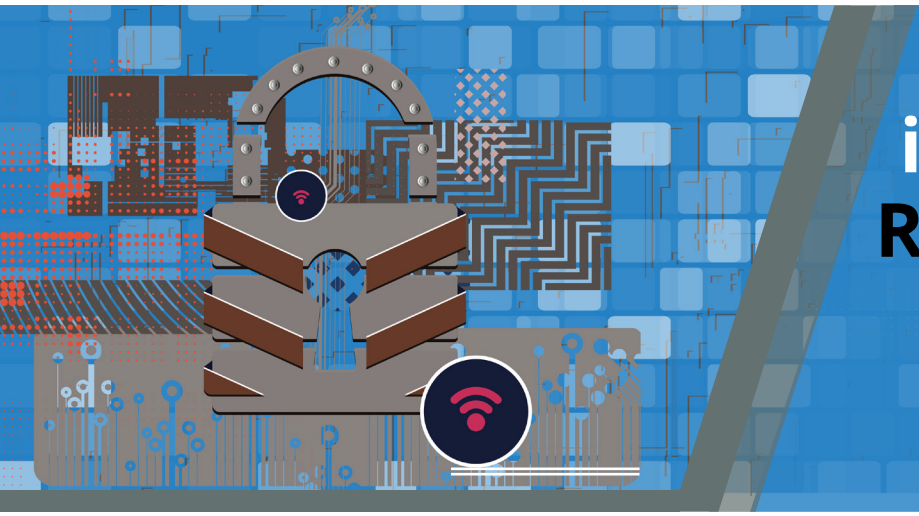

iTBlueprint Fills In Ransomware Gaps

with NetApp Solutions

NetApp
Gold Partner

Problem:

With a rise in ransomware during the pandemic, we have also seen a rise in organizations that have fallen victim to these attacks. While a large majority of these attacks came via email, through phishing or spoofing internal profiles, other attacks have come through security vulnerabilities in products. In the worst cases, local backups proved to be inadequate and/or were compromised.

In one example, a phishing scheme gave hackers administrative access to the network where they were subsequently able to encrypt systems, including the backup server which resulted in deletion of the data residing in the tape library.

In another example, an organization fell victim through a remote access solution's vulnerability. Unfortunately, the customer didn't have all security patches in place, allowing bad actors to encrypt their virtual operating systems. The backup solution, which was also compromised, didn't capture all their data.

Both of these organizations reached out to iTBlueprint to assist in recovery of their systems and data as well as help them fill in security gaps so this wouldn't happen again.

Solution:

The key solution for ransomware remediation is restoring uninfected data. For each organization, NetApp storage was the last remaining fall-back and was recovered using NetApp Snapshots.

It was a close call for one customer, when iTBlueprint Managed Services noticed just 3 months earlier that Snapshots had been turned off and re-engaged the solution to protect file data and subsequently protect the company from total loss.

In addition to Snapshots, the iTBlueprint team recommended further remediation measures, including implementing NetApp FPolicy and SnapLock solutions. FPolicy provides a file blocking methodology that allows organizations to filter or block traffic based on file extensions and file metadata. SnapLock ensures that snapshot copies can't be changed, renamed, or deleted until they are aged out based on the administrators configured policy.

Results:

You never know if you're going to get reinfected. With NetApp solutions like Snapshots, FPolicy and SnapLock, these organizations were able to effectively add another layer of immunity against a variety of threats, including ransomware.

Both customers are back to business as usual, thanks to having more systems in place as well as taking advantage of technologies that they already own to protect themselves. iTBlueprint has helped them to find out how the attacks came in and effectively disinfected all the systems that were infected so they're stronger, should another attempt be made to cripple or ransom their business.

170 – 422 Richards St. Vancouver, BC V6B 2Z4
30 N Gould St., Ste 6107, Sheridan, Wyoming, 82801
1-833-948-2583 - info@itblueprint.ca