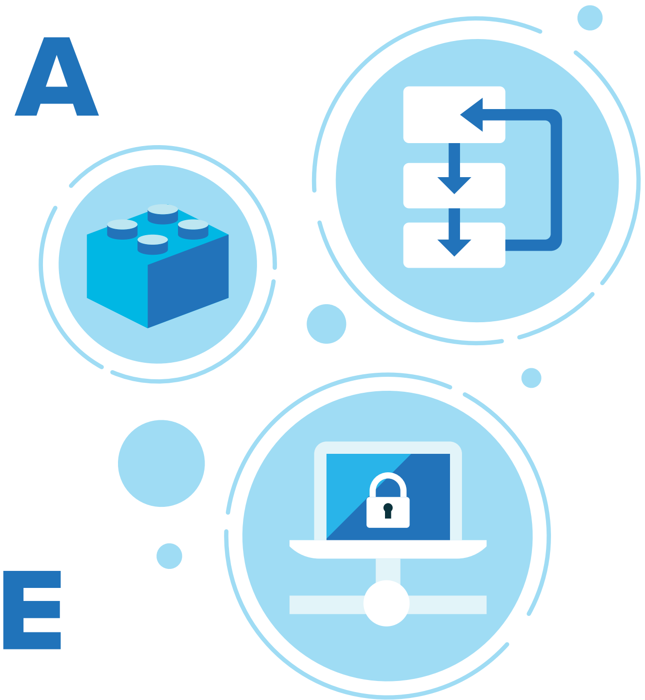
Quantum®

3 STEPS TO CREATING A PROACTIVE STRATEGY AGAINST RANSOMWARE



Attackers are now focusing on backup infrastructure as a primary target, so establishing security measures to protect it is a critical priority. A multi-layer security approach to ransomware protection and recovery is one of the most cost-effective methods to iron clad your data while keeping costs down.

Does your strategy include the protection and recovery of your backups? Your approach should be multi-layered. In 3 steps, we'll show you what a proactive strategy could potentially look like.

1 2 3

STEP 1:

CONDUCT A THOROUGH RISK ASSESSMENT OF YOUR ENVIRONMENT.

Identify any potential security issues and secure all entrances to your network. Approach this holistically across your environment. Any unguarded entry points are going to be a huge risk if left unaddressed.

One entry point is through **PHISHING EMAILS**—the number one vector in which criminals gain access. This means employees clicking through links in emails is all it takes for criminals to gain a foothold—so training becomes critical.

A second is through **REMOTE DESKTOP PROTOCOL (RDP)**, which is widely exploited for its known vulnerabilities. Reduce your attack footprint.

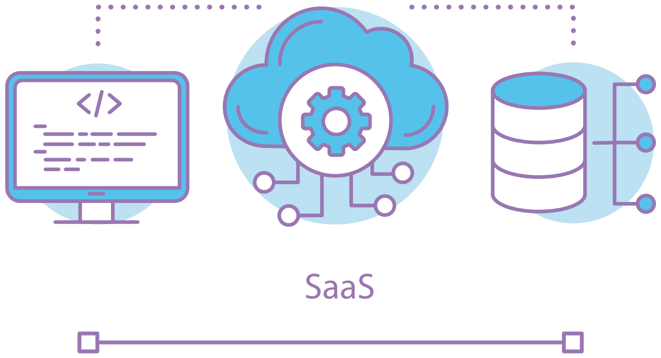
EMPLOYEE TRAINING

Educate on main methods used by criminals and security protocols.

STEP 2:

BACKUP INFRASTRUCTURE MUST BE UP TO DATE.

This means data should be backed up frequently to keep it out of the intruder's reach to ensure you can recover your data when needed.



Also, think about your storage platforms: Are they secure and updated? Is data spread over multiple clouds and compute environments? How are you protecting it?

Do you have a thorough understanding of how data gets in and out of your environment? Data should always remain protected and recoverable from all sources.

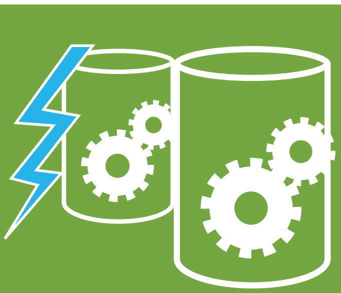
STEP 3:

DETERMINE WHETHER DISK, TAPE, OR CLOUD/OBJECT STORAGE WILL BE THE BEST RECOVERY METHOD FOR YOUR ORGANIZATION.

Regardless of the method you choose, just remember that ransomware protection and recovery must come in layers.

Organizations, such as the FBI, CISA, and NCSC, highly recommend an offline copy to air gap, and your recovery strategy should include some flash, disk, and object storage where tools like object lock are leveraged to provide the immutability your data requires.

It is a best practice to keep a copy of data in true offline media like tape in a multi-layer approach. Tape has an inherent nature to provide physical air-gap protection.



Faster-performing tiers, such as flash, SSD or HDDs, are a critical component to recover swiftly to have your data available when you need it.

Every organization has different needs, and your data will have different risk tolerance—assess this correctly and you can have a cost-effective multi-layer approach to data protection and ransomware recovery.

Quantum can help you protect, defend, and recover your data from any point in the data lifecycle.

Get started on a ransomware recovery plan for your organization today.
Chat with us at: **www.quantum.com/ransomware-recovery**

Quantum®