Checklist: Key Steps to Secure Your Domain Controllers for Ransomware Defense

threadfin

□ Modernize your domain controllers

Ransomware protection starts with modernizing your Active Directory environment. Old domain controllers running on outdated hardware & software are high-risk targets.

□ Back up your domain controllers

Ransomware actors specifically target virtual domain controllers & backups. The absolute best practice is to back up your domain controller, make sure backups are encrypted & that they're completely segregated.

- □ **Identify critical domain controllers:** Determine which domain controllers in your network are critical for your operations. Typically, all domain controllers play a vital role, but you may prioritize certain ones based on their roles and importance.
- □ **Choose backup methods:**
  - System-level backup: Use backup software to create system-level backups of the entire domain controller server. This method is useful for full server recovery.
  - Active Directory backup: Use Windows Server Backup or third-party tools to perform Active Directory-specific backups. This method allows you to back up the Active Directory database, which is crucial for AD recovery.
- □ **Schedule regular backups:** Set up a backup schedule that ensures regular & consistent backups of your domain controllers. Daily or weekly backups are common, but frequency may vary depending on your organization's needs.
- □ **Store backups securely:** Store backup files securely to prevent unauthorized access & ensure they're protected from the same threats that could affect your primary domain controllers. Consider off-site & offline backups to protect against ransomware attacks.
- □ **Test backup restorations:** Regularly test the restoration process from your backups to ensure they're valid & functional. This practice helps verify that you can recover your domain controllers & AD data when needed.
- □ **Document backup procedures:** Maintain detailed documentation of your backup procedures, including schedules, locations & recovery steps. This documentation will be invaluable during an emergency.
- □ **Implement redundancy:** Consider deploying multiple domain controllers in your network & distribute the roles to reduce the impact of losing a single DC. This way, even if one DC fails, others can continue to provide authentication & directory services.
- □ **Use Windows Server Backup (built-in tool):** Windows Server includes a built-in backup tool that can back up system state data, including Active Directory. You can use it to schedule regular backups of domain controllers.
- □ **Consider third-party backup solutions:** Many third-party backup solutions are designed specifically for Active Directory backup & recovery. These tools often offer more advanced features and flexibility.
- □ **Monitor Backup Status:** Implement monitoring & alerting to ensure that backups are completing successfully. This will help you catch & address issues early.
- □ **Review backup retention policies:** Define & adhere to backup retention policies to manage storage space effectively & ensure you can access backups when needed.
- □ **Train staff:** Ensure that your IT team is trained in backup & recovery procedures & that they understand the importance of maintaining up-to-date backups.
- □ **Update disaster recovery plan:** Integrate domain controller backup & recovery into your organization's broader disaster recovery plan, which should include procedures for responding to ransomware attacks, hardware failures & other disasters.

□ Secure administrative access

Monitor & secure administrative access rights to your domain controllers. Implement stringent policies to prevent unauthorized access to these critical components. By controlling privileged access & continuously auditing user account activities, you can limit the damage caused by compromised user credentials & reduce the risk of adversaries gaining initial access to your network.

□ Protect against physical threats

Don't overlook the importance of securing physical domain controllers. Even with state-of-the-art software defenses, unrestricted physical access to your servers can lead to devastating security breaches. Physical security measures such as locked server rooms & restricted internet access to sensitive network equipment are necessary precautions.

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.

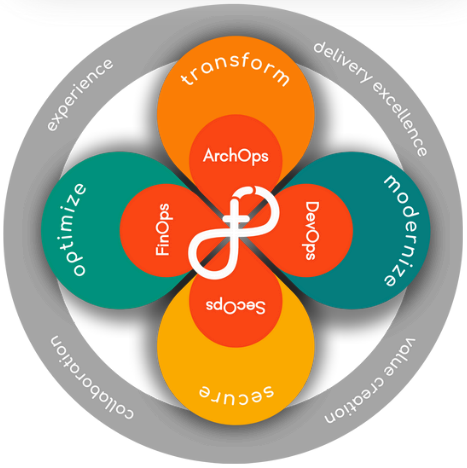
We serve mid-tier and enterprise.
Adept at navigating both simple and complex environments, we serve myriad industries.

Technical Expertise

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

analyze | assess | buildout | data center consolidation | 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 & Backup
- 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.

Click here for our Solution Snapshots.

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

threadfin.com | info@threadfin.com | 904.473.4840