Panzura Customers Don’t Pay Ransoms

In May 2019, it cost the City of Baltimore $18M to recover from a ransomware attack. And, they weren’t alone. Organizations of all sizes and industries are increasingly falling victim to infection by software that makes critical business files inaccessible by encrypting and locking them, until a ransom is paid for their return.

Every minute, organizations are repelling these attacks by intercepting and blocking emails, disallowing software downloads and updates and blocking web-based instant messages. But, it takes just one employee to be fooled into thinking a file or link is genuine, and your entire IT network can be taken hostage.

Panzura
695 Campbell Technology Parkway, Campbell, CA, USA

panzura.com
vizion.ai

It’s Not Just Carelessness or Inattention That Puts You at Risk

While many attacks rely on sheer volume, the potential financial gain means they can afford to be sophisticated and targeted.

For example, one morning, you receive an urgent email from your CEO asking you to explain the attached invoice in the form of a PDF file. You immediately open the PDF, which has an embedded Word document, and you bypass the file scan by saying it is “OK” to open. After all, it was from your CEO. **Except, it wasn’t.**

The embedded Word document you just opened has a Visual Basic macro which downloads ransomware to your laptop and executes it. In just a few moments, you’re looking at a message on your screen confirming the data on your laptop and your entire network drive is encrypted. The only way you’ve ever getting access to your data again is if you send funds using untraceable bitcoin in order to obtain the software keys that will decrypt it.

Worse, you have a deadline. The countdown to your data’s irreversible termination has officially begun and you either send the funds before the deadline or the keys to decrypt your data are gone forever.

On the face of it, the stark choices you’re facing are to attempt recovery, or pay the ransom. Many organizations opt to pay, and who can blame them? The ransom can be a relatively small amount in contrast with the cost of recovery.

In reality, neither of them is a good option. Recovery can be lengthy, expensive and incomplete. Rolling back using backups is generally less than 100% reliable, leaving you with missing data and, depending on the size and complexity of your network, can be a very lengthy process. While you’re working on recovery, you also need to be certain that you’ve solved your vulnerabilities, to avoid immediately being reinfected.

On the other hand, paying the ransom gives no guarantee of the return of your data or of its health from this point forward, and it's no protection against future attacks. And, paying attackers enables them to develop newer and more complicated variants that go undetected by antivirus solutions.

The Numbers Tell Us That Vigilance Is Not a Complete Defense

You can - and should - educate your people on how to avoid social engineering attacks, ignore unknown attachments, avoid questionable websites and be hyper-vigilant about protecting your network security. You should also back up diligently, keep anti-virus and threat software up to date and constantly monitor your network for threats as well as block suspect sites, and proactively scan network storage devices. But, it's not enough.

One user deceived by an authentic-looking email or one moment's inattention is all it takes. Your people and your systems simply can't be vigilant enough. Ransomware relentlessly targets employees and organizational infrastructure, and it's expected to infect businesses and governments every 11 seconds by 2021. The numbers are increasing, along with the value of the organization targeted.

According to Emsisoft, ransomware attacks in 2019 impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion. The impacted organizations included:
- 113 state and municipal governments and agencies.
- 764 healthcare providers.
- 89 universities, colleges and school districts, with operations at up to 1,233 individual schools potentially affected.

To Become Invulnerable, You Need Data Architecture That Is Immutable

While your defenses should be as robust as you can possibly make them, at the heart of every ransomware attack is the ability for your files to be modified, once they are accessed.

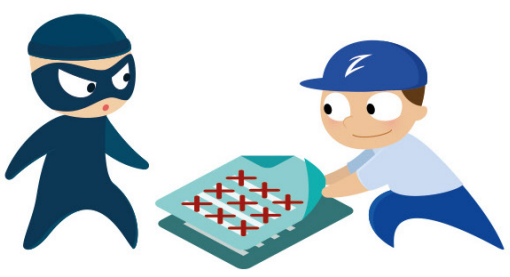
Your data storage solution needs to be built on the fundamental premise that your data is immutable. That the master copy of your data - once it's written, cannot be changed.

With Panzura, at no time does any file update alter the data that has been written to your object store. Blocks encrypted and stored in the cloud are never modified, and are thus immutable and not subjected to ransomware. Instead, when changes are made to a file, the Freedom filer will write those new or changed blocks to additional objects in the cloud. That doesn't mean you can never delete data; secure and complete erasure of files and data can be undertaken whenever necessary, while ensuring data cannot be accidentally deleted.

Synchronization events occur every 60 seconds on all Freedom filers, syncing both to the cloud and to every local filer in your network. This effectively provides a recovery point objective of 60 seconds for all your data.

Immutable Data Architecture Gives You Immunity From Ransomware

Using Panzura's hybrid cloud approach, if ransomware ever gets past your first line of defense and encrypts your data, your local Freedom filers write the resulting encrypted files to your cloud object store as new data.



Your pre-existing data is unaffected and is preserved as original objects in the object store, which means that all files encrypted by the ransomware code can be immediately reverted back to their previous state. This can be done for a single file, entire directories, or an entire global file system.

As a result, if and when you get a ransomware demand, you won't be paying a penny. Recovery is as quick and easy as reinstating the previous, unencrypted version of a file, directory, or file system.

How Can We Help?

Panzura is the fastest global cloud file system on the planet, helping organizations to be massively productive in the cloud, while keeping data completely secure and protected from all manner of cyber threats. With support for all major public and private clouds, and trusted by organizations with the most stringent security requirements in the world, Panzura offers exceptional value as a complete enterprise solution.

To find out how Panzura's global cloud file system can help your organization, visit **panzura.com**.