NetApp

3 questions you should be asking about ransomware protection

No two ransomware attacks look the same. Sometimes attacks start at the perimeter, and sometimes… the call comes from inside the house. With attacks happening every 11 seconds, there's never been a better time to start asking tough questions about the defenses you have in place.

Can I easily block common malware attacks to prevent downtime?

Imagine this scenario: An unsuspecting user clicks a malicious email link, which then launches malware. It starts encrypting file shares and changing file extensions. Suddenly, you can't access your files. Help desk tickets start to pile up… and downtime is costing you $8,662 per minute.

If you use Pure Storage, your best bet is restoration from local snapshots, but that will take time—hours if the problem is extensive. But with NetApp® ONTAP® software, the native FPolicy feature blocks more than 3,000 known ransomware extensions, so you can prevent common attacks to better mitigate the threat and minimize downtime.

Can I detect suspicious encryption before ransomware wreaks havoc?

Using more advanced techniques, hackers can encrypt data without changing file extensions. With the average organization taking 237 days to recover from an attack, downtime costs quickly spiral out of control.

On Pure, there's not much you can do to detect the attack. Instead, you'll rely on data recovery after the attack has occurred. This approach can result in days of downtime. But with NetApp technology, you can identify threats early through sophisticated storage and user behavior anomaly detection and automated response, such as blocking storage access by compromised user accounts. As a result, the majority of users remain unaffected, any damage is minimized, and data is easily restored.

Can I stop an attacker from destroying data?

Angry attackers will typically try to prevent you from restoring data by deleting your backup copies. By hacking an administrator's account credentials, they can destroy volumes and databases, which will knock file shares and applications offline. That might cost you up to 50 times more than the initial ransom.

With Pure, you can recover your data from SafeMode snapshots, but there's a potential back door with social engineering. If Pure support can be convinced to delete SafeMode data, then a convincing hacker could impersonate an administrator and force the issue. Deleting your backup data, even SafeMode data, means that recovery is seriously at risk. But with NetApp solutions, multi-admin verification prevents a single administrator from destroying data. And NetApp SnapLock® Compliance, supported by ONTAP, can lock data securely, without any back doors, to prevent backup data from being deleted in the first place.

Ransomware-proof my IT

NetApp