DATA SHEET

CryptoSpike

Ransomware Protection for NetApp

Detection, Prevention and Recovery for NetApp File Environments

The Ransomware Challenge

- File shares are among the most likely areas to be attacked via ransomware
- CryptoSpike uses a multi-pronged technology approach to combat ransomware
- Infected users are blocked from further access to NetApp file shares, helping to halt the spread of ransomware
- Infected files are identified and can be recovered using NetApp snapshots, without having to over-write entire folders or volumes
- Learner module detects suspicious behavior
- Uses both black-list and white-list approaches
- Simple, affordable licensing based on NetApp storage controller (no file or data size limits)

You don't need us to tell you that ransomware is a major concern. Millions of attacks take place every year causing billions of dollars in damage. Odds are very high that your organization has already been hit, though you might not know it yet. If you want lots of scary statistics, you can find plenty of them here.

Most ransomware attacks happen when files get compromised, so your file shares are among the most vulnerable parts of your organization. File shares are where end users meet the data center most directly, and most ransomware comes through the front door via interaction with end users. It's as simple as someone in your organization getting an email, they click on it, and bang! Your file shares are infected.

CryptoSpike was designed to work with NetApp ONTAP file systems, monitoring every action your users take to protect you from ransomware.

CATALOGIC SOFTWARE ProLion

How CrytpoSpike Works

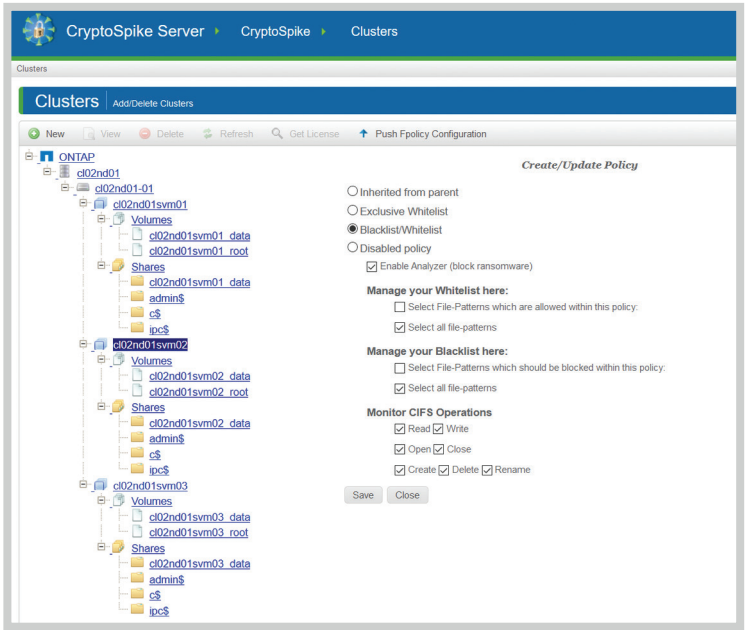
CryptoSpike uses a multi-pronged approach to detect ransomware.

It begins with a **Black List** that includes 1800+ known (as of this writing) ransomware file endings or names. Updates are made every day and downloaded to the CryptoSpike server.

The **White List** is a set of allowed file extensions, such as .doc or .pdf. If a new, unknown file ending is detected, it is blocked. The initial white list is generated via a scan of your current files.

The most important component is the **Learner** module. The Learner tracks user behavior and determines allowable file transactions (e.g. read, write, open, etc.). If any anomalous behavior is detected, the user is blocked. For example, if User A suddenly writes to dozens of files in a few seconds, this behavior is recognized as outside of normal patterns, and the user's write access is blocked.

Different strategies can be applied at different levels in the file hierarchy. One policy can be applied across the NetApp cluster, or different policies can be applied at the level of Storage Virtual Machine or even file share. For instance, you may white list different file types for a developer share than for a marketing share.



CryptoSpike lets you easily configure policies at different levels in your NetApp file environment. A single policy can be applied to all systems, or custom policies can be applied to Storage Virtual Machines, volumes, folders and so on.

Data Access Transparency

Another aspect of overall data security is data access transparency: understanding which users accessed what data, plus when and how often. Because CryptoSpike is monitoring all user file access, it is ideally suited to track and deliver this information.

With CryptoSpike, you can easily examine user behavior down to the level of files and folders. Reports will show you user activity in terms of file opens, closes, writes and so on. This will provide you with definitive information that a volume, folder, file, etc. was accessed by a given user.

Alarms and Real-Time Blocking

CryptoSpike works together with the NetApp FPolicy server, which is required. The FPolicy server will enforce the blocking decisions made by CryptoSpike.

For example, if ransomware is detected by the Learner module, the relevant user will be changed to having read-only access, which stops them from further spreading the ransomware. CryptoSpike lets you know which files have been affected, allowing you to do targeted recoveries, rather than having to roll-back an entire folder or more.

IT security can then be alerted about the infected user and suitable steps taken to disinfect their system. Meanwhile, CryptoSpike provides a list of infected files, allowing you to perform targeted recovery from NetApp snapshots.

How to Purchase CryptoSpike

CryptoSpike is licensed per NetApp controller, with pricing tiered according to the NetApp model number. There are no capacity limitations in terms of total storage or number of files, making CryptoSpike licensing very easy to manage.

50 Tice Boulevard, Suite 110
Woodcliff Lake, NJ 07677 U.S.A.
201.249.8980
catalogicsoftware.com

United Kingdom: +44 (0) 207 712 1667
Germany: +49 (0) 2102 307614 0
Netherlands: + 31 (0) 20 347 23 88