threadfin

PRE-Ransomware Checklist: Enable Rapid Recovery

How to use this checklist:

The actions outlined in this checklist are things your IT team should be doing today—proactively—before a ransomware attack occurs. Following these guidelines could minimize the damage from an attack and accelerate recovery.

This checklist can also serve as a tool for IT and Security teams to work together as they plan for prevention and, as outlined here, recovery.

Why use this checklist?

No system is perfect and no organization can be 100% successful in keeping motivated bad actors out. We know this firsthand. We're often called in to help organizations recover from ransomware attacks. The proactive actions included in this checklist are based on what would have made recovery faster and easier for the organizations we help.

What is and isn't included in this checklist?

This checklist, a do-it-yourself version of our PRE-Ransomware Rapid Recovery Implementation offering, includes 3 sections:

- Backup Architecture
  - Immediate, short & long term
- Protect Data
  - Immediate, short & long term
- Minimize Operational Impact

This checklist represents actions that make sense for most organizations—it's not an exhaustive in-depth analysis of your specific environment.

How to get additional support:

If you don't have the bandwidth or expertise to do-it-yourself or you'd like a customized approach, you can engage Threadfin's experts by calling 904-473-4840 or emailing info@threadfin.com.

Whether you handle it internally or go it alone, we again advise you to start today— proactively—before a ransomware attack occurs. Doing so will shorten the time, effort and cost of recovery, accelerating a return to business as usual when a breach occurs.

threadfin

PRE-Ransomware Checklist: Enable Rapid Recovery

Backup Architecture

Take action on these items before a ransomware attack occurs to better protect your data and enable rapid recovery if/when a breach occurs.

Immediate

- [ ] Upgrade your backup platform to enable the latest malware protection capabilities.
- [ ] Deploy/remediate backup platform monitoring/reporting server and configure for effective alert/report generation/delivery.
- [ ] Limit only the backup platform server access to the backup repository.
- [ ] Consider building and maintaining a cold-standby domain controller via regular air-gapped backups or synchronizations. The default value for the tombstone lifetime attribute is 60 days. More than one cold-standby DC can provide an overlapping series of viable offline domain controllers.
- [ ] Ensure you have immediate access to all backup credentials and license details in the event of an emergency rebuild.
- [ ] Ensure you have up-to-date access and the ability to restore from your current backups.
- [ ] Remove the Domain Administrators group from the backup platform Admin group—only allow 2nd tier access.

Short-Term

- [ ] Institute backup immutability (this can be done readily with a Hardened Repository or Storage SafeMode Snapshots).
- [ ] Use multi-tiered backup immutability to protect backups from intentional or accidental deletion:
    - [ ] Immutable backups in a cloud storage blob
    - [ ] Air-gapped and offline media or tape
    - [ ] Backups retained in an immutable state for X period of time even after deletion
    - [ ] Immutable backups in a hardened repository
- [ ] Employ real-time proactive monitoring & alerting:
    - [ ] Maintain visibility and mitigate issues with pre-set alarms and pre-built reports and heatmaps.
- [ ] Perform and maintain a latest copy/snapshot of backups in the opposite datacenter.

Long-Term

- [ ] Employ the 3-2-1-1-0 Rule as a best practice:
    - [ ] 3 - Maintain at least three copies of your data.
    - [ ] 2 - Store data on at least two different types of storage media.
    - [ ] 1 - Keep one copy of the backups in an off-site location.
    - [ ] 1 - Store at least one of the copies offline.
    - [ ] 0 - Be sure to have verified backups without errors.
- [ ] Replication may also be valuable to protect critical workloads and provide rapid recovery.
- [ ] Consider additional storage infrastructure to achieve sufficient capacity/redundancy for backups.
- [ ] Implement 3-tier account privilege structure (regular, server and domain).
- [ ] Consider a Continuous Data Protection (CDP) plan for critical workloads.

threadfin

PRE-Ransomware Checklist: Enable Rapid Recovery

Protect Data

Take action on these items before a ransomware attack occurs to lessen the attack's impact and enable rapid recovery if/when a breach occurs.

Immediate

- [ ] Enterprise-wide Multi-Factor Authentication (MFA) for all endpoints that support it. Configure MFA for additional account security, requiring continual secondary validation at every login.
- [ ] Turn MFA on for the backup server to provide access through RDP.

Short-Term

- [ ] Use multi-tiered backup immutability to protect backups from intentional or accidental deletion.
    - [ ] Immutable backups in cloud storage with consideration for dedicated bandwidth
    - [ ] Air-gapped and offline media (i.e., removable drives, rotating drives)
    - [ ] Backups on tape (and removed from the library or marked as WORM)
    - [ ] Backups retained in an immutable state for X period of time even after deletion
    - [ ] Immutable backups in a hardened repository
- [ ] Employ real-time proactive monitoring and alerting.
    - [ ] Maintain visibility and mitigate issues with alarms, reports and heatmaps.
- [ ] Create an air gap/enclosed network.
    - [ ] Test and restore the virtual machines (VM) inside that environment.
    - [ ] Eventually automate the testing and validation process.

Long-Term

- [ ] Verify backups automatically to ensure recovery.
    - [ ] Restore your data in an isolated virtual sandbox and scan for malware without impacting production systems.
- [ ] Rearchitect so the backup server is the only client using a direct over-the-network storage tool.
- [ ] Consider recovery orchestration.
    - [ ] Dynamically update and automate recovery plan testing and quickly recover any data type without manual intervention.
- [ ] Validate backups are clean before restoring them.
    - [ ] Scan machine data with antivirus software before restoring it to the production environment.
    - [ ] Perform as staged restore of your recovered virtual machines (VM) to ensure they don't contain any malicious, personal or sensitive data.
- [ ] Conduct and document recovery drills to verify restore capability, sequence, procedures, and eventually map out sequence to inform possible automation of recovery.
- [ ] Cloud-based disaster recovery as-a-service (or customer-managed cold/warm-standby cloud compute infrastructure) to provide offsite business continuance.

threadfin

PRE-Ransomware Checklist: Enable Rapid Recovery

Minimize Operational Impact

Take action on these big picture considerations before a ransomware attack to minimize operational impact in the event of an attack.

Immediate

- [ ] Encryption for all backup data in-flight and at-rest on compatible backup targets.
- [ ] Patch Management: Make sure all software, hardware and firmware in use are running up-to-date software levels that have shored up any known vulnerabilities.
- [ ] Unique passwords for every login source: Ensure that if one password or machine gets breached, the stolen password won't give hackers access to other accounts.
- [ ] Remove unused devices, applications and non-essential programs and utilities from all servers.
- [ ] Implement a 3-tier account privilege structure (regular, server and domain).
- [ ] Turn on MFA for the backup server access through RDP.
- [ ] Realign network architecture to enforce east-west traffic policies based on network segments/zones.

threadfin

Threadfin Business Solutions

We're an IT services-only company that creates incredible value through solutions that transform, modernize, optimize and secure organizations.

We're vendor-independent.
Our solutions are built for your specific needs and unique goals. We're focused on scalability, flexibility and cohesive integration with your environment

We're based in the United States.
We're US-based, with a national footprint and significant global delivery experience.

We know digital transformation.
We combine our proven technology delivery experience with our deep technical skills to provide unmatched digital transformation services.

We've perfected partner support.
Our unique partner support model empowers our partners with our advanced skills and expertise.

We're approachable experts.
Our team prides themselves on deep digital transformation skills and their willingness to collaborate and share their knowledge with our customers.

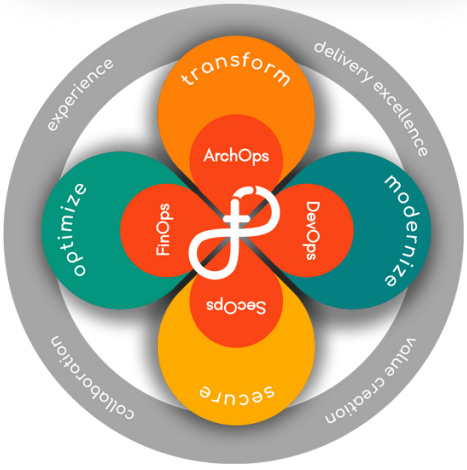
We serve mid-tier and enterprise.
Adept at navigating both simple and complex environments, we serve myriad industries.

Technical Expertise

Aruba • AWS • Azure
Cisco • Citrix • DUO Security
Entra • Fortinet • Google
HPE • Juniper • Meraki
Microsoft • NetApp • Okta
Palo Alto • SolarWinds
Veeam • VMware

analyze | assess | buildout | deploy | design | diagnose | health check | implement
migrate | remediate | refresh | support | transform | upgrade

- Business Applications
- Cloud (Private & Hybrid)
- Collaboration Tools
- Data & Databases
- Development & DevOps
- Enterprise mobility
- Network Infrastructure
- Security & Compliance
- Server Infrastructure
- Storage
- Unified Communications
- Virtualization



Our *Experience Threading Framework* illustrates the way we continuously improve digital experience for employees and customers.

The *Experience Threading* icon in the center represents the lifecycle of human-centered digital transformation. It's perpetual because technology continues to shift. It's pervasive, connecting through all the pillars, because they work in harmony.

Our team has migrated
TENS OF MILLIONS
of users to the cloud.