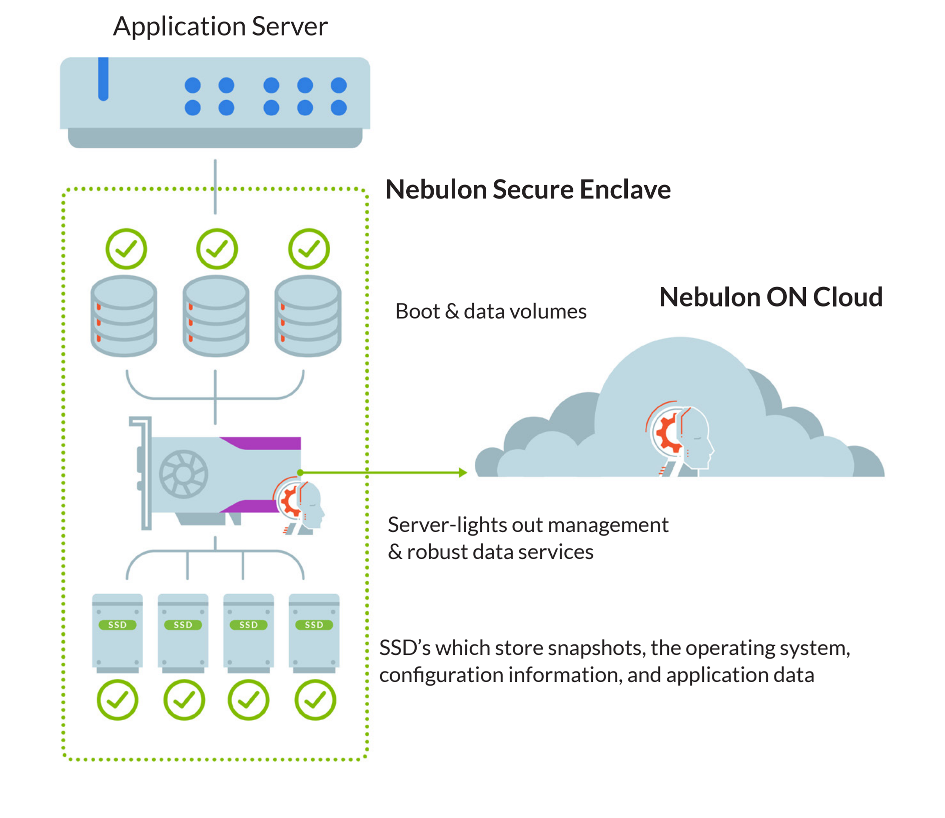
Rapid Ransomware Detection with Nebulon TripLine

The first combined server and storage threat detection for cryptographic ransomware, Nebulon TripLine is your last line of defense to **detect and respond within minutes** to suspicious I/O workload patterns.

What is Nebulon TripLine?

Nebulon TripLine is a new service that can identify potential crypto ransomware attacks on application data as well as the operating system and application software, and is enabled by two key elements of the Nebulon architecture. The first element, Nebulon Secure Enclave, is an isolated infrastructure domain encompassing server lights-out management, data services, boot and data volumes, and attached SSDs. Secure Enclave is a core architectural feature of smartInfrastructure, built-in from the ground up, and cannot be bolted-on to existing system architectures. The second important enabler of TripLine is, of course, Nebulon ON, an isolated administrative domain in the cloud where patterns of possible cryptographic ransomware are identified.

TripLine uses machine learning (ML) running in the Secure Enclave to identify encrypted versus unencrypted blocks in real-time. Every 30 seconds, these results are sent to the Nebulon ON cloud which uses a combination of ML and statistical models to compare that data to the historical average of encrypted blocks for a given volume. A spike in encrypted blocks will generate an alert within a few minutes of the first suspicious result.


Application Server
Nebulon Secure Enclave
Boot & data volumes
Nebulon ON Cloud
Server-lights out management
& robust data services
SSD
SSD
SSD
SSD
SSD's which store snapshots, the operating system, configuration information, and application data

Why Nebulon TripLine?

Hyperconverged infrastructure (HCI) relies on software running on servers to safeguard data. In some cases, HCI's software-defined storage (SDS) is integrated into the hypervisor, while in other cases, it runs as separate software on the server. In either scenario, a sophisticated ransomware attack on the hypervisor layer can encrypt the physical drives that HCI requires to operate, leading to data loss—including all snapshots. This creates a challenge for HCI and other server-based solutions to detect and recover from ransomware.

There are also ransomware detection capabilities available from several backup vendors. While helpful, these are limited to data volumes only, so they miss the operating system and application software attack surfaces entirely. These solutions also are not real-time. Once ransomware is inside your firewall, the goal is to detect and isolate it before it encrypts too much data. The earlier you detect signs of any type of cyberattack, the better your odds are of preventing damage and limiting the blast radius. This rule is especially true for cryptographic ransomware, given the consequences of this type of attack is often severe and irreversible. By the time backup software reports an attack, the spread may already be pervasive.

Because Nebulon maintains the boot and data volumes as a part of the Secure Enclave, TripLine can detect cryptographic ransomware in the operating system, application software, and application data in real time, as data is being written. Equally important, when it is time to recover, having a snapshot of the boot image, configuration settings, application binaries, AND data—all protected within the secure enclave—means recovery can be achieved in minutes.

Learn more about the Nebulon smartDefense portfolio at www.nebulon/solutions

Protect

with ImmutableBoot that maintains a known, good version of the OS

Detect

with TripLine that rapidly detects patterns of a cryptographic ransomware attack

Recover

with TimeJump that enables 4-minute recovery of the entire physical infrastructure