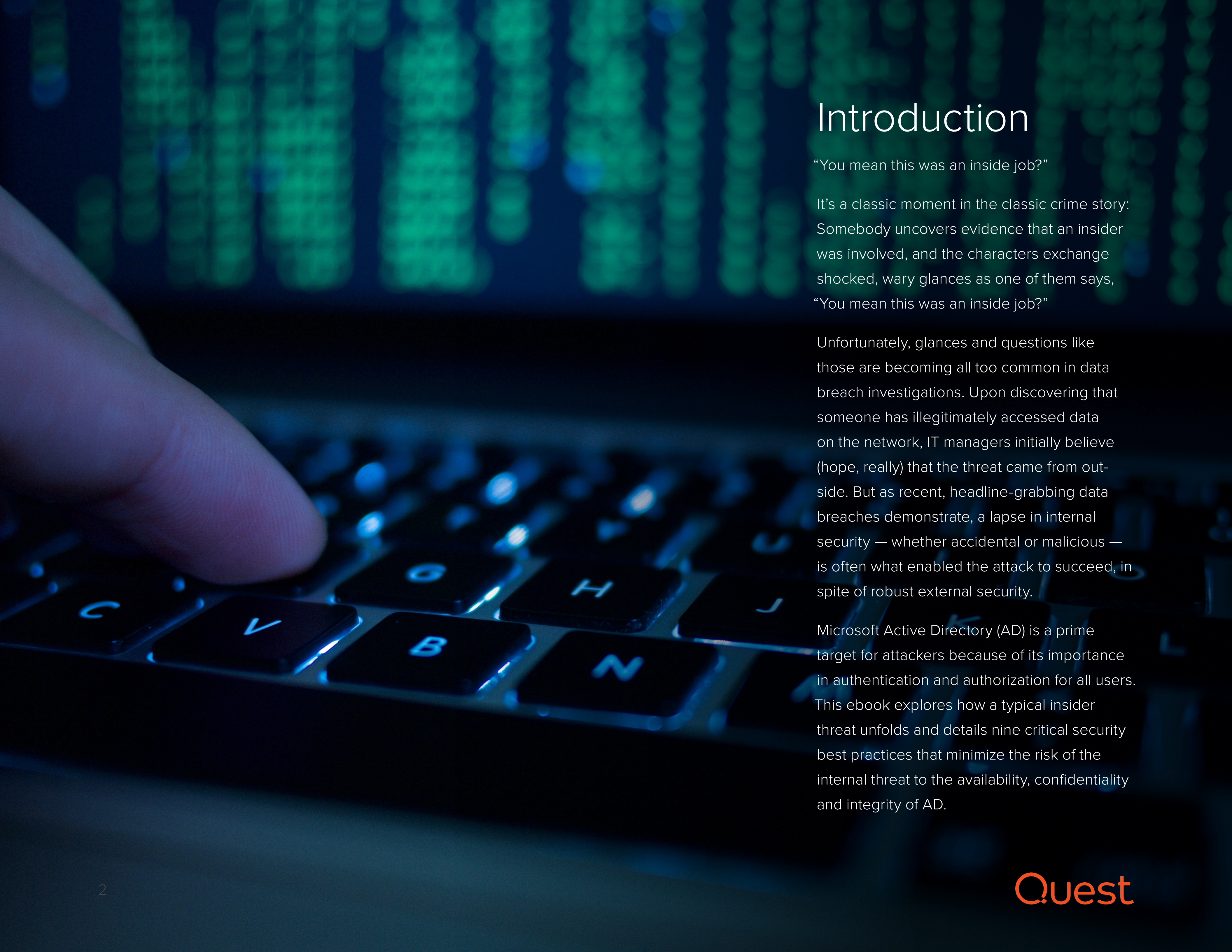
NINE BEST PRACTICES FOR ACTIVE DIRECTORY SECURITY

The anatomy of an insider threat and the best defense strategies

Quest™ | Hybrid Active Directory Security



Introduction

“You mean this was an inside job?”

It’s a classic moment in the classic crime story: Somebody uncovers evidence that an insider was involved, and the characters exchange shocked, wary glances as one of them says, “You mean this was an inside job?”

Unfortunately, glances and questions like those are becoming all too common in data breach investigations. Upon discovering that someone has illegitimately accessed data on the network, IT managers initially believe (hope, really) that the threat came from outside. But as recent, headline-grabbing data breaches demonstrate, a lapse in internal security — whether accidental or malicious — is often what enabled the attack to succeed, in spite of robust external security.

Microsoft Active Directory (AD) is a prime target for attackers because of its importance in authentication and authorization for all users. This ebook explores how a typical insider threat unfolds and details nine critical security best practices that minimize the risk of the internal threat to the availability, confidentiality and integrity of AD.

Insider attacks and their impact

THE KEY PLAYERS IN INSIDER ATTACKS

Many organizations believe that improper insider actions — whether accidental or malicious — can cause as much damage as externally initiated attacks. Attention centers on poorly trained or disgruntled current and former employees, but service providers and business partners play a growing role in committing or facilitating cybercrimes. In addition, the theft of credentials from all these types of insiders is increasingly common.

Insider attacks take many of the same shapes as other crimes, including:

- Cross-border economic espionage
- Well-planned conspiracies to steal trade secrets
- Authorized users copying credit card data and selling it on the black market

THE COST OF INSIDER ATTACKS

No matter the reason behind an insider attack, the cost to the business can be very high. In addition to the time and money required to restore security to systems and notify victims, the total cost involves things like the loss of confidential information, the consequences of failing to satisfy compliance regulations such as GDPR, harm to the organization's reputation that can result in lost customers, and disruption of critical systems such as Active Directory.

How much does this add up to? According to the Ponemon Institute, the average total cost of a data breach in the U.S. is $7.35 million, while the global average is $3.62 million. But more than half of companies candidly admit that they have no idea how high or low to estimate their potential losses from an insider attack.

The average total cost of a data breach in the U.S. is $7.35 million.

Quest

Active Directory: the crown jewels

WHY AD IS A PRIME TARGET

Because Active Directory is the primary authentication and authorization directory for over 90 percent of the world's enterprises and some 500 million active user accounts, it is a common target for cyberattacks. In fact, over 95 million AD accounts are under cyberattack on a daily basis, according to Microsoft.

Hardening external security is no guarantee of AD security, because the biggest threats to AD security are internal, and more than half of insider misuse involves abuse of privileges. That extends to accidental or malicious misuse of AD permissions, elevated accounts and sensitive groups that can weaken security protocols and lead to unauthorized access to sensitive Windows-based data.

HOW THE GROWING POPULARITY OF OFFICE 365 MAKES THE INSIDER THREAT EVEN MORE ALARMING

As Microsoft Office 365 adoption continues to grow, the complexity of securing AD increases. There are over 10 billion AAD authentications annually, and 10 million of those are attempted cyberattacks. Under the hood of Office 365 is Azure AD (AAD). Used by all Office 365 apps to authenticate users, Azure AD serves as the central nervous system that makes Office 365 possible. But every Office 365 instance requires a separate AAD tenant — yet another environment IT must manage and secure.

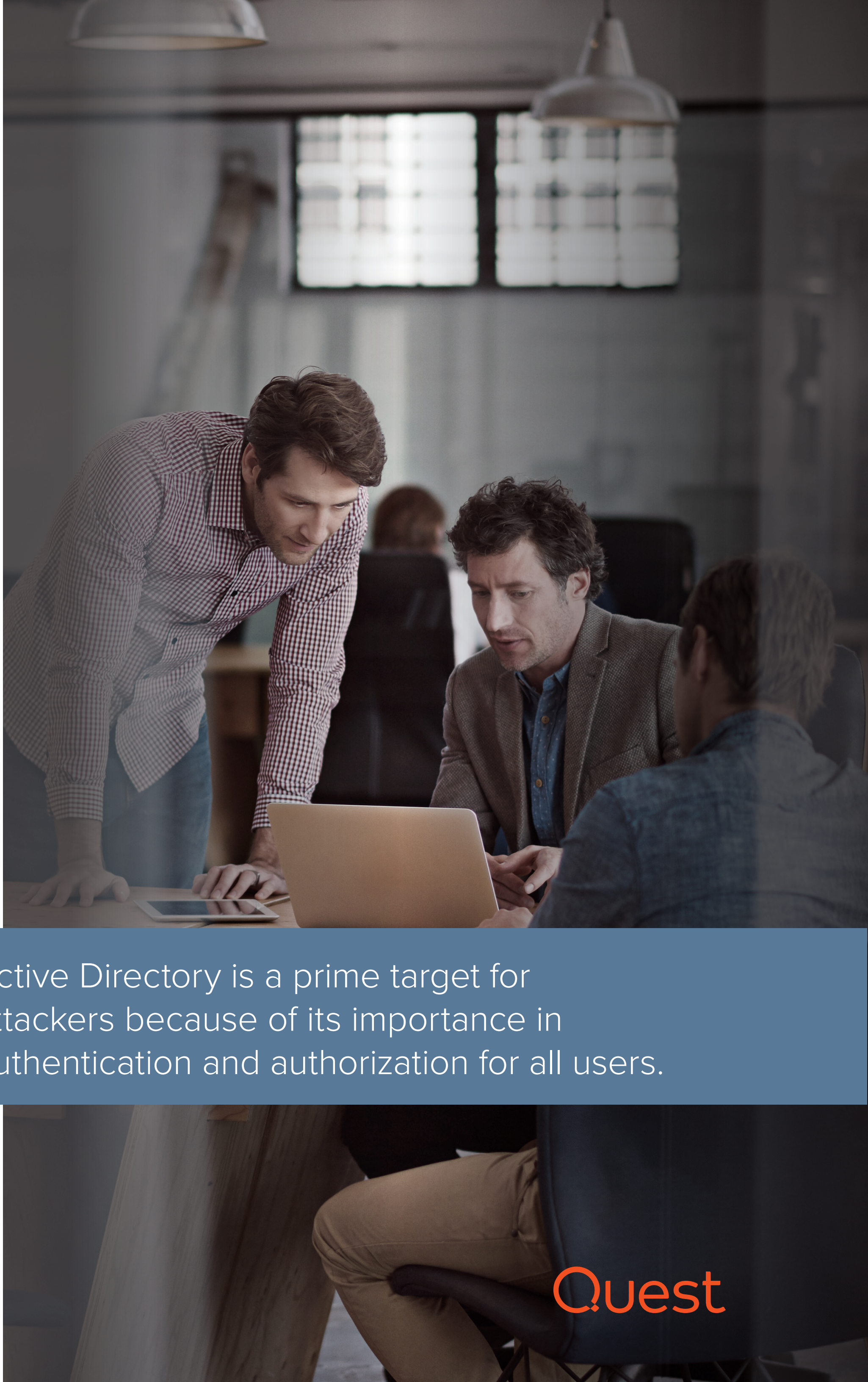
To address this issue, over 75% of customers with more than 500 employees using Office 365 are syncing their on-premises AD to Azure AD to allow for single authentication, thus creating a hybrid AD environment. Specifically, using Azure AD Connect, organizations integrate the two directories, keeping both environments in sync and giving users the ability to seamlessly log into Office 365 using their on-premises credentials. Because it's a one-way sync to AAD, it's important to remember that your on-premises AD environment dictates the contents of AAD. Therefore, your on-premises AD becomes the focal point for governing access controls, creating security compensations controls, and determining how access is granted in AAD and associated applications.

In short, any access gained through on-premises AD can have repercussions not just within AAD; they can also reach well into any web-based applications leveraging AAD. Therefore, you need to put security controls in place within your on-premises AD that will be reflected in your AAD instance, keeping the whole of your hybrid AD secure.

WHAT AN AD BREACH MEANS TO THE BUSINESS

Whether an organization has an on-premises or hybrid environment, without Active Directory, it loses multiple business-critical resources: Exchange, collaboration, real-time communications, SharePoint, SQL Server databases, web servers and more.

Unauthorized access to AD is like having a stolen key card: Once attackers are inside the building, they can take the elevator, wander through offices, open desks and look through drawers. With so many accounts under unrelenting attack from within and without, the insider threat to on-premises and hybrid AD environments is clear and present.



Active Directory is a prime target for attackers because of its importance in authentication and authorization for all users.

The challenges of securing AD

AD is built to be secure, but security breaks down when elevated access is in the wrong hands. Even in hybrid AD environments, where Microsoft promises a financially-backed, 99.9% service-level agreement for Office 365, change control, access governance and overall data security are still the responsibility of the customer.

Consider four main challenges IT administrators have to contend with:

LIMITATIONS OF NATIVE AUDITING

With native AD auditing alone, it can be difficult to detect insider threats and prevent breaches. Limitations include:

- Event details contain limited context, and some actions that insiders exploit (such as change to GPO settings and nested group membership) are not captured at all.
- There is no comprehensive view of all changes from all native log sources. For example, DCs and servers have multiple native logs. Therefore, searching for a specific event is time-consuming and error-prone.
- There is no proactive alerting on suspicious events.
- There is no reporting capability to satisfy internal security groups or external compliance requirements.
- There is no way to prevent unwanted changes to the most sensitive objects.

Native Azure AD auditing comes with its own challenges, including:

- There is no way to monitor audit policies to know if they change or are disabled by other administrators.
- The audit data is very raw and lacks friendly display names, and the format is constantly changing. In fact, there is no normalized 5W format (Who, What, When, Where, Workstation/Origin) across events.
- Audit data is retained for a limited time before it is permanently lost.

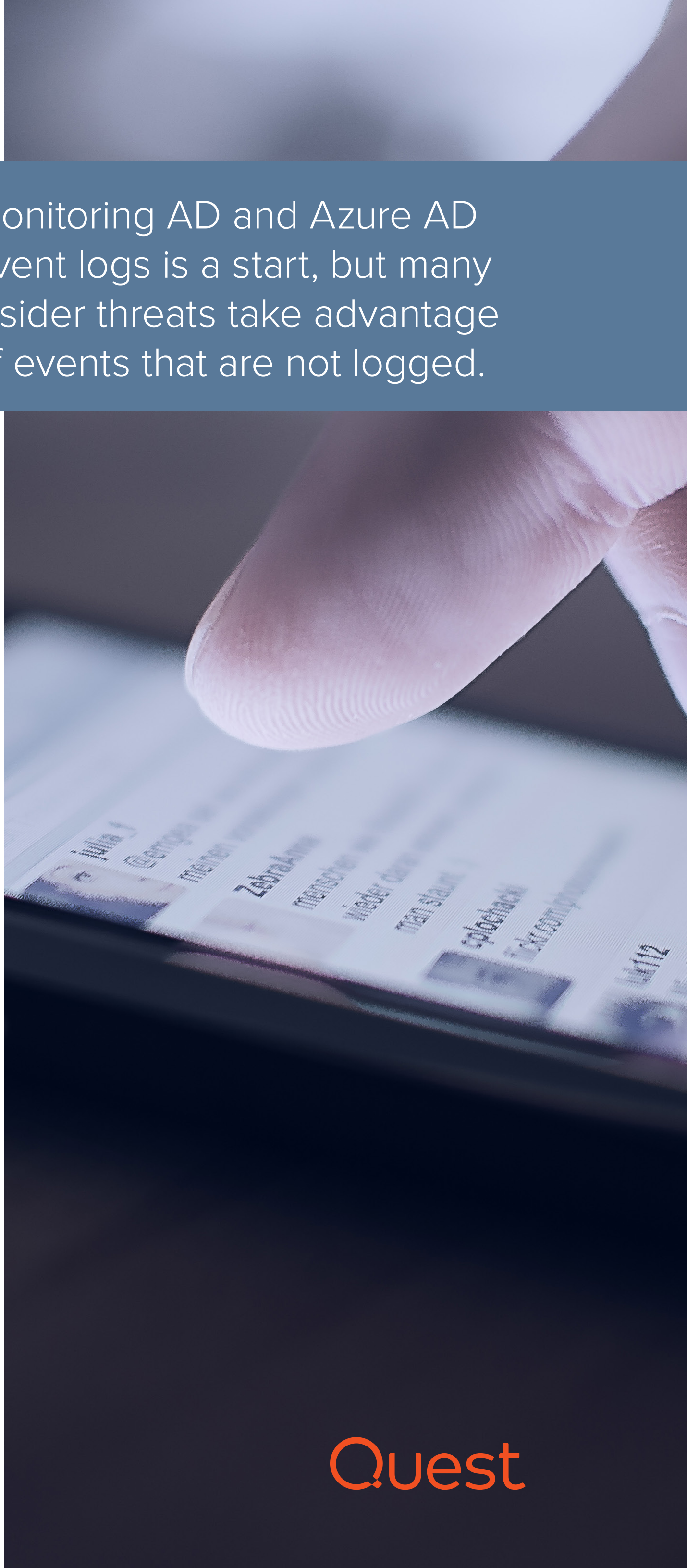
Traditional tools for security information and event management (SIEM) are bound by these limitations of native log auditing. For example, the native audit log indicates that a Group Policy Object (GPO) was modified, but does not record which settings were changed or their values before and after the change, so the SIEM solution cannot report those critical details.

LIMITATIONS OF PERMISSIONS MANAGEMENT

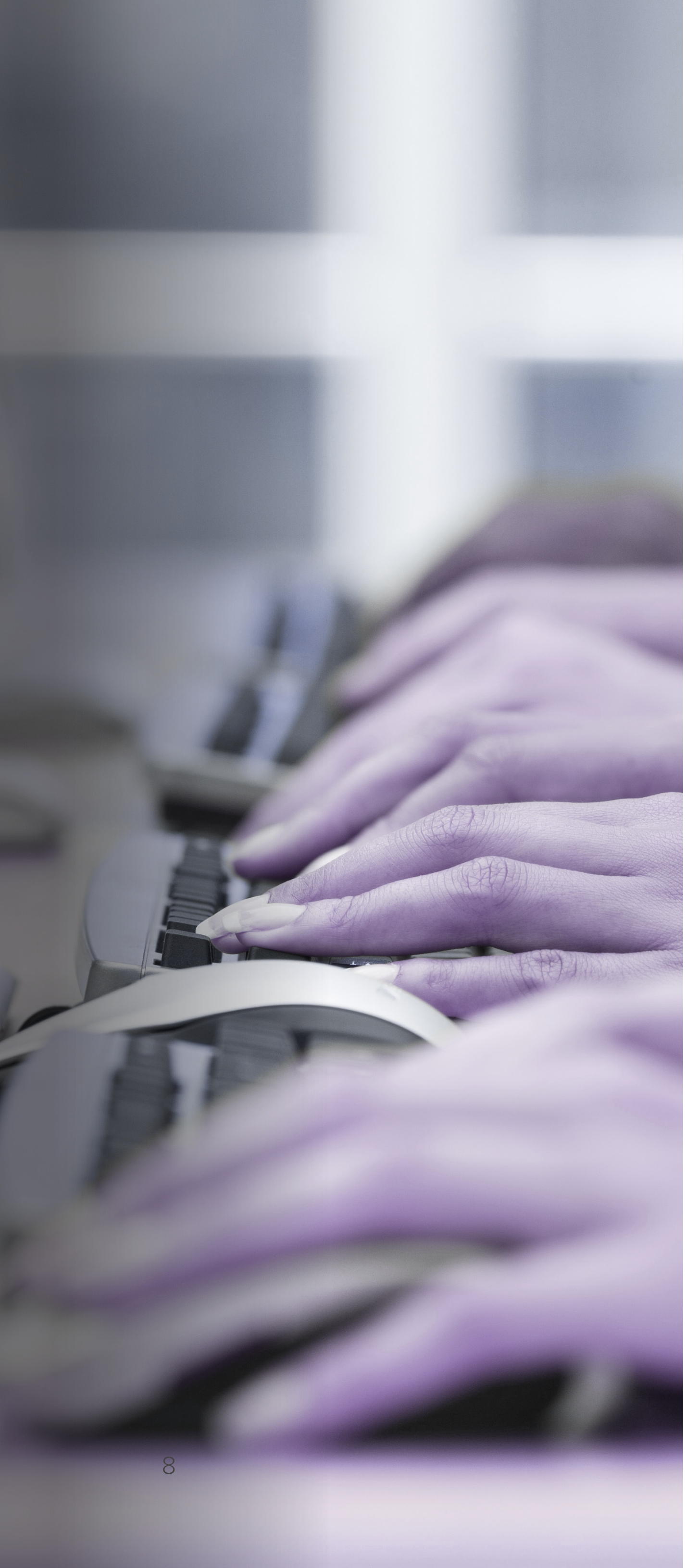
Securing AD and hybrid AD is an ongoing balancing act between granting users the rights they need to do their job and keeping them — even domain administrators — out of security groups that can access sensitive databases, folders and files containing sensitive data, such as Human Resources records, credit card information or health records.

But AD and Azure AD do not enable organizations to enforce a true least-privilege model, so users often have higher privileges and more access than they need to perform their jobs. For example, if an administrator wanted to delegate the ability in AD for help desk employee JSmith to move user objects from the Planning organizational unit (OU) to the Engineering OU, the admin would have to grant JSmith the right to delete any user object from the Planning OU and write to the Planning OU. That encompasses considerably more permissions than JSmith needed (and that the admin really wanted to grant) to execute the move and greatly increases the organization's exposure to risk.

Moreover, it's hard to enforce data fidelity and company naming standards in AD, which adds to the challenges of auditing assets and reviewing entitlements.



Monitoring AD and Azure AD event logs is a start, but many insider threats take advantage of events that are not logged.



LACK OF NATIVE AUTOMATION CAPABILITIES

Security demands that access controls be continually assessed and remediated, but AD and AAD do not provide any way to automate these processes. They offer only limited visibility into who has access to what, how they received the access, who has elevated permissions, and which objects and systems are vulnerable to security threats.

Similarly, preventing prolonged downtime and data loss in AD requires continual testing and revision of full disaster recovery processes, but AD does not natively provide an automated way to test and implement a full AD disaster recovery scenario across all domain controllers (DCs). And when unauthorized AD or Azure AD access or actions are detected, there is no way to automatically prevent or remediate them, and no way for stale credentials to self-clean.

> Security demands that access controls be continually assessed and remediated, but neither AD nor Azure AD provides any way to automate these processes.

Without built-in, automated change controls in AD and Azure AD, companies are subject to accidental and unauthorized access and costly outages.

HUMAN AND BUSINESS FACTORS

When employees transfer between business units, most organizations fail to properly update their permissions, so users retain all the permissions accumulated from previous roles, even rights they no longer need to do their jobs.

Plus, as a matter of business convenience and trust, it is common for employees, contractors and business partners to know and share one another's privileged AD credentials, which increases the risk of insider misuse, either accidental or malicious.

Watch an attack unfold

Consider this fictitious story describing how an insider threat caused by weak security controls can affect AD.

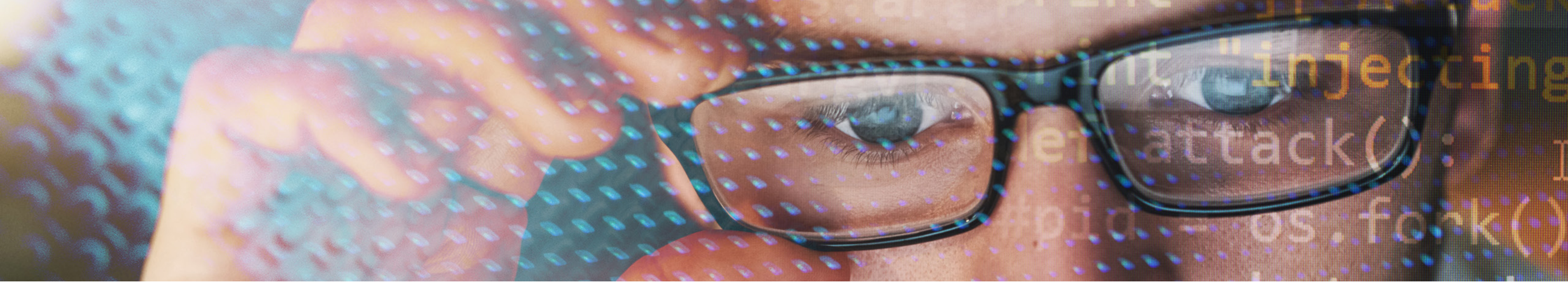
A medical products retailer named Acme just acquired one of its competitors, and now Acme's IT department needs to integrate the two companies' core systems together. Acme hires contractor JSmith under a four-week engagement to help consolidate Active Directory. The AD administrator at Acme adds JSmith to the Domain Admins group.

On Friday of JSmith's second week, Acme terminates the contract, but nobody tells IT to remove JSmith from the administrator group until the following Monday. This security process failure leaves JSmith with a full weekend to misuse his lingering elevated privileges, and he takes full advantage of it. Here's the play by play:

STEP 1. CREATING A BOGUS ACCOUNT

Unhappy that Acme terminated his contract prematurely, JSmith looks for ways to make up the income he had counted on earning. From a friend, he learns of a black-market site where he can make quick money selling credit card data — which Acme has in abundance.

JSmith logs in to Acme's network from home using his still-active administrator credentials and creates a new administrator account, in case Acme removes his original admin account or resets its password. To avoid attracting attention, he calls the new account corpsvcbk1, following Acme's naming convention for backup service accounts.



STEP 2. OBTAINING DOMAIN ADMIN PRIVILEGES

JSmith knows that Acme's generic monitoring system is configured to monitor direct changes to the Domain Admins group, so he can't add corpsvcbk1 to that group to get the privileges he needs to steal sensitive data. Instead, he adds corpsvcbk1 to a group that is a member of Domain Admin, which gives him the same privileges without raising alerts.

STEP 3. STEALING THE DATA

Using his new admin account, JSmith locates the SQL server (SQL1) where Acme stores credit card data. He modifies the GPO that prevents admins from logging on to certain databases and file servers, and then he logs on locally to SQL1. He adds his corpsvcbk1 account to the Local Administrator group on SQL1 and assigns it the system administrator role in SQL Server. Looking around, he finds the unencrypted credit card database and exports all of its records across the remote connection to his laptop.

Then he locates the file server (FSRV1) where Acme stores personally identifiable information (PII) and logs on locally to it. Again covering his tracks, he adds his admin account to a nested group that is a member of the built-in Administrators group on FSRV1. In the Accounts Receivable folder, he finds the file with PII. To access it, he adds his admin account to the Accounts Receivable group; that prevents his account from showing in the access control list, yet still gives him full rights to the file. He opens the file, ensures it's the one he wants and copies it to a mapped network drive on his laptop.

Common security policies and security controls are insufficient to prevent many insider attacks against Active Directory.

STEP 4. SETTING UP EAVESDROPPING

Next, JSmith modifies a Registry key that lowers LmCompatibilityLevel and session security enough for him to install malware that eavesdrops as SQL1 and FSRV1 pass credentials between them. That will enable him to decipher additional credentials in the future as admins authenticate; that way, even if Acme deletes his bogus corpsvcbk1 account, he can continue stealing more credit card data.

STEP 5. CLEANING UP

JSmith removes his corpsvcbk1 account from the admin groups, clears the logs to erase evidence of his attack and leaves the malware he planted in the network for future exploits.

Acme's security policies and security controls are insufficient to prevent this insider attack against Active Directory. JSmith's tactics ensure that it will take a long time for Acme to detect the data breach, by which time JSmith will likely have recovered his lost income and Acme will be in the throes of recovering from the data breach.

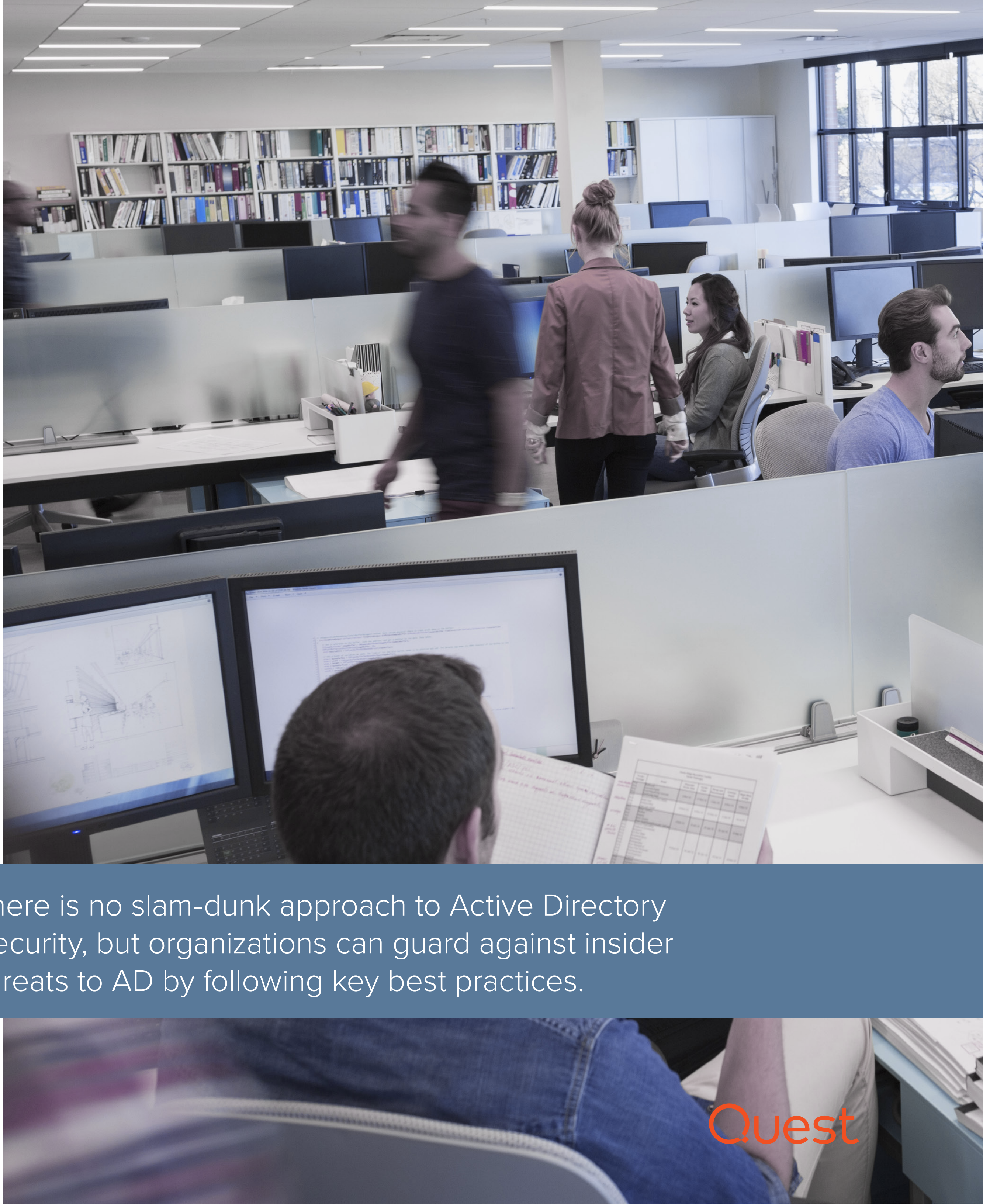
Best practices for AD security

There is no slam-dunk approach to Active Directory security, but organizations can guard against insider threats to AD by these key best practices:

1. REDUCE YOUR ATTACK SURFACE AREA

The first step in reducing risk is cleanup. Begin with the IT environment itself: Reduce the number of forests and domains. Identify and remove duplicate and other unnecessary groups. Remove unnecessary software installed on domain controllers and sensitive servers.

Then reduce the ways that environment could be misused or exploited. Limit permissions of all users — especially privileged users — in strict accordance with the least privilege principle. Be sure to set account expiration dates when creating accounts for temporary staff such as contractors, interns and visitors. Reduce delegation across organizational units, and prevent domain controllers from accessing the internet.



There is no slam-dunk approach to Active Directory security, but organizations can guard against insider threats to AD by following key best practices.

2. HARDEN ACCESS CONTROL TO SENSITIVE SYSTEMS AND CREDENTIALS

To further minimize the risk that your most valuable data can be compromised, require multi-factor authentication on sensitive systems, and ensure admins use jump boxes when connecting using privileged accounts and that they log on only to hardened workstations.

Manage your privileged accounts using a hardened password vault solution. And instead of granting anyone permanent admin access to sensitive servers, use temporary group membership with automatic start and end date/time.

3. KEEP A CLOSE EYE ON PRIVILEGED GROUP MEMBERSHIP

Once your house is in order, you need to monitor the actions of everyone it. Watching for privilege escalation should be at the top of your list. Monitor in real time not only direct changes to privileged groups (which can be tracked in native security logs), but also any additions of members to nested groups (which Windows servers do not log). Privileged groups to monitor include: Administrators, Print Operators, Network Configuration Operators, DHCP Admins, Backup Operators, Incoming Forest Trust Builders, Account Operators, Cert Publishers, Group Policy Creator Owners, Domain Admins, Domain Controllers, Enterprise Admins, Server Operators, RAS and IAS Servers, Schema Admins.

Even better, implement a solution that can prevent anyone from changing your most critical security groups.

4. ALERT ON SUSPICIOUS ACTIVITY

In addition to privilege escalation, you should also look out for other signs of attackers active in your environment. Be sure to alert on the following signs of abnormal or rogue access:

- Suspicious logons to sensitive servers after regular business hours
- Password changes made to VIP and sensitive accounts by third parties
- Successful logons after several failed attempts
- Direct assignment of administrative rights to any user
- Excessive or otherwise abnormal LDAP queries, which can be a sign of reconnaissance and information gathering
- Changes to GPO settings in AD (the before and after values of these settings cannot be tracked in native logs, presenting a backdoor threat to AD)
- Changes to the registry setting HKLM\SYSTEM\CurrentControlSet\Control\Lsa (this is a back-door tactic for lowering values used by the NTLM authentication protocol)

5. CONTINUALLY REVIEW ACCESS CONTROLS, THREATS AND VULNERABILITIES ACROSS AD AND WINDOWS SYSTEMS

Remember that security is not a one-time configuration event, but an ongoing process. You need to understand your AD permissions as they change over time. In particular, be sure to periodically review the membership of privileged groups in AD and across local sensitive systems; AD-based accounts running as services; and SQL Server database permissions and NTFS permissions on AD and SQL file servers. Also regularly report on inactive and disabled accounts, and clean them up before they can be exploited.

Last, but by no means least, frequently report on systems that don't have the latest Microsoft critical security patches and remediate this vulnerability.

6. AUTOMATE, ENFORCE AND REMEDIATE YOUR SECURITY POLICIES

When it comes to security, automation is your best friend. Supplement native tools with solutions that can automatically detect and prevent unauthorized intrusions to privileged and VIP groups and accounts, and that can prevent controls from being bypassed by enforcing rules-based access to sensitive resources.

> When it comes to security, automation is your best friend.

Also automate the remediation of issues. In particular, implement self-correcting policies that automatically remediate compliance gaps, and build rules that automate the reversion of unauthorized changes to sensitive users or groups.

Prevent unauthorized creation of accounts by defining a whitelist of authorized credentials permitted to perform this task. If someone who is not on the approved list creates a user account, the event should trigger an alert, and possibly even disable the creator's account, the created account or both.

Also prevent unauthorized changes to important enterprise groups and GPO settings by using a whitelist of authorized users. With a whitelist in place, even if insiders gain admin rights from compromised credentials, their attempts to change the membership of privileged groups like Domain Admins and Enterprise Admins will be denied. The whitelist also applies to making changes to sensitive GPO settings, such as disabling or denying logon to important servers and weakening NTLM authentication.

7. CENTRALIZE SECURITY INCIDENT INFORMATION FROM MULTIPLE DATA SOURCES

Improve your ability to quickly spot attacks and conduct thorough forensic analysis by collecting not just native logs but other critical audit information that is not logged there, and consolidating it to provide the contextual information about users, resources, time elapsed and entitlement information you need to investigate all stages of an event, from logon to logoff. Ideally, you want a 360-degree view of all related activities across users and resources.

8. PLAN, TEST AND IMPLEMENT YOUR AD BUSINESS CONTINUITY PROCESS

Back up your domain controllers, databases and other systems frequently, and store those backups securely.

Test your business continuity plan continuously, including all stages of your disaster recovery plan. Be sure to incorporate recovery into your security incident response process, and validate that your disaster recovery process meets your recovery time objectives following a disaster or breach.

9. AUTOMATE CLEANUP OF AD OBJECTS

Build rules that automatically detect objects in AD that violate policy and clean them up. For example, automatically detect user and computer accounts that have not logged in in 90 days, disable the accounts and move them to a disabled container, and then delete them in three days if they have not been claimed.

Implement an automated process for deprovisioning users that includes disabling or deleting accounts, removing accounts from all groups and distribution lists, removing remote VPN access, and automatically notifying HR, security and facilities management.

Conclusion

The insider threat to AD is real, pervasive and costly. A disgruntled or avaricious employee, especially one with an administrative account — or an attacker who compromises such an account — can exploit technical vulnerabilities and human factors to launch data breaches from the inside out.

Monitoring AD and Azure AD event logs is a start, but many insider threats take advantage of events that are not logged. Moreover, the list of things to look to look for in order to spot suspicious actions is long, and there is no native way to automate either detection or remediation.

The fact is, users need access to resources to do their jobs, and sometimes they need privileged access permissions. The key to AD security is balancing the need to streamline user access to maximize productivity against the need to protect sensitive data and systems from both accidental and deliberate privilege abuse. By following the Active Directory best practices outlined here, you can improve security and minimize the insider threat.

Securing AD requires balancing the need to streamline user access to maximize productivity against the need to protect data and systems from accidental and deliberate privilege abuse.

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.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners.