Implementing NIST, ESAE and Red Forest Cybersecurity Principles in Active Directory

Using Quest® tools to block increasingly pervasive insider threats

Written by Mark Barr, Software Solutions Architect, Quest

Most organizations have invested heavily in perimeter defense, but the reality is that 90 percent of organizations feel vulnerable to insider attacks.[1] An employee stealing intellectual property to take to a new job or a fat-fingered administrator making a critical configuration error are examples of breaches caused by someone inside the network. Often, an outside attacker takes over a legitimate account: Microsoft has reported that, every day, 95 million Active Directory (AD) accounts[2] and 10 million Azure AD accounts[3] are the target of cyberattacks.

The primary vector has now shifted from direct attack on a compute resource to theft of user credentials, often by means of a phishing attack. Once a user's credentials are obtained, the attacker has access to a workstation on which to run software that captures the credentials of other accounts. Preferred targets are service accounts and Domain Administrator accounts, allowing the attacker to traverse the infrastructure horizontally and vertically.

This paper examines how the United States Federal Government and Microsoft have responded to the increasingly pervasive insider threat. It also describes the Quest management tools with which to protect Active Directory, Azure Active Directory and Office 365 users and resources.

1 "2019 Insider Threat Report," Cybersecurity Insiders, November 2018, https://www.cybersecurity-insiders.com/portfolio/insider-threat-report/.

2 Fontana, John, "Active Directory czar rallies industry for better security, identity," ZDNet, June 9, 2015, https://www.zdnet.com/article/active-directory-czar-rallies-industry-for-better-security-identity/

3 Cimpanu, Catalin, "Microsoft Sees over 10 million Cyberattacks per Day on Its Online Infrastructure," Softpedia News, May 6, 2016, https://news.softpedia.com/news/microsoft-sees-over-10-million-cyberattacks-per-day-on-its-online-infrastructure-503774.shtml.

In most organizations, AD is the foundation for nearly all access to critical, sensitive and otherwise valuable data. There is no better place to apply the NIST Cybersecurity Framework.

THE FEDERAL GOVERNMENT RESPONDS: THE NIST CYBERSECURITY FRAMEWORK

On February 12, 2013, in Executive Order 13636, the National Institute of Standards and Technology (NIST) was directed to work with public and private stakeholders to develop a voluntary framework for reducing cybersecurity risks to critical infrastructure.

The resulting NIST Cybersecurity Framework applies to every organization, regardless of size, industry vertical and IT complexity. The standard is not mandated or compliance-focused; rather, it empowers IT organizations to establish an ongoing process for improving their cybersecurity posture.

NIST designed the standard not to be technology-specific, but to be used as a generically applicable security foundation. The intent is for organizations to use the lens of their business drivers to create a unique set of cybersecurity outcomes and activities that reduce risk.[4]

Applying the NIST Cybersecurity framework to Active Directory security

In most organizations, AD is the foundation for nearly all access to critical, sensitive and otherwise valuable data. There is no better place to apply the NIST Cybersecurity Framework.

As shown in Figure 1, the core of the Framework consists of five high-level cybersecurity functions.

1. Identify: Which assets need protection? The Identify function enables the organization to better understand its systems, applications, assets, data, and capabilities as the foundation for determining, prioritizing, and implementing Framework efforts.
2. Protect: Which safeguards are available? Establishing and implementing safeguards (based on what is discovered during the Identify function) are the focus of the Protect function.
3. Detect: Which techniques can identify incidents? Every implementation needs to be watched to identify the occurrence of a cybersecurity event. Monitoring and auditing the environment as part of the Detect function keeps the organization aware of any issues as they arise.
4. Respond: Which techniques can contain the impact of incidents? Should a cybersecurity event occur, the Respond function seeks to define the events that must be addressed, to mitigate the situation and to improve the state of cybersecurity.

Figure 1: NIST Cybersecurity Framework

4 For more information, see "Securing Active Directory by Using the NIST Cybersecurity Framework," a Randy Franklin Smith whitepaper commissioned by Quest and released in 2018.

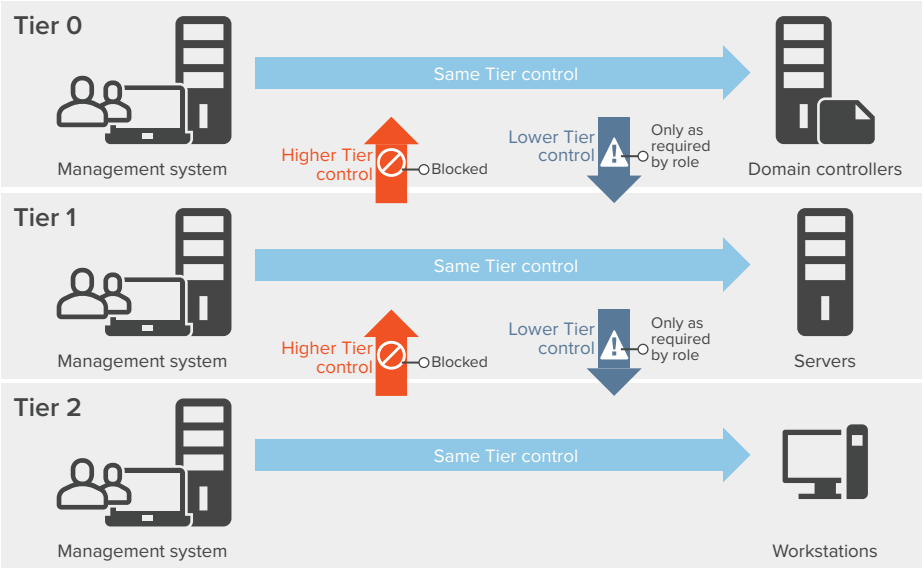

Figure 2: Control restrictions in the Active Directory administrative tier model

5. Recover: Which techniques can restore capabilities? An event often leaves a trail of compromised machines and questionable data. The Recover function seeks to put a plan in place to ensure operational resiliency and the ability to put the affected environment back into a known good state.

Together, the functions make up the strategic view of all the organization's cybersecurity risk.[5] Although designed with a security lifecycle in mind, the functions are intended to run concurrently and continuously.

MICROSOFT RESPONDS: THE ENHANCED SECURITY ADMINISTRATIVE ENVIRONMENT

To thwart attackers pursuing horizontal kill chains with pass-the-hash and related threats, Microsoft has delivered a reference architecture and other best practices that seek to isolate privileged credentials. Microsoft recommends a new security model, the Enhanced Security Administrative Environment (ESAE), for holding the accounts that require additional security due to their privileged access to the production forest.

ESAE is a special administrative forest, also known as a Red Forest, used to manage all privileged identities in AD, making it more secure. ESAE is built on a few core principles:

1. The introduction of the Red Forest, a highly secured bastion forest which contains all privileged-access user accounts for administration of the production forests
2. A reorganization of the production forest into a three-tier environment (depicted in Figure 2) in which administrator accounts are divided into three levels of security:
   - Tier 0: Domain Controllers (DCs), identity management resources, administrator user accounts and service accounts
   - Tier 1: Servers and applications
   - Tier 2: Standard user accounts, workstations, printers and devices
3. Privileged Access Workstations (PAWs): Highly secured workstations used by administrators
4. Multiple AD user accounts for administrators: a standard user account for logging into their workstation, accessing email and browsing the internet; and one administrative account for each tier in which they require elevated privileges

ESAE is a special administrative forest, also known as a Red Forest, used to manage all privileged identities in AD, making it more secure.

5 See also "NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1," April 25,2019, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

Microsoft has added native features and tools to Windows Server and to client operating systems to guard against credential theft.

5. Principle of Least Privilege (PoLP) applied to all user accounts
6. Prevention of any compromised identity from reaching horizontally across a tier or vertically into higher tiers

Incorporating this architecture and set of security principles into an existing Active Directory requires extensive planning, countless hours of implementation, additional compute resources (PAWs and servers) and user education.

Native features in Windows

Microsoft has added native features and tools to Windows Server and to client operating systems to guard against credential theft. Local Administrator Password Solution (LAPS), for example, integrates with Active Directory. LAPS can be configured to automatically manage and reset the local administrator password on every Windows workstation and server joined to a domain. LAPS stores the password in a secured attribute of each computer account in AD. When administrators need access to the computer, they retrieve the password from there.

Microsoft also provides several features for protecting credentials:

- Windows Defender Remote Credential Guard for remote Desktop access
- Restricted Administrator Mode for remote Desktop access
- Windows Defender Credential Guard for local computer access

IMPLEMENTING THE CYBERSECURITY FRAMEWORK AND ESAE WITH SOLUTIONS FROM QUEST

Quest is the go-to vendor for security and compliance solutions for any on-premises or hybrid Microsoft environment. Quest's solution suite enables IT teams to make their internal environment as secure as their perimeter.

For securing Active Directory using the NIST Cybersecurity Framework and implementing Microsoft's ESAE (Red Forest) model, several Quest solutions are particularly well suited, as shown in Table 1:

- Active Roles
- GPOADmin
- Change Auditor for Active Directory
- IT Security Search
- Recovery Manager for Active Directory Disaster Recovery Edition

The following sections map each of NIST's five functions to the Quest solutions for implementing a Red Forest-like end state.

NIST	Native (ESAE) Features in Windows	Quest Solutions
Identify	Legacy Active Directory management is a security risk	**Re-architecture of security and management for greater AD security**
Protect	LAPS, PAWs, Microsoft Identity Manager, Red Forest, 3-tier separation of AD objects, Group Policy Objects	**GPOADmin and Active Roles**
Detect	Reviewing event logs and PowerShell scripts to collect data; may require 3rd-party solution	**Change Auditor**
Respond	Manual intervention, usually long after a security breach occurs	**IT Security Search**
Recover	Windows Backup and authoritative restores —time-consuming and labor-intensive	**Recovery Manager for Active Directory Disaster Recovery Edition**

Table 1: NIST and ESAE models mapped to Quest solutions

Identify: Active Directory

To simplify NIST's Identify function, all of legacy Active Directory management is an identified security risk.

Most organizations fall into the trap of granting elevated access to too many user accounts over the years, resulting in hundreds of users with elevated rights in AD. Often, they are the same accounts used for accessing email and browsing the internet, making them vulnerable to malicious attacks aimed at compromising user credentials. From the external perspective, once attackers control a user account, they also control every resource to which the account is granted access; from the internal perspective, a disgruntled employee with elevated rights could launch a malicious attack.

Those organizations face the risk of unauthorized control of AD in two directions: vertical and horizontal.

Unauthorized vertical control

If administrators log onto workstations, servers, DCs and identity management systems with the same account, then a single compromised workstation means an entirely compromised AD. An attacker would then have credentials granting vertical control over computers in all three ESAE tiers.

To eliminate an attacker's ability to gain control vertically, separate all AD objects into the three ESAE tiers and create boundaries to prevent any single user account from interactively logging onto systems in multiple tiers. This can be accomplished using native AD tools such as the following:

- Security group membership
- Group Policy Objects (GPOs)
- Separate user accounts for administrators (that is, a standard user account and a Red Forest administrator account for each tier in which the user requires elevated access)
- A privileged access workstation for each administrator

Unauthorized horizontal control

In some organizations, desktop support technicians have accounts with administrator access to all workstations, or the server team has administrator access to all servers. In that scenario, an attacker could take horizontal control of all servers across tier 1 from a single compromised server or across tier 2 from a single compromised workstation.

Microsoft offers native tools (described above) to prevent horizontal access from one compromised computer to all computers in the tier:

- LAPS
- Windows Defender Remote Credential Guard
- Restricted Administrator Mode
- Windows Defender Credential Guard

Once those features are active, the real burden consists of the ongoing enforcement and maintenance of the boundaries, the additional AD forest and the additional workstations for each administrator user.

Protect: Active Roles and GPOADmin

Quest GPOADmin and Active Roles are ideal for protecting assets identified in the NIST Cybersecurity Framework in four ways:

First, Active Roles ensures that the security groups used to create the boundaries are not compromised. Once deployed, Active Roles continually monitors AD groups and users to maintain correct and mandatory membership in the groups used to enforce ESAE security boundaries. With automated, rule-based provisioning and deprovisioning, Active Roles adds new user accounts to security groups for the correct ESAE tier. Active Roles can make sure that a user account is added to a tier group and prevent it from being added to the groups of other tiers.

Second, GPOADmin and Active Roles greatly reduce the number of accounts requiring elevated access from hundreds to fewer than 5 or 10 for most organizations. The most effective way to secure elevated-access administrator accounts is to not grant elevated access to administrator accounts in the first place. Active Roles and GPOADmin allow administrators to have administrative access to the entire AD forest without granting their

Most organizations fall into the trap of granting elevated access to too many user accounts over the years, resulting in hundreds of users with elevated rights in AD.

user accounts any elevated privileges to AD security.

Users, groups, mailboxes, workstations and servers can be logically grouped and administrative tasks to those AD objects assigned to individuals using Active Roles managed Units and Access templates. Active Roles can also assign access to users and mailboxes residing in Azure and Office 365.

Similarly, GPOADmin allows for granting administrative access so that users can manage GPOs without the need for elevated privileges in AD. Users can be granted access to one, many or all GPOs, with permission to perform tasks at a low level of granularity. A user can edit a GPO but not deploy it or link it to an organizational unit (OU) without first going through an automated approval process.

An attacker could take horizontal control of all servers across tier 1 from a single compromised server or across tier 2 from a single compromised workstation.

Third, Active Roles and GPOADmin eliminate the need to add a bastion/Red Forest to the infrastructure to house administrative user accounts. A core component of the Microsoft ESAE model is the use of a bastion, or Red Forest, to house the separate administrative user accounts. Active Roles and GPOADmin eliminate the need for elevated rights, so that additional bastion is no longer required. The administrator user accounts can be housed in a separate tier-0 OU within the production AD forest. If a Red Forest is still required to house administrator user accounts for managing other resources outside of the production AD, Active Roles and GPOADmin can grant access to Red Forest accounts.

Finally, Active Roles and GPOADmin eliminate the need for administrator users to have a separate, privileged access workstation for administering AD. Active Roles and GPOADmin remove from the picture any native Microsoft AD tools that require elevated rights. Administrators log into Active Roles and GPOADmin clients installed on servers protected with Windows Defender Remote Credential Guard or published with Remote Desktop Services (RDS) or Citrix. The majority of users log on to the Active Roles Web Console.

Detect: Change Auditor

With Active Roles and GPOADmin protecting AD forests, the next function in the Framework is to detect all changes. Quest Change Auditor for Active Directory collects all changes from agents installed on every DC. Administrators can configure Change Auditor reports for changes to a single attribute or GPO setting, or to all objects in an OU or domain.

Change Auditor displays all changes as they occur, assigning a severity level to each change. Three levels — high, medium and low — are provided, and administrators can add custom levels. They can also configure email alerts for specific addressees based on the severity of the change, the type of object changed or the account making the change.

Change Auditor can be fully integrated with Active Roles, GPOADmin and Recovery Manager for Active Directory, enabling full audit capabilities of changes made through those tools. It tracks changes made in Office 365 and Azure AD instances, providing reports and alerts for changes made to Microsoft cloud assets. Change Auditor can also send data to the organization's Security Information and Event Management (SIEM) tool.

Respond: IT Security Search

When Change Auditor sends an alert about a suspicious change, IT must respond as quickly as possible. IT Security Search is a Google-like, IT search engine from Quest that enables IT administrators and security teams to quickly respond to security incidents and analyze event forensics. The tool's web-based interface correlates disparate IT data from many Quest security and compliance solutions, including those described above, into a single console.

With IT Security Search, administrators can reduce the complexity of searching and analyzing IT data scattered across information silos. They can speed up their investigations and troubleshoot widespread issues should an outage or security breach occur. IT Security Search is provided free to all customers of Quest security and compliance solutions.

Recover: Recovery Manager for Active Directory Disaster Recovery Edition

Imagine a scenario in which a service desk is suddenly flooded with calls from users unable to log into their computers or applications. Investigation reveals that AD for a domain or an entire forest is down because SYSVOL has been corrupted. The cause could be a malicious attack, the spiteful action of a disgruntled employee or a planned change gone horribly wrong.

The options for recovery are to spend hours trying to correct SYSVOL, which may or may not work, or to restore AD from backup. Depending on the size of the forest and the number of remote sites, the complete restore of AD could take several days using legacy backup-and-recovery utilities and following best practices from Microsoft.

Quest Recovery Manager for Active Directory Disaster Recovery Edition provides a centralized console for recovering an entire AD forest in a matter of hours. When it backs up AD, it places a copy of the backup on the domain controller (DC), and it can also store a copy on a central file share. To completely recover an AD, the administrator creates a recovery job, which includes choosing the DCs to recover from the locally stored .bak file, and choosing the DCs to demote and then promote again. The administrator verifies that the server can communicate with the Forest Recovery agent on each DC and starts the job. The console displays the progress and status.

If an AD fails because a virus or natural disaster has rendered all DCs in the forest incapable of functioning normally, Recovery Manager for Active Directory Disaster Recovery Edition can perform a bare-metal restore of all DCs from backup. The only requirement is that the native Windows Server Backup feature must be installed on every DC.

Recovery Manager for Active Directory Disaster Recovery Edition allows recovery of deleted objects and restoration of modified objects to a previous state, without the need to perform a complete forest recovery. It is also useful in preventing accidental corruption in case a planned change goes wrong. Prior to making the change, administrators can use Recovery Manager for Active Directory Disaster Recovery Edition and snapshots of live DCs to build an Active Directory Virtual Lab (ADVL) on VMware or Hyper-V hosts. The resulting ADVL is an exact duplicate of the domain or forest on which the change can be tested before deployment in the production environment.

CONCLUSION

Insider threats, whether accidental or intentional, show no signs of abating, so shielding user credentials from attack and theft has quickly risen as a priority for IT administrators. NIST Cybersecurity and Microsoft's ESAE ("Red Forest") are valuable models for protecting credentials, particularly those that reside in Active Directory.

Quest solutions map directly to functions in the Cybersecurity Framework. They either supplement or outperform native Windows offerings to identify and protect AD and to detect, respond to and recover from attacks on those assets. IT administrators can use Quest tools to implement and maintain a Red Forest Active Directory environment, with user credentials held safely in AD.

> The most effective way to secure elevated-access administrator accounts is to not grant elevated access to administrator accounts in the first place.

FEATURED QUEST SOLUTIONS

Learn more about the Quest solutions featured in this paper:

- Active Roles
- GPOADmin
- Change Auditor for Active Directory
- IT Security Search
- Recovery Manager for Active Directory Forest Edition

ABOUT THE AUTHOR

Mark Barr is a software solutions architect in the Professional Services Organization at Quest. He has more than 20 years of Microsoft Windows server experience and multiple MCSE certifications including Windows NT, 2003, 2008, 2012 and MS Exchange 2013. In his most recent role, he has spent several years working on the architecture of solutions for Quest customers building out their Microsoft infrastructure.

ABOUT QUEST

Quest provides software solutions for the rapidly changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid data centers, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.