NEFER

Sizin İçin SAVUNMA A.Ş.

nefersavunma.com.tr

SureLog

HOT STORAGE

High-Performance Searching & Investigating with SureLog Long Term Hot Storage Capability

To improve operational efficiency and increase system security, tremendous volumes of data are being collected and analyzed.

Data holds huge value for organizations, especially for security and operations teams, but with volumes increasing exponentially, storing it remains a challenge.

The value of your data deteriorates fast when you can't easily access it. Restoring data from a frozen state can be painful, especially when you don't know the exact timeframe you need to look at.

Ensuring you have the right storage for your SIEM environment is a simple but fundamental task.

When it becomes necessary to carry out forensic analysis, SIEM tools must be able to track back through past events. As long as admins identify the breach quickly enough, they may have enough information with access to original data held across the various devices.

Cold and hot data hold different types of information. They're categorized as hot and cold by how often a company accesses them. The more one is accessed, the hotter it is. The less, the colder.

Additionally, your organization also likely needs to keep logs for a period of time for one or more compliance reasons. But as compliance alone clearly doesn't equal security, there's somewhat of a paradox of stashing logs to check the compliance box but not being able to put them to good operational use.

Ultimately, you're faced with the choice between expensive hot or warm storage costs, or using cheaper inaccessible cold or frozen logs.

SureLog hot storage capacity is up to 40 times better than the other SIEMs.

There is no additional HW or special HW. You can achieve it with any VM infrastructure.

With other SIEM and security analytics solutions, data is rarely ever kept in a hot state for a full year due to storage costs.

Even in cases where customers are willing to bear higher storage costs for fast access, handling storage costs are a big issue.

SureLog keeps logs in a hot state for a full year with affordable storage costs without additional HW.

SureLog Hot Storage Requirement for 365 days

EPS: 2500 (max)
Hot state: 365 days
Disk size: 3 TB

SureLog

SureLog takes a different approach to big data. Rather than indexing data at ingest, which can make a system slow and slower as the index grows larger and harder to maintain, SureLog relies on indexing compression after data is stored.

This reduces disk resources required for indexing by up to **40 times.**