

# Agent vs Agentless Log Collection

## Summary of Agents vs Agentless Features

Feature	Agents	Agentless
Minimal chance of logs being tampered with	✓	Logs can be deleted or tampered with before collection occurs
Event processing resource overhead distributed over time and have low CPU cost	✓	Higher system resources used for authentication and log collection.
Virtual Application Firewall • functions limited to agent options	✓	Remote access requires admin privileges which can exceed business need and pose an additional security risk
Firewall Friendly with traffic flow	✓	Not firewall friendly as multiple ports need to be open to allow authentication
Support data diode capability with one-way traffic flows	✓	Not possible as traffic must flow both ways to authenticate and collect logs
Streamlined authentication model • no duplication of host administrator credentials	✓	Administrator credentials need to be duplicated
Processing of logs in near real time	✓	Logs are processed in batch mode and incur higher CPU overhead
Event Rate per Second Controls	✓	Agentless collection does tend to have concept limiting event rate collection, some do have limits on data transfer speed.
Log filtering at the source	✓	Filtering must be applied either at time of collection or at the SIEM system after data has been transferred
Log filtering from the remote collection	Filtering is performed at the agent	
Enforcing local audit policy	✓	Policy cannot be enforced
Central audit policy controls via agent management console	✓	No central control on policy

# Agent Background

For many years systems have produced logs of various types, including Security logs, Application logs and System logs. All the logs have various levels of importance and provide different views of user, system and application activity that assist with forensic analysis of usage.

Most systems, such as Windows and Unix, create logs in areas of the file system that require high level privileges to view, rotate, or relocate. In many organisations, privilege separation implies that the individuals or team responsible for reviewing log data, do not have a legitimate need for broad, high level privileged access. To facilitate this role separation between system or application administrators and security verification and monitoring teams, agents were developed to collect security related information from the local system and then convert it to a format suitable for transmission over the network to a central collector. The agents were designed to run in the background with sufficient privileges to monitor and manage the logging subsystem, utilising only those system resources necessary to collect, process, filter and send the logs to the SIEM host with minimal overhead.

## This architecture has several benefits:

- The agent can function as an application-level 'firewall'. Although it may need to run with full system privileges in order to function on the native operating system, it can provide an interface to external users that is limited only to the functionality required to view and/or manage log data. As such, external/remote access network controls are not weakened to allow remote administrative access into the Operating System, for the sole purpose of accessing the logging subsystem.

Agent-based solutions tend to be firewall-friendly in terms of network flow, compatible with networks that implement multi-level security, and can even work in organisations where unidirectional (data-diode) transfers are mandatory. Agentless collection generally requires remote access to retrieve logs, which may violate the network security policy.

- A push-based system, using agents on the source system means that authentication infrastructure and network access controls can be significantly streamlined.
  - In order to automate log collection and management, privileged user credentials and/or certificates often need to be stored on the server that collects the data. Unless the collection server utilises native passthrough authentication on each and every target system, change management is complicated by the requirement to propagate and record password changes to the collection server when changed on any system that provides log data. Although viable in organisations with a small and/or homogeneous computing environment, in larger installations the security management overhead and associated operational security risks can be a significant barrier to adoption, and can

significantly increase the challenges associated with implementing the requirements of PCI DSS, SOX or related regulatory frameworks - particularly in areas relating to password rotation and management.


- For systems that must be accessed through firewalls, network access controls required to support remote authentication can be a complex administrative overhead - particularly when Windows systems are involved, with a range of bidirectional communications being required over several network ports.
- Logs can be processed in near real time and sent rapidly to the destination SIEM system. This helps to ensure that there is minimal chance of logs being modified or deleted by a malicious user to hide evidence of a successful attack, before any remote collection process occurs.
- System overhead is distributed in small chunks throughout the operating cycle of the systems on which the log data is generated. Agentless implementations have to remotely connect, login and then access log data in batch mode, which tends to induce significant CPU and related resource spikes. System login process can be very expensive with operating system calls to authenticate the user, create memory space then start up programs and processes to then perform their desired function. A simple example of this is the boot time it takes for a host to load the operating system and all of its background processes and the general login process and the time it takes. None of these activities are fast and all incur a high system load. Most system administrators can tell how their systems spike in the mornings and after break times when people log back into their systems after being away.

- Agents can implement log filtering more efficiently. Agents filtering introduces additional intelligence at the hostend, to include, or discard events based on complex criteria that meet organisational security policy requirements. This filtering that is beyond the capabilities of the native event system. This means that the volume of data that needs to transit the network can be significantly reduced, and the processing required to discard events of no security significance, is distributed across a cluster of source systems.
  - File auditing on most operating system auditing implementations, is generally lacking support for the sort of advanced filtering requirements that can meet corporate or national security requirements, particularly those relating to FIM, without flooding local resources and review staff with vast amounts of information.
- Agentless environments can face additional challenges when attempting to enforce consistent local audit policy settings. System settings can be changed locally, without the knowledge or concurrence of the collection server. This could render the collection process useless, or potentially result in vital information not being available for collection. Using an agent with a predefined, centrally managed configuration can simplify the deployment and maintenance of these policy requirements and provide a central overview of all policies and collection rules that the business requires without the need for another central policy control tool such as Active Directory.
  - On Windows systems, audit settings can be controlled by a centralised Group Policy. However, in many organisations that have one or more segregated network zones (such as a DMZ network, or standalone special purpose workstations), systems may run in standalone mode and require local policy settings to be applied. Implementing all of these settings manually can be resource intensive.
- Event Rate per Second (EPS) throttling. Agents are very well suited for managing the speed that logs are sent at. Setting the EPS so the client system will only send logs at a policy defined speed can reduce any spikes in network load for systems that have to send logs over slow WAN links. Not all agentless collection systems can manage the network EPS or bandwidth usage for transferring the logs to the central SIEM system.
- Systems that are designed to send their logs in real time to a syslog collector implement a pseudo-agent-based solution, with logs generally not stored on-system for significant periods of time. Such devices are usually routers, switches, firewalls, wireless access points etc. These devices are designed to generate system logs and then send them real time to a destination SIEM system, without the need for an agent.



The agents were designed to run in the background with sufficient privileges to monitor and manage the logging subsystem, utilising only those system resources necessary to collect, process, filter and send the logs to the SIEM host with minimal overhead.





In summary, agents in general are designed to simplify the configuration and collection needs of the host. Be it a windows agent collecting from the windows event log subsystem, an agent collecting from local application log files from a custom application or web server logs, the process should only take a few clicks and setting the destination IP address details and then logs can start to flow.

The setup costs for remote access and collection in an agentless environment are usually non-trivial, will incur a higher administrative overhead to implement and will generally imply additional management of passwords, firewall rules and change management.

There are several Snare Enterprise agents that are available that can support host log collection needs:

- Snare Enterprise Agent for Windows
- Snare Enterprise Agent for Linux
- Snare Enterprise Agent for Solaris
- Snare Enterprise Agent for Mac OS
- Snare Enterprise Epilog for Windows and Snare Enterprise Epilog for Unix will collect from any text-based application log file.

## About Us

Prophecy International's Snare leadership team are top information technology security specialists with decades of experience in IT Security, including host intrusion detection. Our solutions continue to be used and trusted in the most sensitive areas of Government and private sectors.

Prophecy International intend to continue releasing tools that enable users, administrators and clients worldwide to achieve a greater level of productivity and effectiveness in the area of IT Security, by simplifying, abstracting and/or solving complex security problems.



### Contact us

The Americas: 1 (800) 834 1060  
Toll Free Denver: 1 (303) 771 2666  
Asia Pacific: +61 8 8213 1200  
UK/Europe: +0 (800) 368 7423

### Head Office

Level 1, 76 Waymouth Street  
Adelaide, South Australia 5000, Australia  
ABN: 84 151 743 976