Technology Did It Leverages Keepit to Help US Government Supplier Recover from Ransomware

As a valued Keepit partner, Technology Did It recommended Keepit's backup and recovery solution to a US government supplier. After being hit by ransomware, the US government supplier utilized the Keepit solution to recover from the event. Even in the face of the attack, the Keepit solution ensured that the customer's data remained impenetrable to the ransomware.

Microsoft backup not sufficient

Familiar with the Microsoft shared responsibility model, the US government supplier knew that their versioning and recycling bins were not fully protected. When Technology Did It recommended Keepit as a third-party cloud backup solution, the US government supplier instituted Keepit as an end-user protection tool.

Even though Microsoft data lives in the cloud, you shouldn't rely on Microsoft for backup, as they do not offer sufficient protection.

Tiffany Carra
Owner of Technology Did It

After being hit by Conti ransomware, we were able to restore the data with Keepit, and we were back up and running in 30 minutes.

Tiffany Carra
Owner
Technology Did It

Conti ransomware strikes without success

The US government supplier was hit by Conti ransomware 3 months after their onboarding with Keepit. Conti ransomware encrypts everything it touches, exfiltrating data to another source. The attacker will usually try to extort money from the company, threatening to release the data if a sum of money is not paid. Due to Keepit's secure backup solution, the attacker was unable to get to the data. All data protected by Keepit is stored and protected by a hash-chain object store that prohibits the deletion or manipulation of any data object or backup set. This data protection method means that the data cannot be altered or deleted.

Back to work Monday morning

Following the Conti ransomware attack, the US government supplier decided to restore the data from Keepit back to Sharepoint. They were able to restore all data within 30 minutes. In fact, the attack took place on a Friday, and the company continued business as usual the following Monday. For companies who do not have proper backup in place, a ransomware attack can lead to days, weeks, and even months of downtime, leading to astronomical costs to the business. IT consultancy Technology Did It explains that Keepit allowed the US government supplier to restore their data quickly and easily so that the business could keep running as usual.

The US government supplier was hit by Conti ransomware on a Friday. The entire organization was back up and running on Monday morning.

Tiffany Carra

Technology Did It encourages other companies to use third-party backup

In light of this attack, Technology Did It urges other companies not to rely on Microsoft to back up their data. Even though Microsoft's data lives in the cloud and there are versions and recycling bins that may make you feel secure, they do not deliver a comprehensive backup solution, meaning you could lose access to data in the event of a ransomware attack.

Following this success story, Technology Did It recommends Keepit to other companies who are looking for a secure, reliable and simple backup solution.

Keepit is a no brainer. It's secure, cost-effective and easy to maintain.

Tiffany Carra

About Technology Did It
Technology Did It is a managed services provider focused on providing outstanding IT support for small businesses that otherwise would be unable to navigate the muddled IT waters in the twenty-first century. With close to 40 years combined IT experience, our goal is to provide your small business with the technology solutions it needs to be both agile and cost-effective in your everyday work environment.

Get in touch with Keepit
Reach out for our partner account managers to learn more about our Partner Program.
+45 8987 4757
partner@keepit.com