THREE WAYS A PRIVILEGED USER CAN HOSE YOUR ACTIVE DIRECTORY

And eight ways to minimize the risk and maximize your ability to recover

Quest™

Introduction

A CAUTIONARY TALE

Disappointed with his bonus, UBS Paine Webber IT admin Roger Duronio wrote 50 lines of code and rolled it out to thousands of systems on the company network, using the same standard Unix admin tools used to deliver legitimate files to those systems.

Then he quit.

But his logic bomb didn't. It faithfully counted down the weeks, giving Duronio time to place $20k in orders to short UBS/PW stock. Then, one morning, it detonated. The payload was reportedly "rm -rf /" — which means delete EVERYTHING.

It was pure pandemonium. UBS/PW had to resort to pen and paper to do trades. They spent $3 million in IBM consulting fees alone to get systems restored from backup. Who knows what the total costs were.

ABOUT THIS DOCUMENT

This is just one example of how a disgruntled or careless privileged user can wreak havoc.

In fact, in a Windows environment, it's fairly easy to do, because everything relies on Active Directory (AD). If Active Directory is down, your entire network is down — even if there's nothing wrong with any of your servers and applications.

How easy is it? This ebook shows just three of the many ways a privileged user — or an attacker with stolen privileged credentials — can take down your AD, and with it, the rest of your network.

Then we'll discuss eight critical best practices that can help you reduce this risk and improve your ability to recover if the worst does come to pass.

Three ways a privileged user can hose your AD

METHOD 1: DENY LOGON RIGHTS

There are five ways a user can log on to Windows: locally, from the network, as a batch job, as a service and through Remote Desktop Services. For each of these logon methods, there is a pair of logon rights, one to allow logon and another to deny logon.

By assigning the five deny logon rights in the right way, a privileged user can bring operations to a standstill:

- Users will be unable to log on to their workstations.
- Admins won't be able to get into the domain controllers, even using the local keyboard and screen at the console.
- Service accounts won't be able to log on.
- Applications won't be able to start.

This is a double dilemma: Since you can't log on with a domain account, you won't be able to fix the problem remotely. Instead you'll need physical access to your DCs so you can reboot into DSRM and begin recovery operations from there.

By assigning deny logon rights in the right way, a privileged user can bring operations to a standstill.

METHOD 2: TAKE DOWN DNS

Active Directory uses DNS as its mechanism for locating domain controllers (DCs). Every Windows Server 2003 or later Active Directory domain has a DNS domain name, and every Windows Server 2003 or later computer has a DNS name.

To hose your Active Directory, all a privileged user has to do is delete all of the DNS entries on one DC. Those changes will soon be replicated to all the other DCs using the cached DNS. Then the DNS cache will time out, and suddenly nobody will be able to find anything. In particular, workstations won't be able to find domain controllers using DNS. They will resort to NetBIOS name resolution, which may or may not work.

If DNS is down, everything is down.

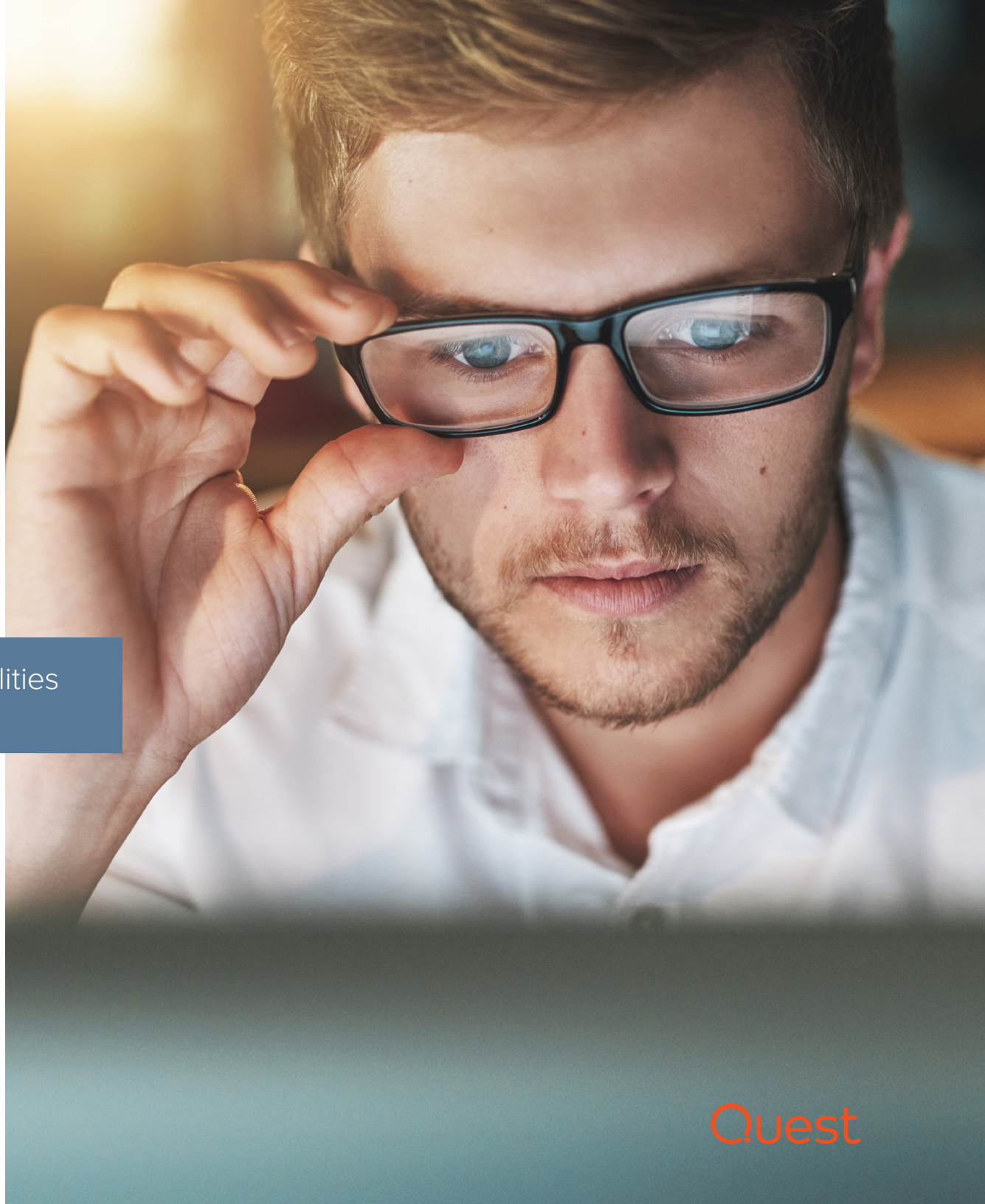
Quest

METHOD 3: EXPLOIT A VULNERABILITY IN THE OPERATING SYSTEM

One day, an organization running Windows Server 2008 found all of its DCs in an endless reboot cycle. It turned out that a privileged user had gone into a subnet and accidentally changed an IPv6 setting to an invalid IP address. When the Knowledge Consistency Checker (KCC) replication setup process encountered the invalid setting, it crashed. That caused the DC to reboot — but not before the invalid setting had been replicated to the other DCs across the entire environment, causing them all to start rebooting repeatedly.

Unknown or unpatched vulnerabilities can bring down your AD.

Microsoft has issued a fix for this problem, so if you're still in Windows 2008 or 2008 R2, make sure you're up to date on patches. But there is no guarantee that there are no other vulnerabilities that a privileged user could deliberately exploit or accidentally stumble upon, with similarly disastrous consequences.



It’s not just disgruntled insiders

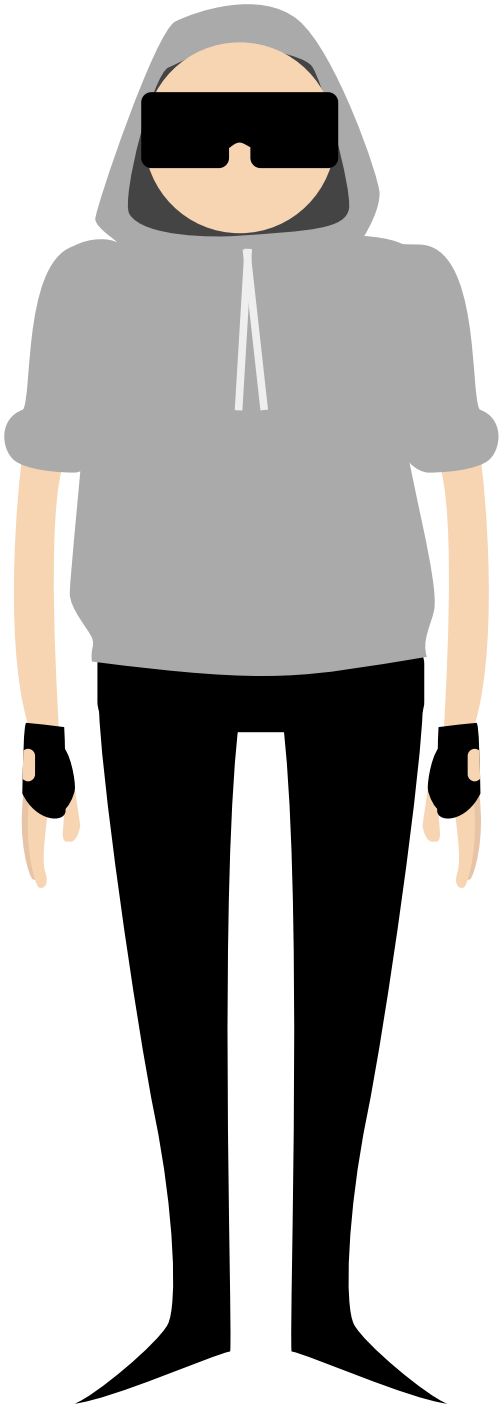
Too many organizations try to dismiss the risk of these types of scenarios by claiming that they don’t have any unhappy or malicious privileged users to become insider threats. Even if you could somehow guarantee that to be true (both now and into the future), you’re still at risk, for two reasons. First, even the most honorable admins can make mistakes, like the invalid IPv6 setting we just discussed. Second, privileged credentials can be stolen and misused in a cyber attack by a variety of threat actors who do have malicious intent, such as:

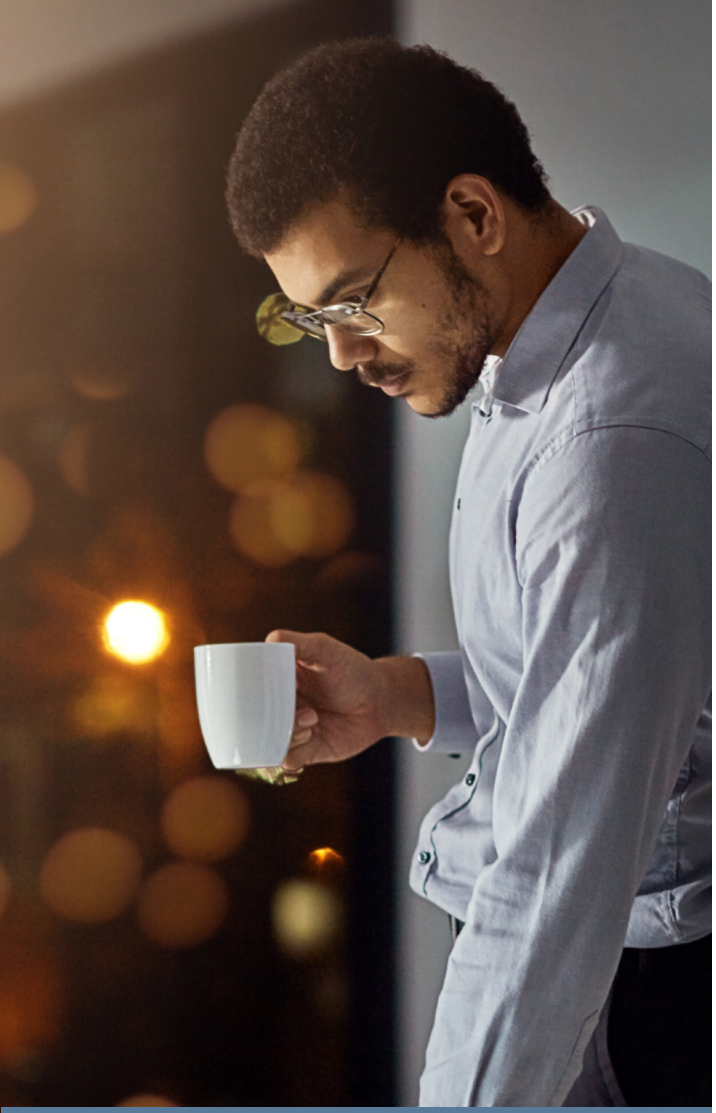
- Hackivists
- A hostile state-sponsored group
- Competitors
- A wronged party
- A nihilistic jerk

Companies are just as worried about data breaches caused by user carelessness, negligence or compromised credentials (51%) as they are about breaches caused by malicious insiders (47%).

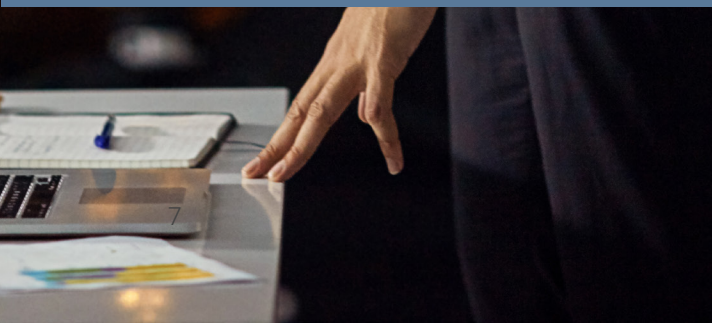
Source: *2018 Insider Threat Report*, ***Cybersecurity Insiders***

Keep in mind that not all of these attackers want to invest the time and effort required to steal your data. Some of them simply want to bring down your services and destroy your business, which is much easier.





It's vital to strictly control membership in privileged groups.



Eight AD security best practices

It's clear that privileged accounts represent a real and serious risk. But of course you can't just eliminate them; they are vital to keeping your systems up and running. Fortunately, there are proven steps you can take to reduce the risk that privilege accounts will be misused, either deliberately or accidentally, and to ensure that you can recover as quickly as possible if those preventative measures should fail. Here are eight key best practices to implement.

1. LIMIT PRIVILEGED ACCESS.

It's vital to strictly control membership in privileged groups, including the following:

- Domain Admins
- Enterprise Admins
- Schema Admins
- Administrators
- DHCP Administrators
- Group Policy Creator Owners
- Domain Controllers
- Network Configuration Operators
- Server Operators
- Backup Operators

Also carefully control all Group Policy objects (GPOs) that affect your domain controllers and all software installed on the DCs. For example, if an agent is installed, people who have access to that agent might very well effectively be domain admins.

The best way to control privileged access is to use a full-fledged privilege account management (PAM) and privilege session management (PSM) solution, with human approvals and live supervision for levels of access that would impact your entire domain. Since no one should need to touch domain controllers in any way on a daily basis, it's practical to require two people to be present for all activity: one person doing the work and one person to supervise. Even if the supervision is done remotely or by a peer, it reduces the ability of a lone wolf to damage your business. In addition, improving accountability and having two sets of eyes reduces the risk of costly mistakes.

Quest

2. SECURE PRIVILEGED ACCOUNTS IN A RED FOREST.

It can be very difficult to harden production forests enough to sufficiently protect your most highly privileged admin accounts without breaking functionality in the domain. Therefore, Microsoft now offers a way to hold those accounts in a dedicated administrative forest, officially named "Enhanced Security Admin Environment" (ESAE) but informally called "Red Forest" — "red" because of the critical nature of the credentials.

A key feature of the Red Forest model is that admin accounts are divided into three levels of security:

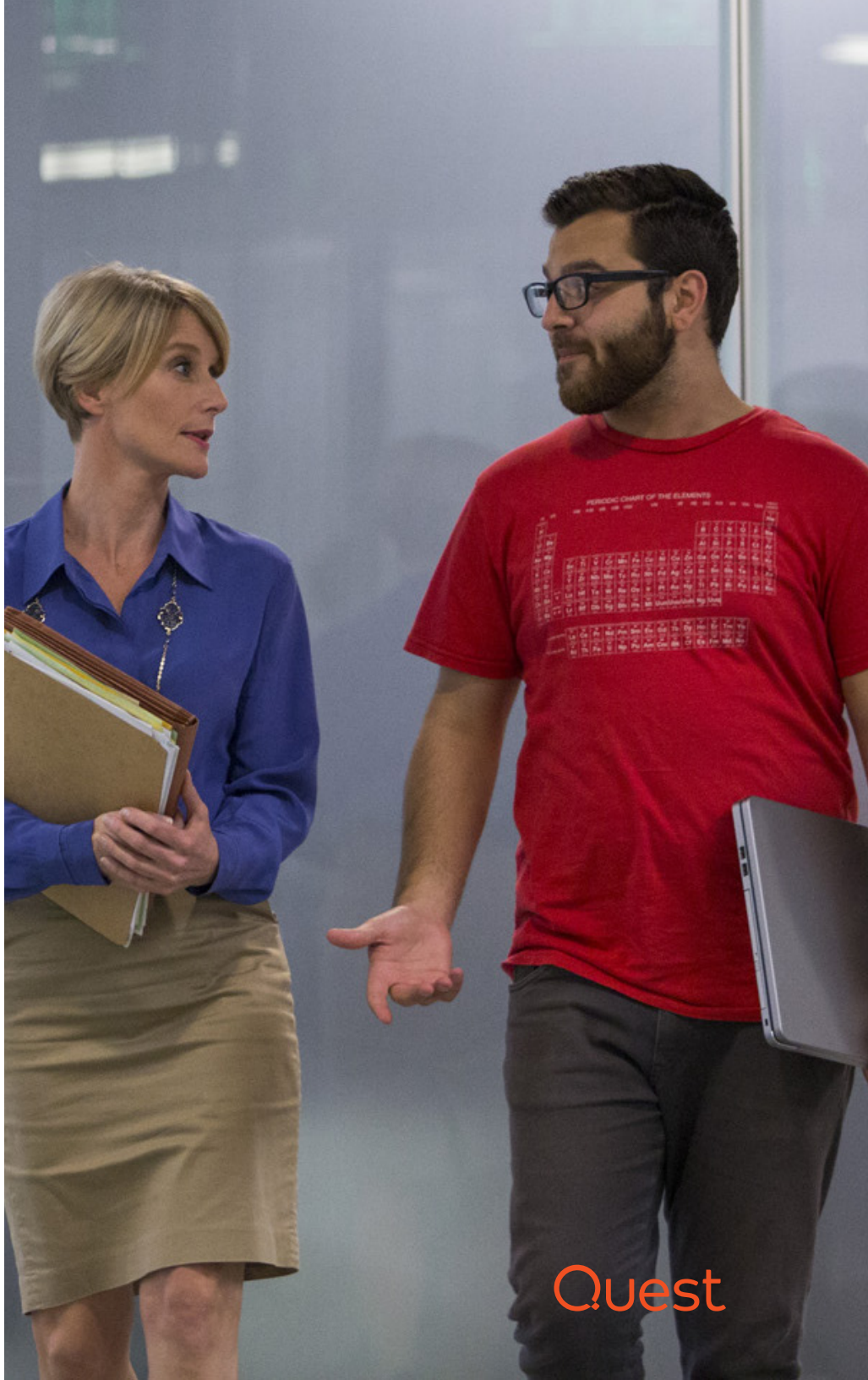
- **Tier 0 —** Forest-level admin authority (enterprise admins)
- **Tier 1 —** Server, application and cloud admin authority
- **Tier 2 —** Administrative control of workstations and devices

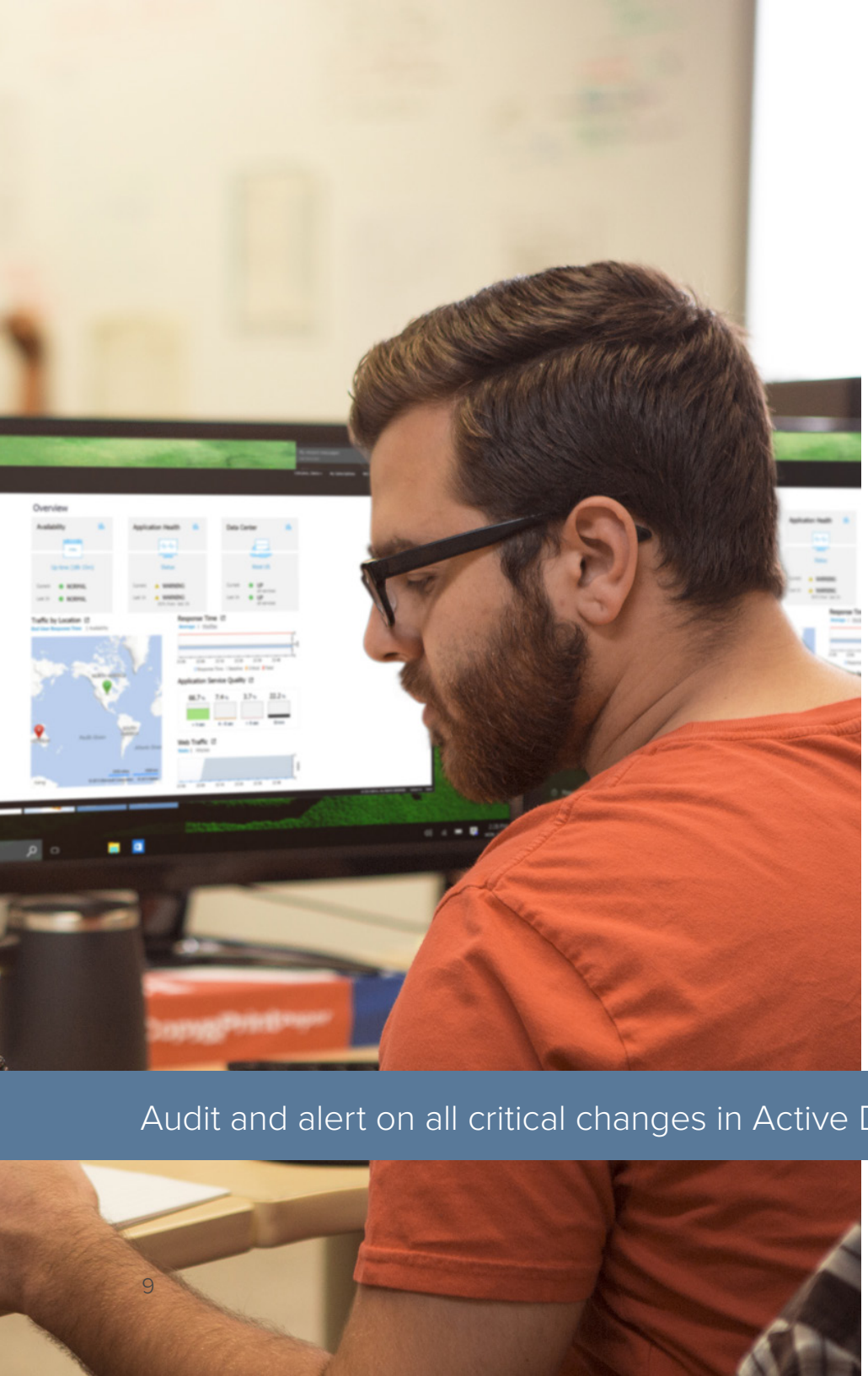
By putting all of your Tier 0 accounts into a separate forest, you can more easily keep a close eye on them — and more easily apply additional security requirements, such as requiring that they log on from a hardened workstation or enforcing two-factor authentication.

Of course, deploying an administrative forest is not a trivial task. For more information, watch a recorded webcast in which security expert Randy Franklin Smith explains the reasons why you might go to this extra trouble — as well as the limitations of the Red Forest model.

3. TEST CHANGES BEFORE MAKING THEM IN PRODUCTION.

To reduce the chances of mistakes hosing your AD, set up a test lab where you can review the impact of upgrades or other changes before making them in the production environment. The more closely the test lab matches production, the better.





Audit and alert on all critical changes in Active Directory.

4. AUDIT.

Comprehensive auditing is important for several reasons. It helps ensure accountability, which can deter malicious actions by insiders and also spur wll-intentioned privileged users to act with more care, reducing the number and severity of errors. It also helps you quickly determine what went wrong and take corrective action, as well as know how to prevent the same issue from occurring again later.

Be sure your audit trail includes native events, application system security logs, directory services logs and other critical data, and that you can quickly review, search and analyze the data. And make sure your audit system is accessible in event of AD failure.

5. MONITOR AND ALERT ON CRITICAL CHANGES.

Be sure you know immediately when a change is made to any critical object, such as a privileged group or a GPO that affects your domain controllers. Since such changes should be rare, you will not get inundated in alerts. Alerts about legitimate changes serve as confirmation that your monitoring system is working. And alerts about unauthorized changes enable you respond quickly, perhaps in time to avert serious consequences.

6. DOCUMENT YOUR AD STRUCTURE.

Take the time to document your AD structure. Keep that record up to date, and store it offline (for example, in Dropbox), where you can access it even if AD is down. Be sure to include information about:

- Forests
- Domains
- Trusts
- DNS
- Subnets and replication links between them
- Each domain controller, including its IP address, its physical location, which domain it controls, the flexible single master operations on it, and whether it is a global catalog

Quest

7. BACK UP ACTIVE DIRECTORY.

Back up Active Directory with an enterprise backup solution. Don't just rely on Recycle Bin recovery.

Remember, the Recycle Bin is a convenience and nothing more. It has multiple serious limitations, which we explore in the white paper, "The Windows Server 2016 and Azure AD Recycle Bins, and Quest Recovery Solutions." For example, remember how we noted earlier that someone could hose your AD by deleting all your DNS records? Well, instead of deleting the records, a malicious user could replace the settings with invalid IP addresses. The Recycle Bin is not going to help you restore those attributes.

8. TEST YOUR BACKUPS.

It's vital to regard backups as faulty until proven otherwise. Check the viability of a backup by actually mounting it and reading an object from it. Also periodically rebuild your Active Directory forest in a test environment to ensure you can recover from a major problem, and do so quickly.

Back up Active Directory with an enterprise backup solution, and test those backups.

Conclusion

When the phones light up and nothing is working, you don't know what's happening or the scope of the problem. It could be that a disgruntled insider has just acted out. Maybe you've been hit by weaponized malware. Or perhaps an accidental mistake has taken down your AD.

Following the best practices outlined here will reduce the chances of these unhappy scenarios, but nothing can eliminate the risk entirely. Therefore, you also need to take measures to facilitate a quick Active Directory recovery, including maintaining a clear and comprehensive audit trail and ensuring you have reliable backups.

You've probably heard nightmare tales of trying to rebuild AD over the weekend. Recovering AD is not as simple as restoring some files that got deleted. And it's not easy to test or simulate, in part because the right AD recovery procedure depends on the particular disaster scenario.

But with the right solution in hand, you can rebuild your entire Active Directory forest with a single click. To learn more, please read our white paper, "That Dreaded Day: Active Directory Disasters & Solutions for Preventing Them."

With the right solution in hand, you can rebuild your entire Active Directory forest with a single click.

Quest

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

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.

Ebook-3WaysToHoseYourAD-US-GM-32410

Quest