ENDURADATA

PROTECTING, DELIVERING AND LEVERAGING DATA

www.enduradata.com

USING EDPCLOUD CROSS-PLATFORM SOLUTIONS TO MITIGATE THE EFFECTS OF RANSOMWARE ATTACKS

Using multilevel approaches to augment resilience against ransomware attacks.

KEY BENEFITS

- Reduce risks of data loss
- Recover and resume operations quickly
- Reduce costs
- Reduce lost opportunities
- Reduce tarnished reputation
- Reduce lost revenue
- Get early warnings
- Increase resilience
- Improve efficiency
- Flexible control
- Full control of data.

Improve redundancy

Resume operations quickly

Protect reputation

Reduce risks & costs

Improve business resilience

Keep an eye on mission data

ENDURADATA

PROTECTING, DELIVERING AND LEVERAGING DATA

Use EDpCloud to protect data and harden operations.

1

ENABLE ARCHIVES

Before a file is updated, a read-only copy is made for recovery of previous versions of the files

2

CREATE UNLIMITED SNAPSHOTS

Create multiple snapshots to revert to in case of an attack. Each snapshot will be immutable

3

REPLICATE TO DIFFERENT OPERATING SYSTEMS

Reduce the risk of ransomware spread by leveraging replication to Linux, OpenBSD, Solaris, or other UNIX

4

ENABLE TRANSIENT CONTAINERS

Replicate to and from independent containers that will be orchestrated on demand

5

SERVER ISOLATION

Schedule server isolation to stop receiving file changes or to resume, creating cascaded snapshot protection

6

WATCH IMUTABLE FILES

Set up alerts on immutable files and invoke actions to pause, send or receive files, and invoke commands to take storage offline.

Use multiple strategies to increase ransomware tolerance and reduce risks.

RANSOMWARE ATTACKS

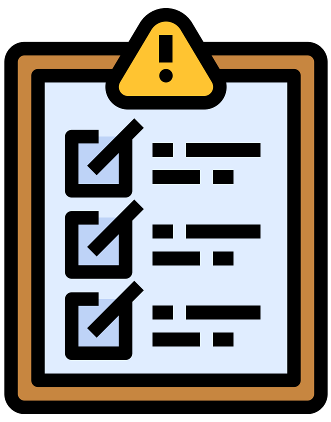
Not a single day goes by without hearing about ransomware attacks on businesses and government agencies. Ransomware encrypts and or leaks data and asks the victims to pay a ransom. Ransom notes range from tens of thousands to hundreds of millions of dollars. Even if the ransom is paid, you may not recover data. Ransomware impacts or stops all businesses, non-profits, and agencies' operations.

THE CHALLENGE

Ransomware attacks increased by more than 350% between 2019 and 2021. Businesses and government agencies cannot operate post a ransomware attack. Ransom notes are approaching $400,000,000 in the first part of 2021. Ransomware is a profitable business, with its own distribution channel and its value add resellers. When ransomware takes over corporate or government data, costs mount and lead to a halt in operations.

What happens after a ransomware attack?

- Sensitive data may be destroyed or maybe leaked, causing significant damage
- Halted operations lead to significant opportunity costs
- Increased liability
- Risks to lives in the case of emergency services or healthcare providers
- Risks of intellectual property increase
- Increased costs of recovery and cleanup
- Loss of digital assets
- Impact on reputation, customer trust, and future business
- Significant financial loss
- A significant disruption of lives
- High costs due to cleanup and restoring of services.

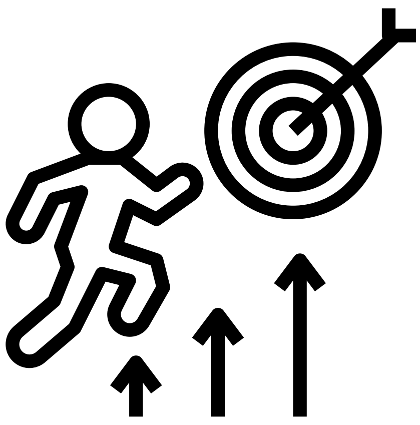


THE BIG CHALLENGE IS HOW TO CREATE AN EFFECTIVE DATA PROTECTION AND RAPID RECOVERY SYSTEM THAT ALLOWS OPERATIONS TO RESUME QUICKLY.

THE SOLUTION

Use EnduraData EDpCloud software to create multiple copies of data on one or more remote or local systems running different operating systems. The solution helps:

- Create multiple copies and snapshots of the data
- Copy data to different non-Windows-related operating systems (Linux, OpenBSD, Solaris, AIX, etc.)
- Create a rotating schedule of continuous data copy and replication with complete server isolation from the network to always keep a "last well-known good copy."
- Create rotating file change archives on rotating isolated servers
- Use post and pre-processing to watch for certain file extensions and file signatures and take action
- Use post and preprocessing to watch for excessive renames and isolate the servers before accepting any incoming data
- Set up policies for file inclusions and exclusions
- Integrate with additional scanning tools via post and pre-processing
- Use post and pre to take action based on types of operations
- Use immutable objects for alerts or automatic actions
- Replicate data to multiple systems (Different operating systems)
- Create multiple server isolation schedules (Yank the server automatically from the network, put it back, reject incoming data, put the server back on the network automatically, etc.)
- Use existing infrastructure or the cloud
- Increase resilience and operational Efficiency
- Use multiple copies to revert to the last non modified data
- Continuous data protection
- Point to the last well-known data(after cleanup) and use it without restoring.



For more info:
Call 1-952-746-4160
email: support@enduradata.com

Visit: **www.enduradata.com**