

Ransomware Defense: How To Secure Your Domain Controllers

Roman Diaz | Practice Lead, Microsoft | Threadfin

September 25, 2024

Today I'm taking you back to the basics. The lock, so to speak, for your organization's digital assets, data and sensitive information. It's something you assume will always work. Something you may have even forgotten about. Until you're the victim of ransomware. And then you realize that you're toast. Absolutely, completely burned up toast.

Today I'm talking domain controllers—specifically how you can secure your domain controllers for ransomware defense. This isn't as exciting as the latest release of AI-whatever, but stick with me here. Domain controllers are the backbone of any Windows enterprise network. They're also often completely neglected, making them prime targets for ransomware actors. And one of the first things a threat actor does is attack domain controllers. If you don't have a copy, that leaves you with... nothing. Except a ransom to pay.

While domain controllers might be old news to some of you, I'm going to start with a bit of background to help all readers better understand domain controllers and why securing them is vital for ransomware protection. Then we'll move on to proactive best practices to safeguard your organization's digital assets and maintain a secure and reliable network environment. If you want to skip directly to the ransomware defense strategy, go to the section titled *Security*.

Domain Controllers Explained

A domain controller is a fundamental component of Microsoft's Active Directory (AD) environment. Domain controllers serve as the central authority for user authentication and network access in a Windows Server-based network. They store user credentials and account information, enforce security policies and facilitate the interaction between users and resources (such as files, printers and other networked devices) within the domain.

They help improve security on a network by providing a single point of authentication for users. This means that all users who want to access resources on the network must provide their credentials to the domain controller, helping to prevent unauthorized access to resources on the network. Here's how that works...

Authentication and authorization: When a user or computer logs into a Windows-based network, they provide their credentials (usually a user name and password). The domain controller verifies their user credentials, ensuring that the user or computer is who they claim to be. If the authentication is successful, the domain controller authorizes network access based on the user's permissions and group memberships.

Database of objects: Domain controllers maintain a database known as the Active Directory database. This database contains information about various objects in the network, such as user accounts, computer accounts, groups and organizational units (OUs). Each object has attributes that define its properties, such as username, password, group membership and more.

Replication: In larger networks, multiple domain controllers exist to ensure redundancy. These controllers use replication to keep the Active Directory database consistent across the network, ensuring seamless access for users.

Global catalog: One of the domain controllers in a network can be designated as a Global Catalog Server (GC). The Global Catalog stores a partial replica of all objects in the entire forest, making it possible to search for objects across domains and forests without the need to contact individual domain controllers.

Group policy: Domain controllers also play a role in applying Group Policy settings. Group Policy allows administrators to define and enforce policies and configurations for user and computer accounts. These policies can control security settings, software installations and other aspects of system behavior.

Secure communication: Domain controllers use secure communication protocols, like the Kerberos authentication protocol, to protect sensitive authentication information as it travels across the network. This helps prevent unauthorized access and eavesdropping.

Logging and auditing: They maintain logs of user authentication events, which are crucial for identifying security risks or unauthorized access attempts.

DNS integration: Active Directory relies heavily on DNS (Domain Name System) for name resolution. Domain controllers often include DNS services, and DNS records are used to locate domain controllers within the network.

Think about it this way: your domain controller is the roadmap to your entire infrastructure and all the permissions associated with that. If you lose your domain controller, all your workstations and your users lose their relationships. It takes an incredible amount of work—and frustration—to rebuild that.

The Evolution of Domain Controllers

Over time, domain controllers have evolved from simple on-premises servers to sophisticated components of hybrid cloud networks. Modern domain controllers, including virtual domain controllers, now support enhanced Active Directory security, improved backup systems and better cloud services integration. They also play a critical role in access management solutions, including support for multi-factor authentication and integration with third-party tools for enhanced security. These benefits—and those listed below—make a strong case for modernizing if you haven't done so already.

Hardware and performance: Today's domain controllers can run on more powerful hardware, including virtualized environments and cloud-based platforms. This allows for better scalability and performance, accommodating larger and more complex networks. Typically hardware can be consolidated and those costs can be reduced.

Operating systems: Modern domain controllers run on up-to-date versions of Windows with improved security features, better compatibility and enhanced performance.

Security: Current domain controllers employ more secure authentication mechanisms like Kerberos and offer advanced security features such as secure boot, [Credential Guard](#) and [Microsoft Defender](#) integration. Security is a top priority, with regular security updates and patch management.

Replication and redundancy: Modern domain controllers use improved replication methods, including more efficient change tracking and replication scheduling. Failover and redundancy are often easier to configure and can be automated for higher availability. Disaster recovery capabilities, like virtual machine snapshots, and better backup and restore options, are improved.

Cloud integration: Organizations are increasingly adopting cloud services and hybrid cloud architectures. This has led to the integration of cloud-based domain controllers (e.g., [Azure Active Directory Domain Services](#)) and the need to manage identity and access across on-premises and cloud environments. Integration with identity federation protocols like SAML and OAuth provide secure access to third-party services and applications.

Role in identity and access management (IAM): Domain controllers handle the authentication and resource access control core functions, but they are also integrated into broader identity and access management systems, including support for single sign-on (SSO), multi-factor authentication (MFA), and identity federation with cloud services. Implementing a robust access management solution around your domain controllers is crucial to prevent unauthorized access and maintain the integrity of your network.

Administration and management: Modern administration tools and consoles, such as the Active Directory Administrative Center, PowerShell and cloud-based management portals, have made managing domain controllers more user-friendly and efficient. Automation capabilities help streamline routine administrative tasks, reducing manual efforts and minimizing the risk of errors.

Why Modernizing Matters

Older domain controllers often run on outdated Windows Server versions with known vulnerabilities that can easily be exploited by ransomware actors. Here's why modernizing is key:

- **Security risk:** Legacy Active Directory servers may lack modern security features and are more susceptible to active directory attacks.
- **Privileged access vulnerabilities:** Older systems may provide unrestricted physical access or administrative access rights that are hard to monitor and control.
- **Backup systems:** Modern backup systems are more robust, offering encryption and segregation, protecting data from being compromised during ransomware attacks.

Now that you've got a basic understanding of domain controllers and the latest developments, let's switch our focus back to security...

Key Steps To Secure Your Domain Controllers for Ransomware Defense

Earlier in this article I highlighted the risk of ransomware, but that's not the only security risk when it comes to domain controllers. Compromised credentials, denial of service attacks and even physical attacks are worth mentioning. These domain controller compromises can lead to devastating breaches and expose your entire network to severe threats.

Obviously you want to deploy robust security measures on your domain controllers (firewalls, intrusion detection/prevention systems and physical security controls like locks and guards), but here I'm going to focus in on what I believe are the most critical: modernizing and backing up.

See the following pages of this article for a checklist of the steps outlined below.

Modernize Your Domain Controllers

Ransomware protection starts with modernizing your Active Directory environment. Old domain controllers running on outdated hardware and software are high-risk targets for ransomware strain infections. Here's why you should modernize:

- Older operating systems may have known security vulnerabilities that are no longer receiving security patches or updates from Microsoft. Modern domain controllers often run on the latest operating systems, which receive up-to-date security patches, helping to protect against known vulnerabilities.
- Legacy domain controllers may not be compatible with newer technologies and applications, limiting the functionality of the entire network.
- Older hardware and software may not provide the same level of performance and scalability as newer solutions.
- In some industries and organizations, compliance regulations may require the use of up-to-date and secure technologies, making legacy domain controllers a compliance risk.
- Newer versions of Windows Server and Active Directory offer improved security features, including better authentication mechanisms and enhanced protection against cyber threats.

Learn more from Microsoft directly [here](#).

Back Up Your Domain Controllers

Modernizing alone isn't enough. Backing up your domain controllers is just as important. While most everything is virtualized, ransomware actors specifically target virtual domain controllers and backups. The absolute best practice is to back up your domain controller, make sure backups are encrypted and that they're completely segregated. Whether that's in another cloud, in a closet or in the trunk of your car, it must be segregated.

While even grabbing an old server for this purpose will do in a pinch, here's what I recommend to ensure your backup systems are up to the task:

1. 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.
2. Choose backup methods:
 - a. 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.
 - b. 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.
3. Schedule regular backups: Set up a backup schedule that ensures regular and consistent backups of your domain controllers. Daily or weekly backups are common, but the frequency may vary depending on your organization's needs.
4. Store backups securely: Store backup files securely to prevent unauthorized access and ensure they're protected from the same threats that could affect your primary domain controllers. Consider off-site and offline backups to protect against ransomware attacks.
5. Test backup restorations: Regularly test the restoration process from your backups to ensure they're valid and functional. This practice helps verify that you can recover your domain controllers and AD data when needed.
6. Document backup procedures: Maintain detailed documentation of your backup procedures, including schedules, locations and recovery steps. This documentation will be invaluable during an emergency.
7. Implement redundancy: Consider deploying multiple domain controllers in your network and 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 and directory services.

8. 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.
9. Consider third-party backup solutions: Many third-party backup solutions are designed specifically for Active Directory backup and recovery. These tools often offer more advanced features and flexibility.
10. Monitor backup status: Implement monitoring and alerting to ensure that backups are completing successfully. This will help you catch and address issues early.
11. Review backup retention policies: Define and adhere to backup retention policies to manage storage space effectively and ensure you can access backups when needed.
12. Train staff: Ensure that your IT team is trained in backup and recovery procedures, and that they understand the importance of maintaining up-to-date backups.
13. Update disaster recovery plan: Integrate domain controller backup and recovery into your organization's broader disaster recovery plan, which should include procedures for responding to ransomware attacks, hardware failures and other disasters.

Secure Administrative Access

It's also vital to monitor and secure administrative access rights to your domain controllers. Implement stringent policies to prevent unauthorized access to these critical components. By controlling privileged access and continuously auditing user account activities, you can limit the damage caused by compromised user credentials and 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 and restricted internet access to sensitive network equipment are necessary precautions.

So there you have it—everything you may (or may not) have ever wanted to know about domain controllers. Let me close out this article by imploring you to make sure that yours are secure, up-to-date and backed up.

The importance of security, access control, and vigilant maintenance cannot be overstated. If you need support in this, Threadfin can conduct a well-planned modernization effort to help you stay competitive, secure and adaptable. We can also work with you on back up plans. [Contact us today](#) and we'll talk through it with you.

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.

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



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 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.

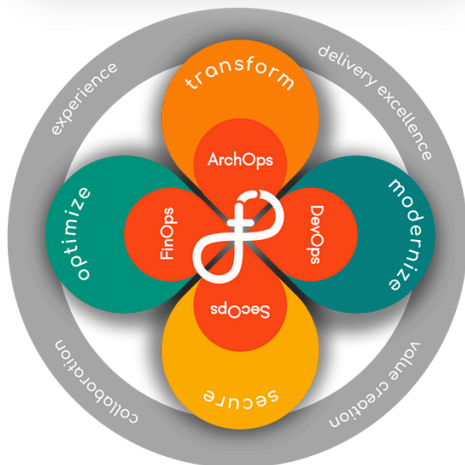
Adept at navigating both simple and complex environments, we serve myriad industries.

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.

