NetApp

Unfear ransomware without taking your hybrid cloud offline

Preparation is the enemy of fear

Ransomware attacks are part of the connected reality. But you don't have to go dark to protect your data. Stay connected and integrate ransomware protection, detection, and recovery capabilities with powerful products, solutions, and services from NetApp.

Big problems require big protection

By 2025, at least **75% of IT organizations** will face one or more ransomware attacks[1]

74% of threats detected are zero-day malware[2]

Challenge

- Ransomware attacks are evolving, and some are specifically targeting backup data and administrator functions.
- If the constant barrage of phishing doesn't produce an opening, bad actors find another way, such as exploiting zero-day vulnerabilities.
- Safeguarding what feels like endless endpoints and sprawling applications can be daunting.

Opportunity

- Ransomware is a big, multi-layered problem that requires a multi-layered security solution. But under the surface, the attacker wants your data.
- You need protection at every access point, with a tamperproof way to protect the data and to recover in case it is compromised—this is where NetApp excels.

Why NetApp?

NetApp features—such as read only Snapshot copies, indelible SnapLock file locking, efficient and secure SnapMirror data replication, and malicious file screening with FPolicy—create highly effective preventative measures to keep your data safe during an attack.

Detective skills built into your data storage

Challenge

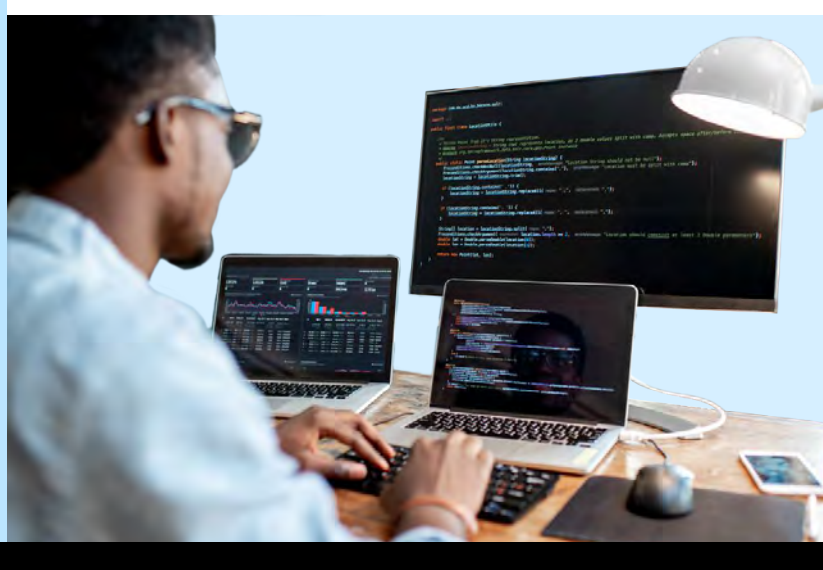
- After a hacker infects a client machine with malware, ransomware encrypts the contents of files so that they are inaccessible without the encryption key.
- Endpoint sprawl makes companies more susceptible and detection more difficult.
- The longer it takes you to detect the infection, the further the encryption can spread.

Opportunity

- If you can detect when a ransomware event begins to occur, then you can prevent it from spreading.

More endpoints and a diffuse network means, on average, **companies take 197 days** to identify a breach[3]

47% of individuals fall for phishing scams while working from home[4]



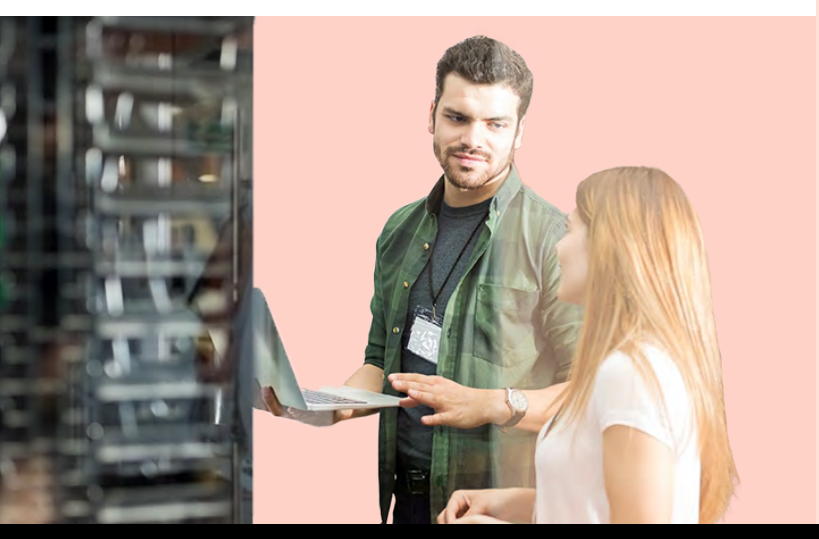
Why NetApp?

With NetApp ONTAP data management software, you have detection capabilities built in. Onbox workload and data entropy monitoring, along with alerts about unexpected changes in Snapshot reserve size or storage efficiency, can all help detect a possible ransomware attack. With Cloud Insights' ability to detect user behavior anomalies, combined with ONTAP intelligence, you can identify bad actors and abnormal storage behavior. Active IQ will help identify the best practices in your environment to ensure the best possible outcome.

Don't pay the ransom, recover your data in minutes

$350 million in ransoms were paid in the last year[5]

The average downtime due to ransomware is **more than 16 days**[6]



Challenge

- During a typical ransomware attack, the primary data is encrypted.
- Most backups are immutable and can't be changed.
- Bad actors will hack into accounts and delete backups before encrypting the primary data so that the organization can't restore from a backup.

Opportunity

- Reliable copies of data are needed to effectively recover from an attack.

Why NetApp?

With NetApp, companies can restore petabytes of data in minutes, avoiding downtime and costly ransom payments. At the same time, ONTAP SnapLock prevents Snapshot copies from being deleted, so you always have an untouched backup to restore from.

Data protection is part of ransomware protection

Learn more about NetApp ransomware solutions →

[1] Gartner, "How Modern Backup Applications Can Protect You From Ransomware" https://www.gartner.com/doc/reprints?id=1-25RBI8JH&ct=210407&st=sb
[2] Help Net Security, "Zero day malware reached an all-time high of 74% in Q1 2021." https://www.helpnetsecurity.com/2021/06/29/zero-day-malware-q1-2021/
[3] IBM, "Cost of a Data Breach Report 2020." https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] Deloitte, "The case for increased cybersecurity." https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
[5] IMC Grupo, "FBI Reports 300% Increase in Reported Cybercrimes." https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/
[6] Coveware, "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate." https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate