link download, or a software update.

The Snare software suite provides an easy-to-use solution that is fast-to-deploy using our lightweight agents and [Snare Central Server](#) centralized logging platform. **Most sites are up and running in as little as an hour**, and immediately capable of collecting and reporting on activity.

As for our v8.4 release, we have over 550 out-of-the box, customizable reports, a dynamic query feature that facilitates advanced searches and data drilldown, and active dashboards provide key statistics on system logs, and real time alerting and threshold reporting,

Snare Central provides a comprehensive logging, detection, and analysis tool for any cyber team.

Snare does not link licensing with forensic storage - customers are not penalized for collecting and storing a wide range of forensic information for later analysis in the event of an identified incident. Subject to server resource availability, customers can collect as much data as they like and keep it for as long as they need. Data often needs to be retained for several years to track bad actors who have been in a network for an extended time and keeping a low profile to help avoid detection.

As per 7 (c,d), the [Snare CLM](#) suite helps to facilitate and compliment EDR solutions with enhanced logging and detection to provide a source of forensics data for threat hunting activities.

For Windows-based systems, Snare Agents integrate with the Windows Sysmon utility to collect additional forensics data including but not limited to: user actions, process activity, PowerShell usage, DNS usage, command parameters, additional hashes used on commands and files, file system and permission changes, drivers and signatures, network actions with IP and port protocol details, registry changes, events seen early from system boot to track system startup just a name a few areas.

These additional forensic events can provide additional context for incident response processes.

As per 8(b), Snare Central and Snare Agents use cryptographic hashing functions to detect event tampering. The Snare tools use multiple levels of validation of data to detect any malicious activities.

In a typical Snare deployment, logs would be collected from all systems - ie: all servers and desktops, all network devices such as firewalls, routers, switches, wireless access points etc. Snare Agents should be deployed on all systems capable of running an agent to track user and system activity. All network devices should be configured to send their activity logs to Snare

Central for short or long-term storage, threat hunting and compliance reporting. Snare Central can then be used to filter, tag events, and reflect the logs to other SIEM systems for further analytics and threat detection.

NIST ZT highlights that the standard model of having only role-based access controls and trusted authentication mechanism is not enough for a modern organization. There are many zero-day exploits that bypass the authentication subsystem and role-based access controls, giving the bad guys administrator-equivalent access to the system.

Monitoring networks and systems for unauthorised activity helps with the "who, what, when and where" covered above to determine how attackers got in and determine the incident danger and exposure.

Snare Agents can also be used in networks separated by a data diode, where the physical return path of the network is cut, and the data can only travel one way due to the security of the network. This allows forensic log data to be collected from low security networks and consolidated and reviewed on higher security systems. This avoids the layers of authentication and access controls required by agentless solutions and negates the trust requirements between networks of different security levels.

Snare is under complete control of the customer. There are no hidden automatic updates to pull down changes from the Internet without the customer's awareness. Snare is designed to operate in air-gapped networks and does not need to phone home to the internet to send to receive information. Customers control their updates and download the software from the portal so they can vet the software and test it via change control processes before internal deployment.

There are many areas and use cases that Snare Agents and Snare Central help facilitate such as:

- constantly collect data relating to the actions of users on systems and
- network devices securely retaining data for as long as the organization

needs, away from the systems that generated the data where the risk of data tampering is high

- provide regular scheduled reporting on what users are doing and what commands or tools they are running
- provide regular review of user privilege levels and access to sensitive information, in order to see unusual usage patterns
- provide a capability to execute "what if" data analysis and hunting for threats and usage patterns. use standard capabilities to see
 - data patterns with heatmaps, graphs with tabular output cross link and correlate data over multiple data sources and systems, for common data elements.
 - tracking when users are performing activities; Is it during normal working hours or out of hours
- tracking lateral movement around the network, and monitoring remote access from local systems
- monitor privilege escalation, and track whether escalation was via a privileged shell, a software flaw, or an application escalation. Determine whether role-based access controls were circumvented.
- Monitor for abnormal software behavior to detect viral or supply chain compromise, such as an application that accesses systems or network ports or resources without reason, or running commands when it should not
- detect data that has been changed or accessed in sql databases. Determine what tools were used, and from what systems the databases were accessed
- Monitor system and network traversal for situations where data was copied out of the system

All these sorts of questions can be answered with the collection of the relevant logs from systems, applications, and devices. Snare also has broad coverage with the MITRE ATT&CK framework that helps the security teams with detecting known APT threat actors using standard out of the box capabilities. <https://www.snaresolutions.com/portfolio-item/mitre-attack/>