Ransomware protection measures

FlexPod

NetApp
June 04, 2021

Table of Contents

Ransomware protection measures

This section discusses the key features of NetApp ONTAP data management software and the tools for Cisco UCS and Cisco Nexus that you can use to effectively protect and recover from ransomware attacks.

Storage: NetApp ONTAP

ONTAP software provides many features useful for data protection, most of which are free of charge to customers who have an ONTAP system. You can use the following features at all times to safeguard data from attacks:

- **NetApp Snapshot technology.** A Snapshot copy is a read-only image of a volume that captures the state of a file system at a point in time. These copies help protect data with no effect on system performance and, at the same time, do not occupy a lot of storage space. NetApp recommends that you create a schedule for the creation of Snapshot copies. You should also maintain a long retention time because some malware can go dormant and then reactivate weeks or months after an infection. In the event of an attack, the volume can be rolled back using a Snapshot copy that was taken before the infection.
- **NetApp SnapRestore technology.** SnapRestore data recovery software is extremely useful to recover from data corruption or to revert only the file contents. SnapRestore does not revert the attributes of a volume; it is much faster than what an administrator can achieve by copying files from the Snapshot copy to the active file system. The speed at which data can be recovered is helpful when many files must be recovered as quickly as possible. In the event of an attack, this highly efficient recovery process helps to get business back online quickly.
- **NetApp SnapCenter technology.** SnapCenter software uses NetApp storage-based backup and replication functions to provide application- consistent data protection. This software integrates with enterprise applications and provides application- specific and database- specific workflows to meet the needs of application, database, and virtual infrastructure administrators. SnapCenter provides an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, and file systems. Its ability to provide application- consistent data protection is critical during data recovery because it makes it easy to restore applications to a consistent state more quickly.
- **NetApp SnapLock technology.** SnapLock provides a special purpose volume in which files can be stored and committed to a nonerasable, nonrewritable state. The user's production data residing in a FlexVol volume can be mirrored or vaulted to a SnapLock volume through NetApp SnapMirror or SnapVault technology, respectively. The files in the SnapLock volume, the volume itself, and its hosting aggregate cannot be deleted until the end of the retention period.
- **NetApp FPolicy technology.** Use FPolicy software to prevent attacks by disallowing operations on files with specific extensions. An FPolicy event can be triggered for specific file operations. The event is tied to a policy, which calls out the engine it needs to use. You might configure a policy with a set of file extensions that could potentially contain ransomware. When a file with a disallowed extension tries to perform an unauthorized operation, FPolicy prevents that operation from executing.

Network: Cisco Nexus

Cisco NX OS software supports the NetFlow feature that enables enhanced detection of network anomalies and security. NetFlow captures the metadata of every conversation on the network, the parties involved in the communication, the protocol being used, and the duration of the transaction. After the information is aggregated and analyzed, it can provide insight into normal behavior.

The collected data also allows identification of questionable patterns of activity, such as malware spreading across the network, which might otherwise go unnoticed.

NetFlow uses flows to provide statistics for network monitoring. A flow is a unidirectional stream of packets that arrives on a source interface (or VLAN) and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow. You can export the data that NetFlow gathers for your flows by using a flow exporter to a remote NetFlow collector, such as Cisco Stealthwatch. Stealthwatch uses this information for continuous monitoring of the network and provides real-time threat detection and incident response forensics if a ransomware outbreak occurs.

Compute: Cisco UCS

Cisco UCS is the compute endpoint in a FlexPod architecture. You can use several Cisco products that can help to secure this layer of the stack at the operating system level.

You can implement the following key products in the compute or application layer:

- **Cisco Advanced Malware Protection (AMP) for Endpoints.** Supported on Microsoft Windows and Linux operating systems, this solution integrates prevention, detection, and response capabilities. This security software prevents breaches, blocks malware at the point of entry, and continuously monitors and analyzes file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defenses.

  The Malicious Activity Protection (MAP) component of AMP continually monitors all endpoint activity and provides run-time detection and blocking of abnormal behavior of a running program on the endpoint. For example, when endpoint behavior indicates ransomware, the offending processes are terminated, preventing endpoint encryption and stopping the attack.

- **Cisco Advanced Malware Protection for Email Security.** Emails have become the prime vehicle to spread malware and to carry out cyber-attacks. On average, approximately 100 billion emails are exchanged in a single day, which provides attackers with an excellent penetration vector into user's systems. Therefore, it is absolutely essential to defend against this line of attack.

  AMP analyzes emails for threats such as zero-day exploits and stealthy malware hidden in malicious attachments. It also uses industry-leading URL intelligence to combat malicious links. It gives users advanced protection against spear phishing, ransomware, and other sophisticated attacks.

- **Next-Generation Intrusion Prevention System (NGIPS).** Cisco Firepower NGIPS can be deployed as a physical appliance in the datacenter or as a virtual appliance on VMware (NGIPSv for VMware). This highly effective intrusion prevention system provides reliable performance and a low total cost of ownership. Threat protection can be expanded with optional subscription licenses to provide AMP, application visibility and control, and URL filtering capabilities. Virtualized NGIPS inspects traffic between virtual machines (VMs) and make it easier to deploy and manage NGIPS solutions at sites with limited resources, increasing protection for both physical and virtual assets.