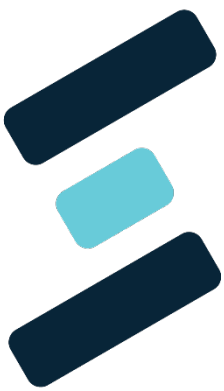
snare
A PROPHECY SOLUTION

HOW AGENTS CLEAN UP THE MESS

Whitepaper



Why SYSADMINS ARE ADOPTING AGENTs for LOG COLLECTION

When many enterprise SIEM solutions seem to be a “one-stop shop”, it’s difficult to resist the initial appeal ofagentless deployments. Especially as agentless appears to be the way forward; seeming easier to deploy and manage. After all, the fewer installs, the better... right? Not so fast. When budget, scalability, scope, throughput, performance and security are a concern, as they should be, you need to think about agents. With the right tools agents are easier to manage, and when properly designed they don’t add any new software dependencies. Moreover, agents provide real-time data delivery of your logs, which is a critical success factor for SIEM deployments. Thus, when premium agents are built with sysadmins in mind, everybody wins.

SOLUTION MANAGEMENT

While deploying agentless log collection solutions may seem easier at first when you get down to the nuts and bolt this is far from the case. As once you get past installing the software, you must configure the solution and consider: How many endpoints are you pulling from? What are their individual and collective EPS rates? Why does a ‘chatty’ domain controller require an entire agentless collector server to itself? Have you configured the collector with the credentials of every machine it is pulling from? All of a sudden agentless deployment becomes far more tedious than an agent-based solution. Agents with centralized management, like Snare, can make the process of monitoring and managing agents ‘effortless’. Users can monitor the activity status of their agents, which enables them to know when there is an interruption in the logging, while also validating policy configurations on all endpoints. Thus, once installed agents are managed en masse via a management console that turns your agents into a single cohesive solution, rather than requiring individual configuration.

STACK DEPENDENCIES

Agents can be built to be platform agnostic and not require a specific framework or operating system, such as IIS, Java or .NET - this negates concerns around additional software dependencies and saves significant time during deployment. Snare does this to not only make deployment more manageable, but also to tie together log collection across disparate systems seamlessly. Furthermore, Snare agents are compatible with any SIEM, which is why Snare is the go-to for companies with mixed topographies, complex network settings and those migrating SIEMs. It is Snare's flexibility that allows our clients to scale efficiently and prevents introducing new vulnerabilities through additional software.

NEW SOFTWARE VULNERABILITIES

When faced with putting agents on each machine on a network or using agentless collectors it may appear, at face value, that agentless is the more secure approach. However, this is far from the truth. Agentless collectors require the login credentials of every machine they access, providing a honeypot for malicious actors to penetrate the network. It is far easier for malicious actors to attack an agentless collector, as successfully accessing one endpoint can allow them to inundate the collector server exposing every system it collects from and making it difficult to analyse the activity forensically. Conversely, purpose built security agents, mitigate these vulnerabilities.

RESOURCE USAGE

As your collection efforts increase, your hardware and bandwidth requirements need not grow exponentially. In the past, agents were considered 'resource heavy' monsters; bogging down machines with large footprints and clogging networks. However, today's lightweight agents consume almost no CPU. Snare agents add a full complement of noise

reduction capabilities, from verbose truncation to multi-level log filtering. Which, translated, means that sophisticated output-based filtering is applied to reduce the log.

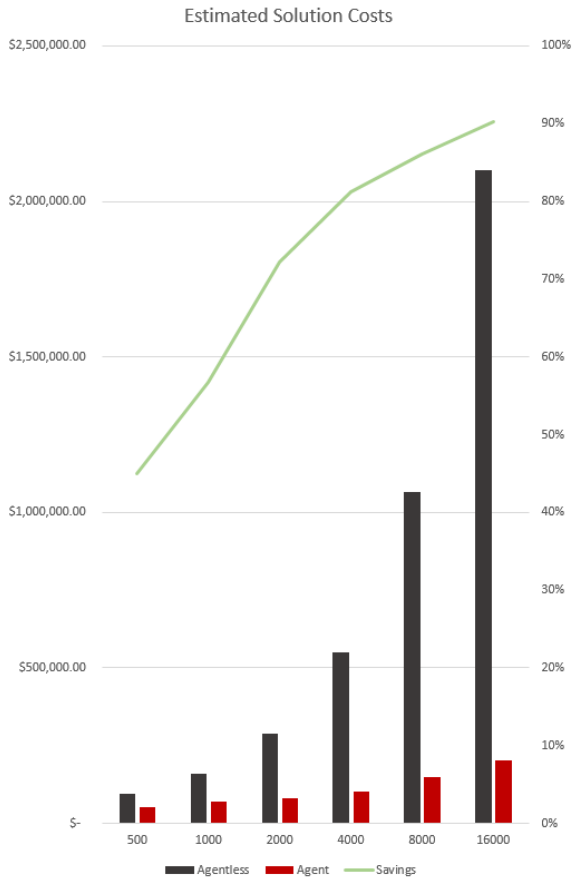
THE AGENT ADVANTAGE

Many institutions are aware of the shortcomings of agentless solutions. When faced with the very real threat of digital malfeasance the lag time of agentless logging is unacceptable. As it can take anywhere between five to thirty minutes, or beyond, for logs to send. Which is enough time for malicious actors to penetrate a network and wreak havoc, without your knowledge. When security is at a premium, companies everywhere should be cautious of agentless solutions.

While many SIEM solutions offer agentless collectors; it is wise to seek out agents as many of our clients do. Be it because of cost, reliability or resource management. There are many reasons why users deploy agents, yet the common denominator for doing so is that they understand the need for collection and analysis to happen in real time. Snare, unlike most agents, is not an afterthought companion to a larger SIEM solution but purpose built to assist every SIEM solution, regardless of vendor.

SNARE ENTERPRISE AGENTS

Snare is a highly scalable suite of security products utilizing output-driven noise reduction technologies to find, filter and forward event log data. Snare log sources include Windows, flat files, databases, Linux, Mac and Solaris with coverage for desktops and servers. Snare removes multiple levels of noise via managing audit policies, filtering and truncation. Snare's reflector technologies enables destination directives to ensure only relevant data ends up in the relevant location. Snare's noise reduction technologies can significantly reduce MTTD, ensure faster and more accurate analysis,



Pricing is is a critical component of scalable solutions. As demonstrated by the graph on the left, the larger the deployment the steeper the savings in agent-based solutions.

ADDITIONAL RESOURCES

To learn how Snare can help you optimize your SIEM solution, visit:

www.snaresolutions.com