How to Recover from Ransomware using CrashPlan

CrashPlan

TECH OVERVIEW

At best, ransomware attacks are disasterous to productivity, tie up valuable resources and threaten your business's bottom line. At worst, they can spell the end of a business. But with CrashPlan, restoring your data to a version prior to the attack can be completed in a few simple steps.

Situation

When ransomware strikes, business productivity and output suffer. Business leaders estimate that their response time to a ransomware attack ranges from several hours to several days per device. Without reliable backup copies, there is no certainty of data recovery–despite an organization's best efforts. Even paying the ransom is no gurantee of decryption. Furthermore, the FBI specifically recommends against paying ransoms, and has provided specific reporting guidelines for organizations that pay to recover their data.

Analysts and industry experts recommend frequent backups to mitigate risk of data loss and eliminate the need for ransom payments; but not all backups are created equal. To be useful in a time of crisis, backups must happen automatically, continuously and offer versioning that supports reliable file restore.

Solution

After a ransomware event, IT admins can initiate a full device restore to a new or re-imaged device by following these steps:

01 **Identify the time of the infection.** If the time is unknown, take precautions to prevent the spread of a possible re-infection. Next, restore several versions of an individual file to determine the correct timeframe or analyze file timestamps to identify the timeframe of recent file modifications.

02 **Select the root folder** from which you would like to restore.

03 **Select the date and time f**rom which you would like to restore prior to the ransomware infection.

04 **Initiate the restore.** If specific files are needed to resume work immediately, select and download these files first before initiating a full device restore. By default, files will be restored to original folder structures and locations.

05 **Tell users they can get back to work** while files download in the background.

06 **After restoring files** to a new or re-imaged device, you can save time, storage and bandwidth by using CrashPlan's built-in workflow to pick up the backup archive where the old device left off.

Customer Spotlight

A financial technology company of more than 5,000 employees uses CrashPlan to protect the critical end-user data on its laptops and desktops.

TEAM

- IT support specialist
- 6 VP-level executives

CUSTOMER PRE-CONDITION

Prior to CrashPlan, the company relied on Syncplicity and SOS Online Backup for data protection. When six of its executives were hit with ransomware, Syncplicity synced the infection to its saved files as well. SOS Online Backup also proved unreliable—it had not successfully completed a backup for six months. The end result: complete data loss.

CUSTOMER POST-CONDITION

"After deploying CrashPlan, two of the same executives were hit again with ransomware. What might have been a repeat nightmare proved no issue thanks to automatic backups and extensive versioning."

The IT support specialist was able to restore all data and garner the ultimate praise from an executive who said, "'Thank God for this software and good job bringing it in.'"

CONCLUSION

This data recovery story is one of many as the threat of ransomware and the cost of recovery continue to grow. In 2021, the median cost of a ransomware attack was $11,150. CrashPlan offers a full year of end-user data protection for a fraction of the cost of a single ransom payment. With CrashPlan, IT teams can view, analyze and restore employee files and remediate and recover from any data incident. When ransomware inevitably hits, you'll restore devices in less time, with less effort—all without paying the ransom.

QUICK FACTS

- Financial technology company
- Prior to CrashPlan, the company experienced a ransomware attack on six executives
- Restoring from legacy backup proved non-viable
- Incident became a fire drill for the IT support specialist and resulted in full data loss
- After deploying CrashPlan, two of the same executives were once again hit with ransomware
- All end-user data was quickly recovered without paying the ransom

CrashPlan

Corporate Headquarters
100 Washington Avenue South
Minneapolis, MN 55401
612.333.4242

crashplan.com