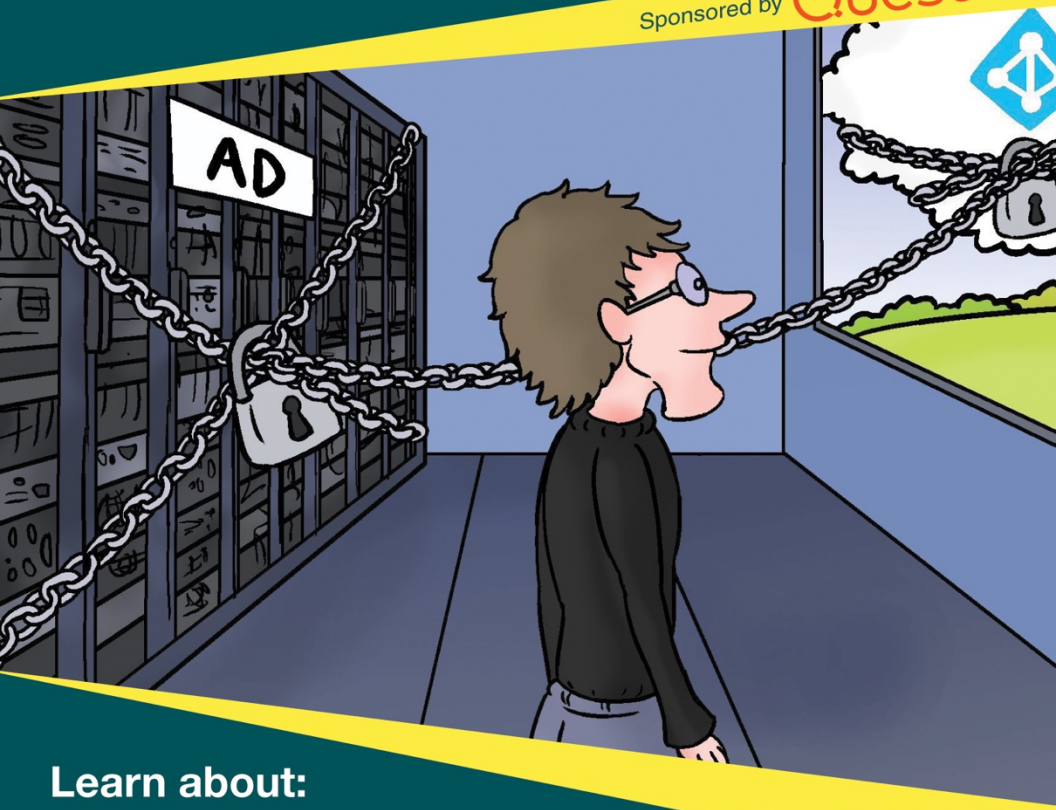
Conversational Hybrid Active Directory Security

A ConversationalGeek® Book

Sponsored by Quest



Learn about:

- Why on-prem AD security matters – even when you move to Office 365 and Azure AD
- The 4 questions you should be able to answer in a truly secure hybrid AD
- How to get started using native tools on-prem, in Azure AD, and in Office 365

2nd Edition

By Nick Cavalancia (Microsoft MVP and Co-Founder of Conversational Geek)

Sponsored by Quest®

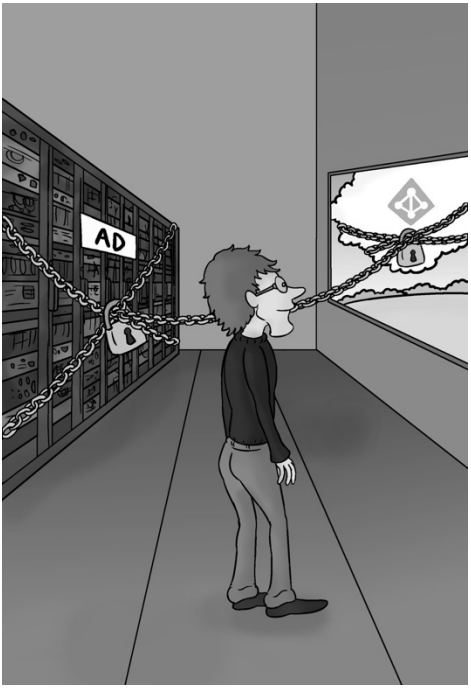
Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 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.

Quest

For more information, visit www.quest.com

Conversational Hybrid AD Security

By Nick Cavalancia



ConversationalGeek®

Conversational Hybrid AD Security

Published by Conversational Geek Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Nick Cavalancia
Project Editor:	J. Peter Bruzzese
Copy Editor:	John Rugh
Content Reviewer:	Karla Reina

Note from the Author

Active Directory has come a long way. When it was first introduced in 2000, the very idea of a security was limited to the simple (but, then, effective) mantra of "AGLP". Accounts were put into Global Groups, Global Groups into Local Groups, and Local Groups given permissions.

But, with the advent of interconnectivity via the Internet, both Active Directory and the security necessary to protect it have moved from being on-premises only, and have made the leap beyond the walls of the organization and created an AD environment that both exists on-premises *and* up in the cloud.

This means you're going to need to adjust your focus and methods by which you protect your hybrid AD instance, all the while realizing that – at the same time – there's nothing really new under the sun.

- Nick Cavalancia

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

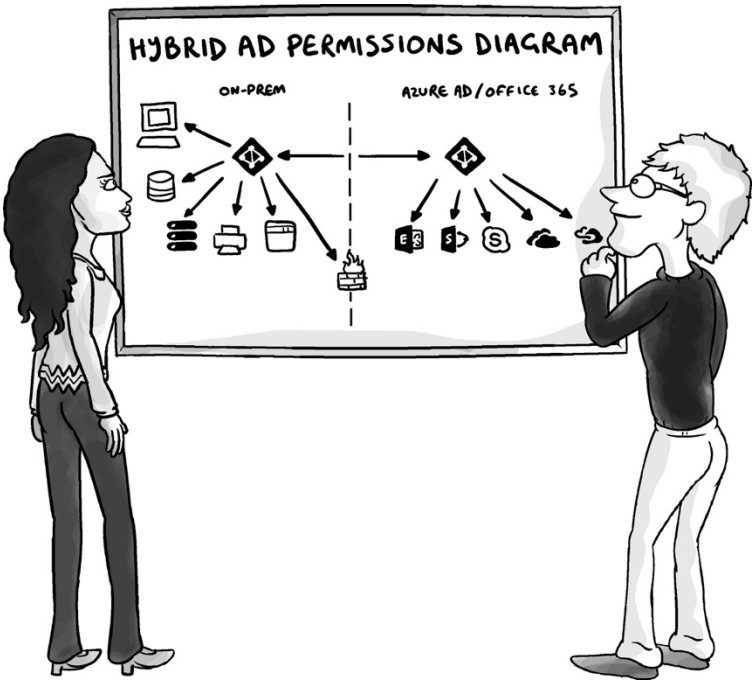
These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Within these boxes I can share just about anything on the subject at hand. Read ’em!

Why Worry About Hybrid AD Security?



Unless you've been hiding under a rock, it's going to come as no surprise that the adoption of Office 365 is happening at a rapid pace. With primary drivers like Exchange Online, OneDrive for Business and Skype for Business, Office 365 is obtaining an average of around 1 million new subscribers each month.

What's this got to do with Hybrid AD security?

Plenty.

Under the hood of this robust online offering lies an equally impressive directory service – *Azure AD.* Used by all Office 365 apps to authenticate users, Azure AD (AAD) serves as the central nervous system that makes Office 365 possible.

Unbeknownst to those using it, every Office 365 instance requires a separate AAD tenant, creating the need to manage *yet another* environment IT is responsible for. To address this, over 75% of customers with more than 500 employees using Office 365 are also syncing their on-premises AD to Azure AD to allow for single authentication – thus creating a Hybrid AD environment.

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-prem credentials. Because it's a one-way sync to AAD, it's important to remember that your on-prem AD environment *dictates* the contents of AAD.

Because of this, your on-prem AD becomes the focal point for governing access controls, creating security compensations controls, and determining how access is granted in AAD and associated applications.

Even so, you might wonder why bother worrying about AAD when AD is already a large enough target. Over 500 million on-prem AD accounts exist today, representing 90% of companies around the world representing that are reliant upon AD daily.

According to the 2018 *Verizon Data Breach Investigations Report*, the use of stolen credentials was the #1 threat action in data breaches, making AD a prime target.

But AAD's numbers are even more impressive and a cause for concern:

- 240 million AAD user accounts in existence
- 2.9 million organizations using AAD

- 10 billion authentications weekly

With over 10 million cyber-attacks hitting the entirety of the Microsoft cloud infrastructure (including Office 365, Xbox, MS Live, etc.), the conclusion is clear:

Any access gained through on-premises AD can have repercussions not just within AAD, but also reach well into any web-based applications leveraging AAD. Therefore, *you need to be putting security controls in place within your on-premises AD to be reflected in your AAD instance, keeping the whole of your hybrid AD secure.*

Now, this won't be without challenges. To properly secure your Hybrid AD, you're going to need to be able to discern:

- What *can* they do? – ideally, you need to be able to tell which users have permissions to external apps and data, or even who has rights to, say, manage passwords across all of AD.
- What *are* they doing? – In many cases, there is either not enough detail or no audit trail at all to provide a clear indicator of what was specifically changed in a given application or within AD itself.
- Is privileged access inappropriate? – When IT accesses data they shouldn't be accessing, who is watching the watchers? Groups used for on-prem access to resources could also be giving access to cloud resources.
- Will changes affect business continuity? – A simple erroneous change within your on-prem AD will propagate across all of AD and into AAD, making it difficult to recover (e.g. forest schema corruption).

To address these challenges and help you implement proper hybrid AD security, you'll need to start at the source – *your on-premises AD* and put security controls in place that don't just make AD more secure, but also AAD and the data, applications, and systems relying on AAD.

So, how do you secure the entirety of your Hybrid AD?

I'll use the four questions above as a framework throughout the remainder of this book to allow us to dig deeper and deeper into what's needed to make your Hybrid AD more secure.

The first place to start is with an understanding of the current state of your AD environment, and user's abilities within it.

What Can They Do?

Today's security isn't just about whether it is configured correctly; it's about proactively having a secure stance in the face of both cyber-attackers seeking to take over a user's credentials and insiders misusing privileges for their own gain. To assess the potential risk that exists, you need to have an understanding of your organization's current security configuration – that is, get a definition of what "they" can do in your environment.

Now, who is this "they"? Is it just privileged IT users? Application or line of business owners? Low-level users? Who should you be concerning yourself with as you look to assess the current state of security?

If you follow the *Data Breach Investigation Reports* Verizon puts out each year, you'll know that for all privilege misuse incidents (which can be performed by either a cyber-attacker using commandeered credentials, or by an insider themselves),

the breakdown of roles responsible within the organization looks like the following[1]:

14%	Executives and Management
14%	Privileged Users (IT & elevated users)
72%	Regular Users

While it's evident from this data that "they" is *pretty much everyone*, this more so makes the point that you need to be focusing on the permissions assigned and not so much on roles.

To put it another way, focus on the *Do* in "What can they do?" and not the *They*.

So, are we just talking about permissions within AD (and, therefore, AAD)?

In short, *no*.

Your Hybrid AD serves as the foundation for access to applications, systems, and data both on-premises and within Azure (read: Office 365 applications and Azure applications). For example, a lower-level user in Finance could be in charge of the department's SharePoint Online site, where they store sensitive financial reports and data. If that account was compromised, an attacker could potentially gain access to information the organization most definitely wouldn't want to get out. That's why you want (as much as is possible) to know what permissions are assigned to your AD users and groups.

So, in general, you need to be focused on anyone with a set of elevated privileges – that begins in AD with users that are members of groups like Domain Admins, but also those with

---

[1] Verizon, *Data Breach Investigations Report* (2016)

permissions to reset passwords, manage group memberships, etc. Then you need to go well beyond AD and consider any and all applications utilizing AD users and groups to assign permissions, identifying those users with elevated privileges in each application. Lastly, consider looking outside AD/AAD to Azure itself to understand what security is in place that could be used maliciously to gain access to, say, a virtual DC hosted in Azure.

The challenge is, of course, none of the external permissions assigned to a given AD object are stored with the object itself. In essence, you need to look to the application or system in question and see how its' security is configured. And, given the ginormous number of systems you have, that's a daunting task. At a minimum, you have permissions within AD itself, File Shares, NTFS file systems, SQL Server databases, Exchange/EOL, SharePoint/SPOL, databases, and proprietary applications. And then there's everything else within Office 365, as well as any other Azure-integrated applications.

In a perfect world, this needs to be documented (and, if it were up to me, I'd want a *Permissions Assigned* tab be added to objects in AD and any system that selects a given object adds an entry to the list so you'd have a central place to see anywhere an object has permissions). There are, of course, ways to do this manually via any built-in reporting within a given application's management console and, in the case of Microsoft applications, there's always PowerShell.

In some cases, such as AD or Exchange Mailboxes, it's a relatively simple task using a single cmdlet (e.g. AD's *Get-Acl* and Exchange's *Get-MailboxPermission* cmdlets). Venturing out to other Microsoft applications and services (whether on-prem or within Office 365/Azure) will require some relatively more robust scripting – more than can be covered here.

Do keep in mind PowerShell cmdlets are generally application object-centric. That is, you're not asking "Show me everywhere Bob has permissions." Instead, you're asking "Who has rights to this specific object?" so you'll need to look for ways to first have PowerShell enumerate all the objects (e.g. folders in a file system, mailboxes in Exchange, etc.) and then pull permissions.

Third-party solutions do exist to report on the current state of permissions – usually per-application – providing centralized intelligent reporting that reduces the amount of time you'll spend on this kind of task, while improving the accuracy and completeness of the resulting data.

And then there's everything else that may integrate with AD – non-Microsoft or homegrown applications, as well as SaaS-based apps outside of Azure, etc. You'll need to look for built-in reporting to determine what assignments have been made.

Regardless of how you choose to determine what permissions every user has within your organization, the likely problem is you'll be looking at the permissions at only a point in time. Reporting on the current state won't show you that someone was given full rights to Finance's SharePoint Online site for 3 days and then removed. You only see the permissions as they are today, where that person does not have permissions. You're missing some context around the true nature of your Hybrid AD security.

This is why you need to be concerned with the actions taken by your users.

What Are They Doing?

Since it's far more likely you don't have a grasp on what permissions are assigned to your users and groups, having visibility into actions taken is the next best thing. If you can see a user *exercise* a permission they've been granted, you can conclude a minimal set of privileges assigned to them.

In addition, part of securing your Hybrid AD revolves around auditing all actions taken on systems that either contain, or provide access to, sensitive or valuable data.

In general, your response is to audit actions such as:

- Permission changes in AD
- Group membership changes in AD
- File Server access and permission changes
- SQL Server Database access and permission changes
- Exchange permission changes
- Non-Owner mailbox access in Exchange
- SharePoint access and permission changes

Depending on whether an application generates an audit trail and whether you're using native or third-party tools, this list can and should be much longer. Admittedly, this goes well outside of the context of AD. But I think it's important to have a grasp of what's going on within your organization so you can see when permissions (that stem from access granted via AD) are being exercised so that you can go back to AD and make changes as needed to tighten up security.

That's going to generate a lot of data. What should you specifically look for?

There's no single right answer to what specifically you need to be watching in your organization.

In general, you're looking for anything that falls either outside your security policy or outside the norm. For example, your security policies may dictate any changes made to the Enterprise Admins group require authorization. So, auditing for changes to that group makes sense as a precautionary measure. Users accessing particularly sensitive data on a file server could also be audited to detect when an abnormal number of files are read. This could be an indicator of someone copying and entire folder's contents to a USB drive.

Neither external attacks, nor insider threats are going to wait for you to begin taking advantage of audit log data; the time to begin is now.

So, where should you start your auditing?

Microsoft does provide you with a wide range of tools – some old and some new – to get you started.

Auditing AD with Native Tools

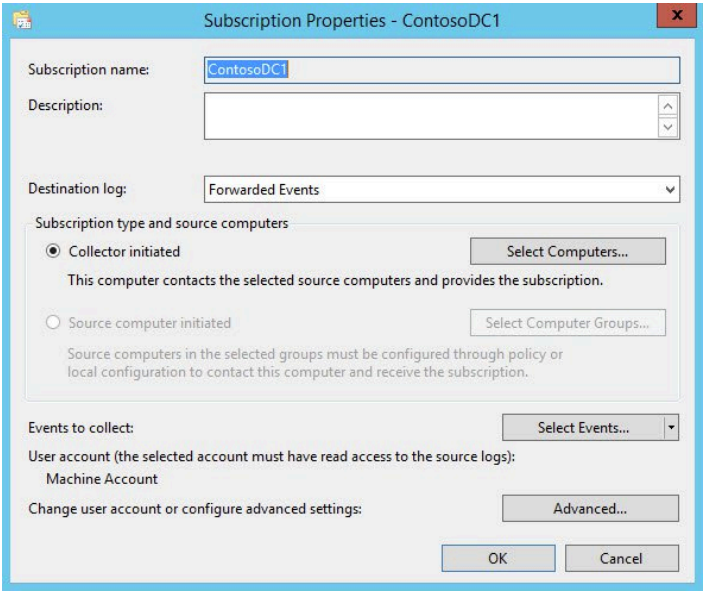
I'm going to make the assumption you've used Event Viewer before and, at very least, have the basics down regarding the types of logs available to you. So, I want to instead focus on how to centralize your log data and how to proactively get the most out of the Event Viewer tool.

Centralized Auditing with Event Subscriptions

Since your security focus is on a user and their activities, ultimately, you want to be able to make a request like "show me everything Bob did yesterday." While it doesn't look like Event Viewer will be doing that anytime soon, you can get yourself a bit closer using *Event Subscriptions*. If you haven't used these before, they allow you to setup events to be forwarded to a central computer (presumably a server). By centralizing log data, you'll be a step closer to having the "everything" part of the Bob query in one place to review.

Because I want to focus on how to get the most out of your auditing, you can read a great article on how to set this up at ***bit.ly/EventLogSubs***. It's a relatively short set of simple steps.

Once configured, you can create a subscription on the collector computer, where you can select which computers the data will be pulled in from and even which events you'd like pulled in, as shown below. This is useful if you're only auditing a specific application or system.



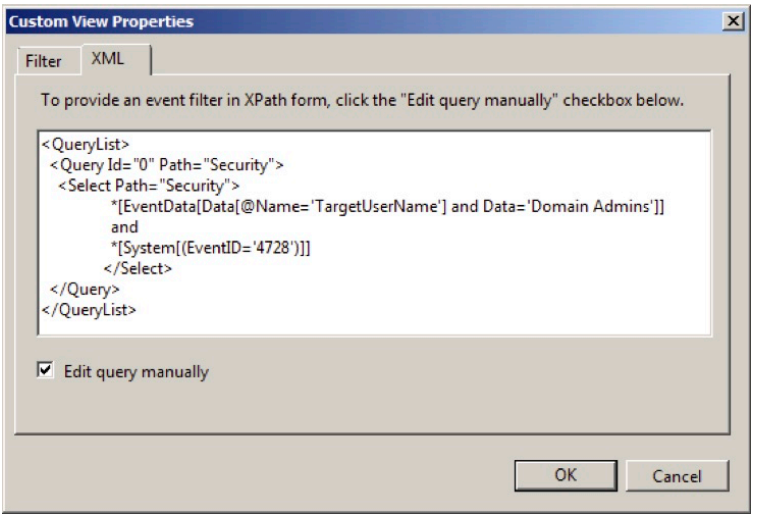
Please note that this isn't intended on replacing event log management or SIEM solutions; after all, eventually all the event log data you collect is going to take up a ton of storage and the queries in Event Viewer will slow to a snail's pace. This tech is simply a way for those of you that need to get started now and have a number of computers hosting logs to be able to look at all your data in one place.

The next step is to find ways to make finding the answer you need much faster than manually running filters.

Speed up Searches with XML Filtering

There's a two-fold problem with the default searching and filtering in Event Viewer. First off, it may take you some time to build just the right query, and secondly, the GUI-based filtering doesn't take advantage of all the data found in an event entry.

The most productive way to filter log data is to proactively build your own XML-based custom view. You can start with providing all the needed detail on the Filters tab, but then switch over to the XML tab (shown below) to augment the XML query.



For example, the XML filter above was built to specifically show any changes made to the Domain Admins group.

XML Filters allow you to take advantage of every piece of event metadata (which you can view by looking at the properties of a given event and selecting the XML tab), along with boolean operators (you know – *and* and *or* statements) to create as complex a filter as you need. Want to know what three specific

users did yesterday, or need to put events from multiple logs into a single view? XML Filters can do this and much more.

The limitation here is, while XML filters does get you much closer to asking the real auditing questions you want like "Who accessed the CEO's mailbox yesterday?" (because that XML filter *can* be built), it still doesn't provide you with the ease of use found in third-party solutions. Also, at the end of the day, you're still left looking at raw event log data – there's no intelligence or insight there; just information.

Auditing via PowerShell

I'd be remiss if I didn't at least cover this, even if in brief. The *get-eventlog* cmdlet serves as a powerful foundation for auditing. For example:

```
$a = get-eventlog -logname Security|where {$_.eventID -eq 4728}
$a | format-list -property *
```

Whether you're simply pulling the data from a single event, as shown in the code above, or using PowerShell to pull from multiple data sources, and then filter, manipulate, and present the data via complex coding, it's a viable option for those of you that want to do this yourself.

Auditing Azure AD

You can access audit data using the *Azure Portal* where activities are broken down into the following categories:

- Users and groups
- Applications
- Roles
- Devices
- B2B
- Administrative Unit
- Directory
- Policy

For each category, you can run pre-defined reports whose results can be honed down using a somewhat small set of filters. With nearly 100 reports, this tool provides a lot of value.

You can see a full list of the built-in AAD auditing reports found inside the Azure Portal at bit.ly/AADAuditEvents

The built-in reports definitely cover a larger majority of your auditing needs. But should your audit turn into more of an investigation, where the answer to one query becomes the question for the next, you may find the built-in reports limiting.

Auditing Office 365

Ok, this one's a bit more complex. Unlike the previous two sections, where there was by and large a single tool to use, auditing Office 365 is a bit all over the place. With data in multiple locations, varying delays before audit data is available, and the need to use multiple consoles, auditing Office 365 will take a bit of work.

To start, you need to enable audit logging in the first place. This is done within the Office 365 Security & Compliance Center. You'll also need to separately enable mailbox logging for each mailbox if you want to see this kind of activity logged. By doing this you gain access to a wide variety of activity:

Admin Activity in

- Azure AD (O365-related)
- SharePoint Online
- Exchange Online

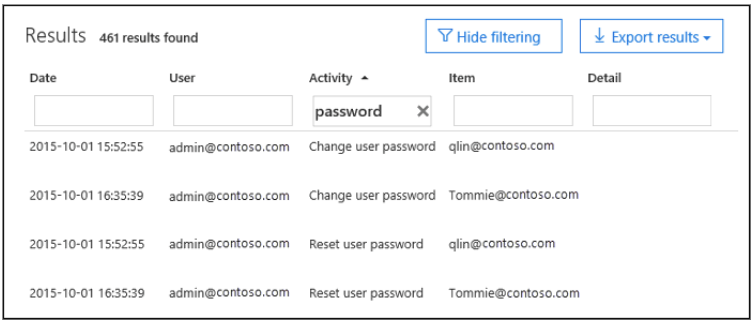
User Activity in

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Sway
- Power BI
- Yammer

Auditing in the Security & Compliance Center

Microsoft has centralized access to all this data within the *Audit Log Search* function of the Office 365 Security & Compliance Portal. The *Audit Log Search* feels a lot like a simplified web-based Event Viewer but with the benefit of having over 100 pre-defined activities (a complete list is available at bit.ly/O365AuditActivities) to speed up the process of finding just the right log entries.

Results can be filtered (shown below) using simple text-based values. Within the context of Office 365, this gets you fully to "What did Bob do yesterday"-type questions, as you can put in the user's name and yesterday's date in the filter and have your answer.



Results can be exported to a CSV file, with options to only export the first 1000 loaded results as they appear in the console, or all results, which includes additional detail for each log entry.

Auditing Using PowerShell

Office 365 makes all of this same information available via PowerShell. It's a detailed process to initially configure – one too long to fit in this book (so lengthy, in fact, it could be a book of its own!). In short, you'll need to enable auditing, establish a PowerShell session with Office 365 using the *New-*

PSSession cmdlet, and use the *Search-UnifiedAuditLog* cmdlet to retrieve the desired data.

Can You Really Tell What Are They Doing?

The goal here is to have visibility into the access and changes being made to both AD and applications that leverage AD. You've obviously got a wide range of tools to choose from, but there are some downsides. There's the obvious on-prem vs the cloud division that exists with the data itself; no single console provides you an ability to look at both on-prem AD and all the AAD/Office 365 data in one place. Which bring me to the second issue which needs no explanation – multiple consoles (yuck!). And lastly, the built-in tools are solid for the basic questions when the answer can be determined from filtering a few fields.

Built-in tools are great when you have a limited set of queries to run and are expecting a raw events for each for you to parse through. But when you need intelligence, centralized access to all data sources, and an interface designed with both in mind, you may need to look at third-party tools.

Lastly, there's a discussion that needs to be had around whether raw filtered data will give you the answer you need, or whether you need to corroborate data from more than one log to see a series of activities in order to gain some level of context around whether a user's actions are well-intended, suspicious, or downright criminal.

Is Access Inappropriate?

It's often a tough call. If someone in IT accessed the CEO's mailbox in Exchange Online, is it inappropriate? Were they asked to as part of a support call to undelete a message, or are they just snooping around? Same goes for a scenario where the CEO's password gets reset. You see, the action on its own doesn't necessarily tell the story.

To determine whether access is business-related or not, you need to have some level of policy that dictates what is out of the normal scope for any user with elevated privileges. Just about all of the actions I listed at the beginning of the *What Are They Doing?* Section apply here, but probably with a bit more specificity around which user accounts, mailboxes, NTFS folders, files, etc. are generally off limits.

And it's not just IT that need to be watched. Certainly, you need someone "watching the watchers," but just about any user with access to sensitive information should be included. The reason is there is a lot of concern today about users being *over-privileged* – access granted through group memberships of groups that haven't been properly vetted in years. If you can't say you're reviewed to a group's membership, evaluated all the access granted, and attested to a group's existence in quite a while, you may have users with way too many permissions.

Over-privilege is more rampant than you think. According to the Ponemon study, *Corporate Data: A Protected Asset or a Ticking Time Bomb?*, 71% of users have access to resources they should not be able to see!

You won't know if an action is inappropriate or not just by looking at it, so the focus here should be more on defining those critical data sets and parts of AD that should be doubly under review and ensure there is some level of notification configured.

Event Viewer has the ability to send emails using the Basic Task Wizard. PowerShell has the *Send-MailMessage* cmdlet. And

Office 365 has Activity Alerts in the Security & Compliance Center. We're talking about ensuring AD and the resulting access it provides is secure here, so be certain you have some level of alerting configured so IT isn't finding out about inappropriate access days, weeks, or months too late.

When notified about a suspect change, it's critical to understand the root cause – for example, when the CEO's password was changed, it's not just a question of who made the change; the story may go deeper should you find out the person who changed the password normally doesn't have permissions to do so. You then need to find out who gave that person permissions, and so on.

When investigating changes, you should be gathering needed context around that change, including what, specifically, was changed and how many users, domains, applications, etc. are impacted. This may, like the CEO example, become a chain of investigations – all to uncover the full scope of what changes were made, who did them, how permissions were attained, and how many people were involved.

Inappropriate access may just be an issue of someone seeing information they shouldn't. But, in some cases, you need to be worried about changes that have a much greater impact – one that can take the business down, even if for a short period of time.

Will Changes Affect Business Continuity?

Some changes can be indicative of a breach, making the current state of AD no longer trustworthy. For example, take an external threat actor gained access to your network via a malware attack and utilized the compromised user's AD permissions to grant himself significant access throughout AD. In this instance, you'd need to be able to recover AD in the same way you think about recovering from any other disaster to ensure business continuity.

The kinds of changes that require focus from a BC perspective both inside AD and out are:

- Mass or significant changes to AD groups or permissions
- Changes to AD topographic settings (e.g. Sites, Subnets, DNS, etc.)
- Evidence of data manipulation

At a minimum, have frequent enough backups of AD and critical data sets that meet recovery time and recovery point objectives (that is, the amount of time you can take to recover and how old can the backup be, respectively) in a breach scenario.

In a perfect world, having a wide and deep ability to recover any part of AD, including features like recovery testing and automated recovery would make your response far more exact and timely. This kind of advanced functionality can be found in third-party solutions.

The Big Takeaways

The shift to syncing your on-prem AD with the cloud extends the risk of inappropriate access to data and applications well beyond the extent of IT's visibility and, often times, administrative reach. The good news is everything starts with your on-prem AD and extends out from there.

By putting controls in place around your on-prem AD, you create a security layer around AD, AAD, Office 365, and your web applications. The 4 questions covered in this book provide you with perspective around how to best get a grasp of what's changing both in AD and the applications it impacts, how those changes affect your organization, and ensuring you're ready to react when they happen.

Vendor Sponsor Chapter: Quest

"How'd you figure that out so quickly?"

It's evident from the native tools Microsoft provides that they believe securing AD, AAD, and Office 365 is rather important. But it's also not their primary business, which usually translates to the tools they provide being adequate for the occasional or "less than in-depth" need, but not necessarily for situations where one needs to investigate suspect activity that may transcend multiple users, applications, actions, and weeks or months of time.

It's important to recognize that in your time of need, you will want to be able to have not just an ability to ask the auditing "question", as it were, and get back a set of matching events. You're going to want to obtain an intelligent answer in a timely fashion, and be able to use that answer as the basis for digging deeper, should it be necessary.

Quest has built a number of solutions using a security methodology that enables you to improve your security posture by taking control of your on-premises AD and extending those safeguards to the cloud. This methodology rests on 4 key pillars for hybrid AD security. The pillars are:

- Continually Assess
- Detect & Alert
- Remediate & Mitigate
- Investigate & Recover

Continually Assess

Your need to have a handle on the state of your security isn't something to focus on once a year with an audit; it's an ongoing, ever-present part of AD security that requires up-to-the-minute visibility. Continually assessing the state of your AD security and the applications that rely on it is necessary to have a current understanding of how security is configured, and who has access to what.

Quest Enterprise Reporter provides visibility into both the current state, as well as historic changes made to permissions, privileged users, and sensitive groups within AD, Azure AD and many critical enterprise applications. Automating the task of discovering, reporting, and auditing, Enterprise Reporter simplifies the work of ensuring security and compliance with your security policies.

Detect & Alert

While continual assessments assist in gaining an understanding of the state of security, organizations still require the ability to more rapidly respond to immediate threats. IT teams are spending too much time chasing false positives while sifting through heaps of audit reports and raw data to find legitimate

alerts. IT needs the ability to audit changes in real-time and proactively detect threats based on user behavior patterns.

Quest Change Auditor monitors and detects changes made at OS and application level in AD, Azure AD and your critical enterprise applications. This is different from Enterprise Reporter in that Change Auditor is actively watching the applications and systems for changes, whereas Enterprise Reporter collects the current configuration and compares it with a prior version. Change Auditor notifies IT in real time to changes made, minimizing the impact of an inappropriate configuration.

Quest Change Auditor Threat Detection models individual user behavior patterns to detect anomalous activity that might indicate suspicious users or compromised accounts. Using user and entity behavior analytics (UEBA) and sophisticated scoring algorithms, Change Auditor Threat Detection ranks the users presenting the highest risk in your organization, identifying potential user threats and reducing the noise of false positive alerts.

Quest InTrust is an event log management (ELM) solution that consolidates log data from a myriad of sources, looking for changes found in the log data, and alerting IT when specific events are found. The benefit of InTrust is an ability to consolidate not just AD data, but also logs from other sources that can be used to provide further context around suspect events.

Remediate & Mitigate

Inappropriate actions don't always require a response equal to that of trying to stop threat activity. In many cases, over-privilege can simply be the culprit, where a number of responses can be appropriate. This can include automated prevention (where changes are automatically rolled back),

automated responses (think along the lines of scripts used to perform tasks like disabling an account, etc.), or empowering IT to use activity data to create a Least Privilege environment based on actual use rather than just taking away elevated privileges. Whether in a case of over-privilege, insider misuse, or external threat, the ability to proactively have a response lying in wait is critical.

Quest Change Auditor uses policy-based preventative measures when specifically monitoring changes in AD to stop attempted changes to your AD's most critical objects, which creates a watchful layer of security around your AD security, keeping it in check.

Quest GPOADmin provides a version control system and least privilege access capabilities for your Group Policy objects. In the event of an unwanted change, you can quickly roll back to a previous version.

Quest InTrust provides policy-based actions to respond to actions. Defined in advance, InTrust can perform multiple tasks to both mitigate the threat and inform IT. For example, if someone was to enable the Guest account, InTrust could be configured to automatically disable Guest, disable the person that tried to enable it, and notify the security team.

Quest Active Roles creates a least privilege AD environment, where every change is made via a portal (rather than to AD directly), acting as a proxy. This allows restriction of visibility (so privileged users can't see objects they can't manage), limited administrative functionality (only allowed actions are available), and the use of workflow for approvals and accountability to be added to the process of managing AD.

Investigate & Recover

When a security incident occurs, the ability to reduce response time is critical. Having a context-rich 360° view of the

configuration and changes made to your entire Hybrid AD environment (including the applications it touches) will help to speed up root cause analysis and remediation.

In cases where a security incident impacts the organization's operating ability, it's often a bigger issue than just recovering AD or Azure AD. Recovery testing may be necessary to ensure an older version of AD won't impact other applications. And, in the worst of AD disasters, the need to recover entire forests may require automated recover to make certain the environment is recovered based on the application and system dependencies.

Quest Recovery Manager solutions provide deep backup and disaster recovery functionality down to an attribute level for on-premise and Azure AD, and recovery solutions for email both on-premise and Office 365.

Quest IT Security Search gives those investigating suspect activities a view into data from Change Auditor, Enterprise Reporter, Recovery Manager, and InTrust, providing comprehensive visibility into your environment's configuration and changes across AD and all your most critical applications. This correlation of data using an interactive search engine allows for quick incident response and forensic analysis.

Four Pillars, One Objective

Your IT organization strives daily to make the network environment more secure. And as you extend the environment out into the cloud, you lose visibility and control, which puts the entire environment at risk.

Quest solutions provide a layered approach to security, covering the areas of continual assessment, detection and alerting, remediation and mitigation, and investigation and recovery – all working together to put you completely in control of your security, no matter where it is.

Easily "converse" about Hybrid Active Directory Security in any setting.

As organizations leverage Azure AD and Office 365, the adoption of a hybrid Active Directory is quickly becoming the norm. This book covers the high-level best practices necessary to continually ensure your on-prem – and, therefore, your AAD or Office 365 – AD instances are all secure.

About Nick Cavalancia

Nick Cavalancia is self-proclaimed "techvangelist" and is a 20+ year IT veteran who regularly speaks and writes for some of today's more recognizable companies.
Follow Nick on Twitter @nickcavalancia and @techvangelism.

ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.