Threat Detection for NetApp: AI-Powered Cloud Data Security

By Yaron Knochen

Announcing AI-Powered Threat Detection for NetApp

Since file scanning is inline, a file will not be released to the user until the scan is completed. That is, configuring the agent policies for Threat Detection for NetApp is essential to ensure seamless integration with NetApp volumes.

NetApp uses a dedicated OS for their files, so traditional endpoint agents are incompatible. This is why storage vendors provide a dedicated solution for their customers.

Generally, poor scanning performance negatively impacts user experience when accessing the file. Frequent signature updates are an administrative nightmare. They rely upon AV signatures which are easily evaded. Reliance on signatures renders organizations vulnerable. Therefore, our solution must deliver the best protection available.

Legacies solutions often require a separate security management console, further increasing administrative overhead.

Frequent signature updates are an administrative nightmare. They rely upon AV signatures which are easily evaded. Reliance on signatures renders organizations vulnerable. Therefore, our solution must deliver the best protection available.

They rely upon AV signatures which are easily evaded. Reliance on signatures renders organizations vulnerable. Therefore, our solution must deliver the best protection available.

SentinelOne is pleased to announce general availability (GA) of Threat Detection for NetApp. Part of the new Singularity™ Cloud Data Security product line, SentinelOne customers can now seamlessly manage cloud data security alongside user endpoints.