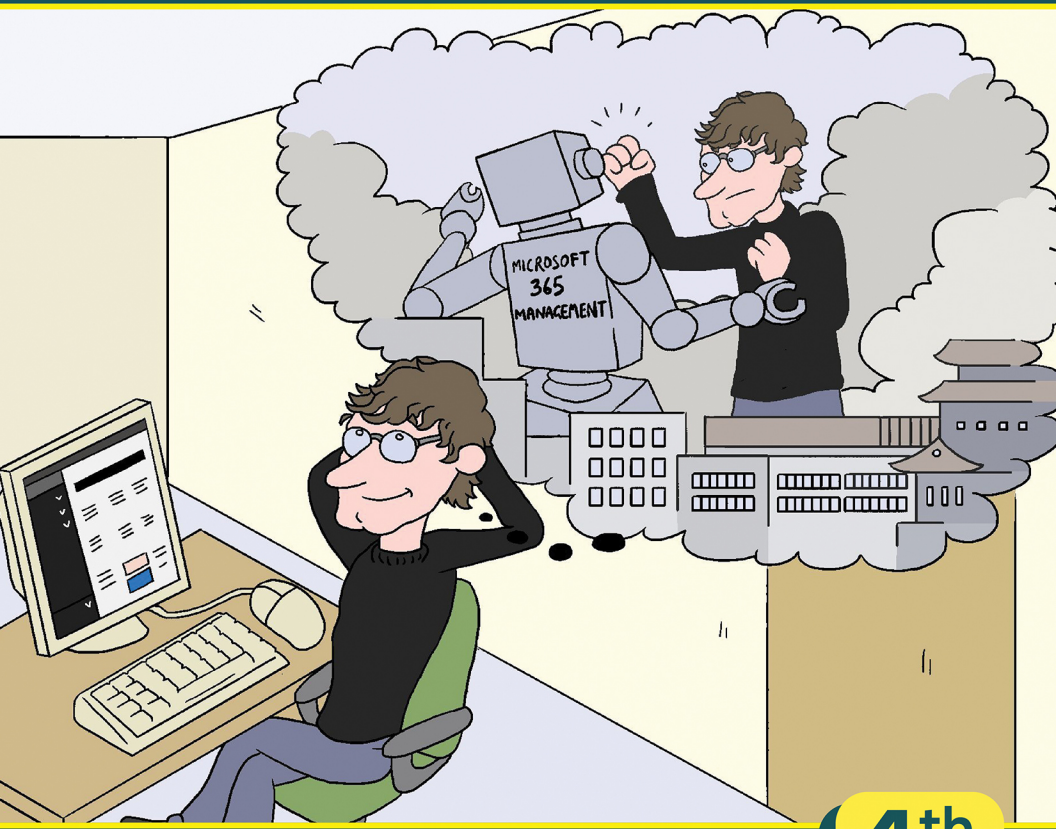
ConversationalGeek®

Conversational Microsoft 365 Management

By Heather Severino (Microsoft Office Apps and Services MVP)



4th Edition

In this book, you will learn:

- Licensing and management challenges of Microsoft 365
- The gaps in native M365 administrative tools to handle license management, RBAC, compliance and more
- The value of a Microsoft 365 Management Platform to plug those gaps

Sponsored by
CoreView

Sponsored by CoreView

CoreView is the Global Leader in Effortless Microsoft 365 Security, Governance, and Administration. CoreView's end-to-end solution stretches across the whole M365 ecosystem – from your tenant-level configurations, right up to your most critical workloads.

Created by M365 experts, for M365 experts, CoreView makes best practice for M365 effortless by simplifying, unifying, and enhancing the M365 admin experience. CoreView empowers 1,500 organizations worldwide to turn the tide on endless tasks, deliver best-practice security, and drive ROI.

CoreView | Because Microsoft 365 is at the core of your business.

For more information, please visit
www.coreview.com

Conversational Microsoft 365 Management

By Heather Severino

© 2024 Conversational Geek

ConversationalGeek®

Conversational Microsoft 365 Management

Published by Conversational Geek® Inc.

www.conversationalgeek.com

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Trademarks

Conversational Geek, the Conversational Geek logo and J. the Geek are trademarks of Conversational Geek®. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

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:	Heather Severino
Project and Copy Editor:	Ian Whiteling
Content Reviewers:	Joelle Palmer Rob Edmondson

Note from the Author

Greetings!

Microsoft has always left the door open for an ecosystem to spring up around their solutions and enhance what they did out of the box. Microsoft 365 (M365) is no different in that it opens the door for new cloud-based solutions to take what is built-in and make it better, giving us more options.

Areas I see this being valuable in are securing, governing and administering M365. There are solutions on the market that help prevent deadly misconfigurations, find and fix critical collaboration and identity risks, minimize privilege exposure, secure data, unlock wasted spend and supercharge productivity, automate things that you would typically have to do manually (or through a script you must take the time to figure out and build), and more.

The world of IT continues to become more complicated as IT teams try to do more with less. With a need to reduce costs, cope with staff shortages and hiring freezes, while managing more complicated cloud-based solutions, smart IT teams need to leverage solutions that will help them not just survive, but thrive. This book will explore the value of M365 tools to assist in doing just that.

Heather Severino

Getting Your Arms Around Securing and Governing Microsoft 365

The Covid-19 pandemic forced organizations to rely further on cloud-based communication and collaboration solutions like Microsoft 365. As a result, the number of active users has grown at a rapid pace. At the latest investor earnings release (quarter ending March 31, 2024), Amy Hood, executive vice president and chief financial officer of Microsoft, said: “This quarter Microsoft Cloud revenue was $35.1 billion, up 23% year-over-year, driven by strong execution by our sales teams and partners.” And Satya Nadella, chairman and chief executive officer of Microsoft, in commenting on the future, said: “Microsoft Copilot and Copilot stack are orchestrating a new

era of AI transformation, driving better business outcomes across every role and industry."

Details regarding Microsoft 365 are based around Microsoft's FY24 Q3 results.
goto.cg/MSFY23Q1

Each quarter there are hundreds of products being released/enhanced and this past quarter most of the major Microsoft 365 releases were Copilot features.

Copilot for Microsoft 365 is an AI-assistant that works alongside you in many of the apps, such as Outlook, Teams, Word, Excel, PowerPoint, OneNote, OneDrive, Forms and Whiteboard.

Every day I request intelligent real-time assistance from Copilot for Microsoft 365 in my work to get the right tone and length for emails, create feedback forms, write and summarize reports, create presentations, analyze data in worksheets, and summarize Teams meeting discussions. Getting this assistance helps me to be more creative and productive. And I'm not alone, a recent ZDNET survey found that 81% of workers using AI reported that it boosted productivity and overall quality of work.

With this rapid AI transformation, an organization may face challenges such as sensitive data being at risk of oversharing or overexposure. Gartner's recent 2023 Microsoft 365 survey reported that almost 60% of respondents said that oversharing, data loss and content sprawl were among the biggest risks to their organizations. If an organization hasn't prepared their Microsoft 365 tenant for deploying Copilot, end users or even contractors could prompt Copilot with a question and surface sensitive content they didn't know they

had access to (files that have been overshared to more people than needed).

To prepare your Microsoft 365 tenant for Copilot, there are pre-requisite and best practices that can help mitigate these risks such as applying the Zero Trust security principles.

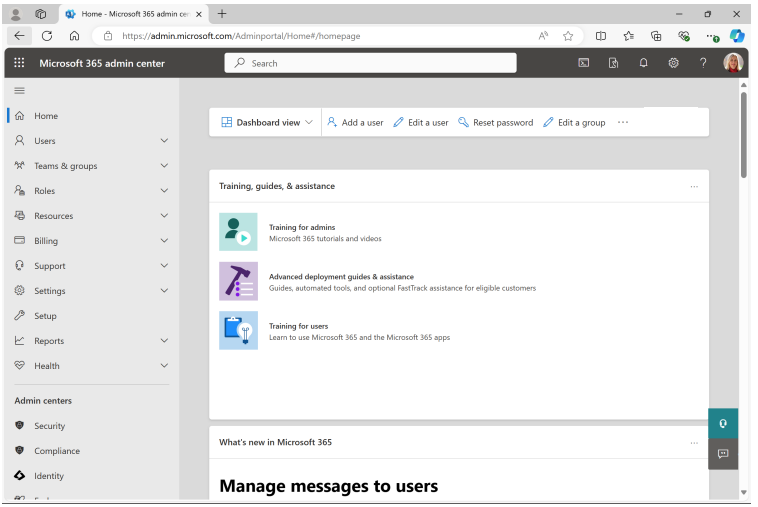
Learn more about Zero Trust strategy principles for Copilot in a Microsoft 365 tenant.
goto.cg/4dg4CdT

With such large volumes of users communicating and collaborating in many Microsoft 365 apps, such as Teams, Outlook, Loop, OneNote, Word, and Excel, as well as prompting Copilot, there comes the need for IT to manage this complex and sprawling environment to meet the specific needs of the organization. As Microsoft did with their legacy on-premises solutions, they've also done with Microsoft 365; they've provided us with a variety of tools used to address daily and one-off administrative needs. Managing configurations and enforcing policies across all the Microsoft 365 apps manually could lead to human misconfigurations.

But similarly, it's understood that Microsoft has so many customers with such varying needs, that it's impossible for their management capabilities to be comprehensive in nature. As you'll see, Microsoft has put thought into what kinds of management are possible out of the box, but some more advanced functionality either requires customization, scripting, or third-party help.

In moving from an on-premises world to a cloud-based one, there are major gains, but also very clear control losses for IT. Enterprises need to look at the current state of their environment with the goal of getting things back under control,

and that can be accomplished with both built-in and bolt-on solutions. You just need to know what can be done out of the box (or cloud, so to speak). Let's begin by looking at what comes right "out of the cloud".



The Microsoft 365 Admin Center

Out of the Box Microsoft 365 Administration Tools

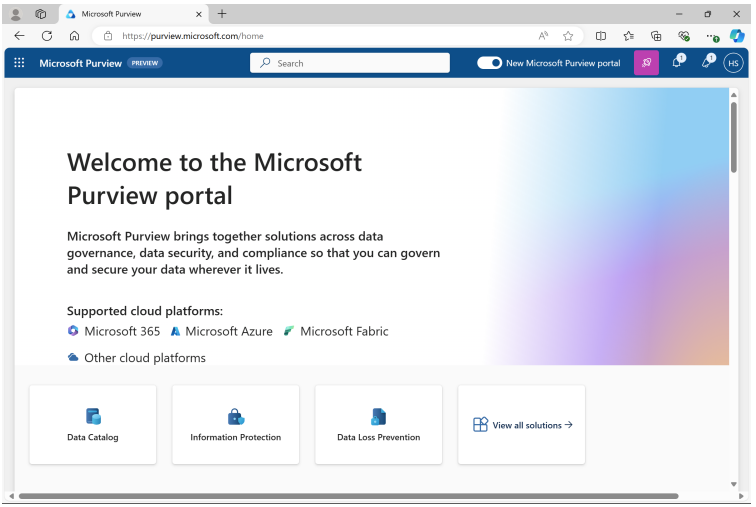
Microsoft provides a basic set of admin tools through administrative consoles that, where applicable, port back to their on-premises counterparts.

For example, when working with specific features of Microsoft 365, like Exchange Online, an admin will have the ability to work with a web-based portal solution like what they use on-premises.

More and more, however, Microsoft is working to create new dashboards that help to surface specific management tools so that admins can find them based on the technology and

manage them across different parts of the platform. Granted, it's not ideal to develop this way, but they're starting from a disparate server scenario and trying to merge architectures together (Exchange, SharePoint, Groups) while building new solutions on top (Teams).

A perfect example of this is the effort to pool together Security and Compliance for the entire platform into one dashboard. From within these consoles (the Security and/or Compliance console) you can establish settings for multiple built-in solutions. For example, a retention policy that applies to email, SharePoint sites, OneDrive accounts, Teams, and more.



In addition, you can establish a remote PowerShell connection to Microsoft 365 and perform most (but not all) tasks through the command-line as you would through the GUI (Graphical User Interface).

Although PowerShell is a great tool for command-based administration, some IT admins prefer to avoid the heavy lifting involved with scripting and such, and take a more automated approach.

Some smaller organizations might look at what Microsoft 365 offers and say it's "good enough" for their needs. Others might want greater transparency and visibility in reporting, license administration, role-based access control (RBAC) features, and more.

It's not a slight against Microsoft, or any other Software as a Service (SaaS) vendor for that matter, to say the out-of-the-box, built-in administrative consoles and features might not fully satisfy the management requirements of an organization – especially a large shop. But you can't let that deter you from pursuing the valuable communication and collaboration services platform provided through Microsoft 365. Microsoft has always left gaps for third parties to fill in – and Microsoft 365 is no exception.

The Microsoft 365 Management Battlefield

There are many aspects to consider when it comes to governing, securing and managing a Microsoft 365 tenant.

From a collaboration governance perspective, allowing guests/external users to access your Microsoft 365 tenant provides an enhanced way to communicate and collaborate all in one place. It can also provide guests/external users access to sensitive information that they should not have access to.

You may have heard this phrase or something like it before: "You can't govern, secure or manage what you can't see." If you can't easily see what guests/external users have access to, how can you be effective with governing or securing your

organization's data? The same applies to onboarding/ offboarding employees, securing sign-ins, managing licenses, policies and feature options.

Managing all of these can be both time consuming and prone to human error. Let's consider a few:

- Provisioning users is a clear example. First, you need to determine if you have enough licenses (and the right ones for the users), which isn't entirely an intuitive task. The Microsoft 365 Admin Center console will have you searching for the Licenses page (under Billing – Licenses). You can assign licenses from here or you can go back to the Active Users page (under Users) and begin the process of manually provisioning each user. Scripting the onboarding process for bulk user provisioning can be done through a remote PowerShell connection with a lot of research as well as trial and error.

- Deprovisioning is an even bigger issue, especially due to the security threat posed should a terminated user not be deprovisioned properly. Admins typically have a list of deprovisioning steps in mind provided by Microsoft that includes saving the contents of a former employee's mailbox (either through an export to .PST or by converting the mailbox to "inactive"), forwarding their email, wiping and blocking their mobile device, blocking access to their mailbox and data, moving their OneDrive content, removing the license, and deleting the account. And to accomplish all of this, you're moving from one Admin Center to another (e.g. from the M365 Admin Center to Exchange to SharePoint).

I'm assuming you understand the difficulty of having different Admin Centers (roughly a dozen now). Some were on-premises centers that are now cloud-based and include a wide array of configuration options. Others are less intense. The point is that there is a unique complexity to each Admin Center. And using each one requires an administrative skill set that isn't intuitive once you get below the surface and start diving into the real administrative side to Microsoft 365, as larger shops would.

- The onboard/offboard process taps into the **license management** side of Microsoft 365, which is yet another cause for angst. When first getting started with Microsoft 365, many IT admins will scan its different license plans, see the features connected with each plan (E1 / E3 / E5/ F3), and make quick decisions on the number of licenses they need based on the end-user count and perceived use of services. Done! *But is it really?* Every plan has a base of services that, in a buffet license arrangement, may feel right for a swath of your end users. You may think "I'll level up or down" depending on your needs. But the challenge is first finding out what you really need *before* you can right size.

I often see environments where the licensing is either oversized (perhaps you've bought more applications than your users need) or underutilized (due to a lack of adoption).

Speaking of adoption, Microsoft does provide easy-to-follow resources to help with Microsoft 365 adoption efforts.
To learn more: **goto.cg/4eeKNVS**

- Security governance and management is another key aspect of Microsoft 365. Microsoft now provides a Secure Score report (through the Security admin center that takes you to Microsoft 365 Defender settings) which will tell you, from a very high-level point of view, where you need to bolster security (hint: a large part of your score is based on multi-factor authentication [MFA] for all users). From the Secure Score dashboard, you can quickly select recommended actions to address and assign to an action plan.

- PowerShell is used to manage policies and feature options and to provide visibility into Microsoft 365 (goto.cg/2RPe7J0). Admins with too much permission can create scripts that punch holes in your Microsoft 365 security perimeter or measures. There are situations that require PowerShell, because it's the *only* way to accomplish the task. For example, PowerShell is sometimes the only way to obtain information that isn't available anywhere in the Microsoft 365 Admin Center. One example is the Deleted Item Retention Time. By default, it's 14 days, but you can adjust it up to 30 days through a remote PowerShell connection and the *Set-Mailbox-RetainDeletedItemsFor* command. PowerShell is also necessary for reporting on anything that spans the organizations tenant of apps and services by collating and combining that information.

We could go on, but the point is clear that organizations of all sizes will appreciate the services of Microsoft 365, and the governance, security and management tools provided along with those services may need an assist from a third-party management tool.

The Battlefield Isn't Just in the Cloud

Despite Microsoft 365 being a critical cloud environment, organizations struggle to implement best practice security, governance, and administration due to the complexity and size of the tenant.

Microsoft 365 has over 5,000 manual configuration types and about a dozen application admin centers. Having so many configurations and admin centers to manage manually can lead to dangerous human misconfigurations. This could result in downtime and more. Gartner says that 99% of cloud data breaches are the result of human misconfigurations. Automating your tenant configurations can include configuration templates, change management and audit processes, securing your Defender configurations, and providing test environments that replicate your production environment.

In addition to the security and governance challenges that come with trying to address the previously mentioned aspect of Microsoft 365 management, IT organizations themselves are facing a continual battle of their own that impacts their ability to properly govern, secure and manage platforms like Microsoft 365. These include:

- A Call to Reduce Costs – The economics of the past few years have resulted in a tightening of budgets, with IT organizations left trying to help grow the business with less spend to begin with.

- A Shortage of Staff – Many organizations are short of a few people needed within IT. In some organizations, budget cuts, hiring freezes, layoffs, and furloughs – while not commonplace – are a regular occurrence today, making it even more difficult for IT to address every Microsoft 365 governance, security

and management need. And in those organizations that continue to thrive, IT hiring isn't easy these days, with plenty of open headcount but not enough IT practitioners with adequate experience, skill, and expertise.

- More Complicated Environments – The past few years have accelerated digital transformation, causing organizations to rely on many of the applications within Microsoft 365 as their "digital workspace", only multiplying the workload on the already strained IT teams.

- An Expectation to Thrive – Despite the decline in resources dedicated to IT, many organizations still expect that IT will thrive, and enable the organization to be more productive and effective through its investment in Microsoft 365, driving growth.

The outcome of these challenges placed on IT is that to meet the need, IT will need to find ways to "do more with less" – a strategy that includes the use of third-party solutions designed to simplify, automate, and streamline governance and security for Microsoft 365.

Microsoft 365 Management Platforms

As we've discussed, Microsoft 365 uses a bevy of different SaaS applications and management consoles that are Frankenstein'd together. This fragmented set of Microsoft 365 features and administrative options are an opportunity to reinvent the management side and help admins through consolidation of management features.

There are seven functional management categories: *administration, role-based access control (RBAC), configuration*

management, policy management, license management, workflow automation, and *reporting*. The major players in this space will hit some or all these categories (and perhaps a few additional ones where they feel the out-of-the-box SaaS platform needs a boost, like security and compliance).

According to Gartner, "Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes." Compliance regulations, like General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI-DSS), and Health Insurance Portability and Accountability Act (HIPAA), make for another argument in favor of a management solution to assist with improved monitoring, reporting, and analytics.

The market direction, according to Gartner, is for management platforms to focus on "tactical IT administrative challenges in the native SaaS administrative consoles". Here are some places I see a bolt-on management platform being of value to organizations large and small that are feeling the pain of managing Microsoft 365.

Eliminating Reporting Silos

In the out-of-the-box Microsoft 365 Admin Center, there are a variety of different dashboards and management tools to access reporting, service information, and so on, adding to the complexity in trying to administer what are essentially massive server solutions stitched together with their individual consoles. Keep in mind, if Microsoft was starting all of this from scratch, they would have designed that unified console from the beginning, but that's not how Microsoft 365 was built. It started as on-premises endpoint and server solutions that are

now cloud-based, hosted solutions. So, a single pane of glass simply doesn't exist. This takes us back to the saying "you can't govern what you can't see". There's a need for a single pane view to see everything relating to governance, security and/or management.

Imagine a licensing report generated by a third party that can provide insights to unused licenses (that should be reclaimed), licenses that should be downgraded based on usage or mailbox/OneDrive document library size, and charge back license costs to business units based on SKUs. Or a report that presents financial reporting on SKU usage by department, team geography, company, etc.

That's where a third-party solution can help by offering up a single pane view dashboard with the ability to perform administration and reporting, and to handle permissions and such, that can make it easier to manage Microsoft 365 as well as provide visibility into the use of the solution.

Security & Compliance

Compliance is a term applied to a variety of different aspects for a business, but in this context, we need to lean towards security concerns within your Microsoft 365 environment. What happened? When did it happen? And what is the response generated? These are the key concerns that need to be addressed. This requires monitoring, alerting and automated resolution, because, with the excessive issues coming at IT each day, it's impossible to rely on manual response times to immediate threats.

Microsoft has some built-in monitor/alert/remediation functionality and additional ones you can purchase to extend your options. But here is where third-party compliance mitigation can really be a life saver.

Role-Based Access Control (RBAC)

The concept of least privilege is an important security principle that requires that RBAC be implemented properly. Microsoft 365 does offer a variety of admin roles, but they paint with a very wide brush (goto.cg/3IxCDdT).

If you scan the different admin roles, there is a *global administrator* (which can do pretty much anything… including handle services like Exchange, SharePoint, Teams and so on). On the lower end there are *global readers* (which have read-only access to admin centers). There is a *helpdesk admin* for password resets, support ticket management, and service health. There are also *service admins* (like for Exchange, SharePoint and Teams). And then there are category-focused roles for collaboration, devices, identity, read-only, security and compliance, and a few additional ones. The problem, however, is that even though the roles might narrow control, these are *global* credentials. Perhaps in small shops that kind of approach works, but in global environments where you have different teams and tiers, a granular approach that allows the management of specific groups, departments, geos, etc. is needed.

Despite Microsoft recommending you limit the number of folks who have global admin access, even when you restrict what a Microsoft 365 admin can do, they still have global credentials.

License Management

Microsoft 365 offers many apps and services for users to communicate and collaborate. An organization may use Viva Engage for enterprise-wide social, C-level executives likely communicate mostly through Outlook emails, and many business units, such as Human Resources, Finance and

Marketing, primarily use SharePoint sites or teams with channels to manage the day-to-day work. And everyone is probably using Teams chat for those one-to-one or small group quick communications. If these collaboration services (Viva Engage, Outlook, Teams, etc.) are not available or set up properly, users will go find something on their own and purchase it for their use. This scenario is what's known as Shadow IT. This is a security risk for many reasons including ensuring security of the organizations data, adhering to service compliance, not being able to manage user access, as well as other factors.

An organization needs to have a collaboration governance strategy for services such as Microsoft 365 groups, Microsoft Teams, Viva Engage and Outlook. Microsoft 365 groups provide many communication and collaboration services. When a group is created, other connected resources are also created, such as a SharePoint site, a Planner plan, a group mailbox and a calendar (may also include a team). An organization should define a collaboration governance strategy.

To learn how to create your collaboration governance plan go to: **goto.cg/4eiBJit**

Let's use Microsoft 365 groups as an example for what should be considered from a collaboration governance strategy perspective. You should consider implementing controls for naming conventions, an expiration policy and a blocked words policy.

Microsoft Teams (backed by Microsoft 365 groups and SharePoint sites) was released about five years ago. Shortly after Teams was released, some organizations enabled Teams but did not have policies in place for which users could create teams, how the teams were named, etc. As well, training and adoption efforts had not been implemented yet and it became the Wild West. Users were creating so many teams with varying names. Many of the teams were duplicates of others, just with different names. This is known as team sprawl. And then within a team there were too many channels, some covering the same topics just with a different channel name than the other.

To avoid having a Shadow IT issue within your organization, you should follow best practices during the planning of your collaboration governance strategy. Once you've identified the business requirements, risks, benefits, etc., you can establish the tools/features needed. This is where licensing should be considered.

Need to control team and site sharing? A Microsoft 365 E3 or E5 license should be assigned.

Need to restrict team or group creation for members of a security group? A Microsoft 365 E3 with Microsoft Entra ID P1 or P2, Microsoft Entra Basic EDU, or Microsoft 365 E5 licenses should be assigned.

Understanding licensing requirements early is not only a financial savings opportunity, from a Shadow IT perspective, it's also a security and governance opportunity. And it's a less license work to manage down the road opportunity!

Personally, I've bought into the Microsoft 365 communication and collaboration, 21st century modern workplace story. I believe the key to it is balancing the licenses needed along with increasing adoption efforts. This includes adoption of newer tools, such as Copilot. Help your users embrace the AI tools you've given them with the Copilot Success kit provided by Microsoft. To learn more: goto.cg/3ZGz3XB

Having optics on the adoption and consumption of your licensing and usage can ensure your money is better spent by right-sizing software spend. SMPs providing granular visibility into license usage can assist in the identification portion of these kinds of scenarios, as well as the downsizing of licensing.

In the past two years, between February 2022 and April 2024, the cost of a Microsoft 365 E3 license has increased by 95%. If your licenses are mismanaged, that could be a BIG cost hike!

Configuration Management

The Microsoft 365 environment is rapidly evolving, becoming more complicated every day. With that, the complexity of deploying and managing Microsoft 365 app configurations within your tenant also increases tremendously. There are more than 5,000 types of configurations that are split across more than a dozen admin interfaces for approximately 40 different workloads and services. And there are so many configuration variables. If you manage a large organization, you could be dealing with as many as 1 million configurations.

Microsoft provides a Configuration Manager to deploy and update Microsoft 365 apps to different channel groups. By using different update channels (Current Channel, Monthly Enterprise Channel, and Semi-Annual Enterprise Channel), you can choose how frequently users receive feature updates (as soon as they are ready, monthly, etc.). There are many factors determining which update channel you choose, such as user training and adoption, business unit needs, or other organization needs.

As mentioned earlier, according to a Gartner report, 99% of data breaches involve a human element and many of these are tied to misconfigurations that went undetected. To avoid a disaster like this, a third-party solution can help with strengthening configurations by:

- Providing pre-built configuration templates
- Automatically detecting when configurations drift off course
- Backing up configurations for restore (in case of accidental or intentional deletion)
- Auditing of configuration changes (for compliance)
- Change management process for configurations

Implementing these best practices not only strengthens Microsoft 365 users' security postures, it also saves hundreds to thousands of hours of work.

Workflow Process Automation

You can use the various Admin Center user interfaces (UIs) to accomplish the basic administrative tasks. And you can resort to PowerShell (command-line) to accomplish deeper bulk

administrative functions. However, the amount of time wasted and the degree of error or missed steps make the out-of-the-box consoles less than ideal.

Automation is one of those areas third-party solutions tend to focus on. Why should every admin in every organization have to research, build, test, and deploy PowerShell scripts for the basic process automation of their environment? Having access to one-click, graphical user interface-based options make much more sense and help eliminate the user error that comes from poor execution of home-grown scripting solutions.

Another area of concern is policy management and proper service configurations. While it's easy to get Microsoft 365 up and running with the basic settings, the deeper configuration and management sides to it require a great deal of effort for admins to research, test, and deploy (rinse/repeat). Having an easier means of deploying services with best practices in mind through default policy controls would prevent misconfigured accounts.

The Big Takeaways

Microsoft has done an incredible job of building a 21st century communication and collaboration solution for the modern workplace. As of May 2024, Microsoft 365 was being used by 345 million people and is evolving in many ways, visually to the end-user as well as behind the scenes for the administrators. One of the key challenges to moving on-premises solutions to the cloud, tying them together, and adding new solutions to the mix is the lack of a clear set of administrative tools.

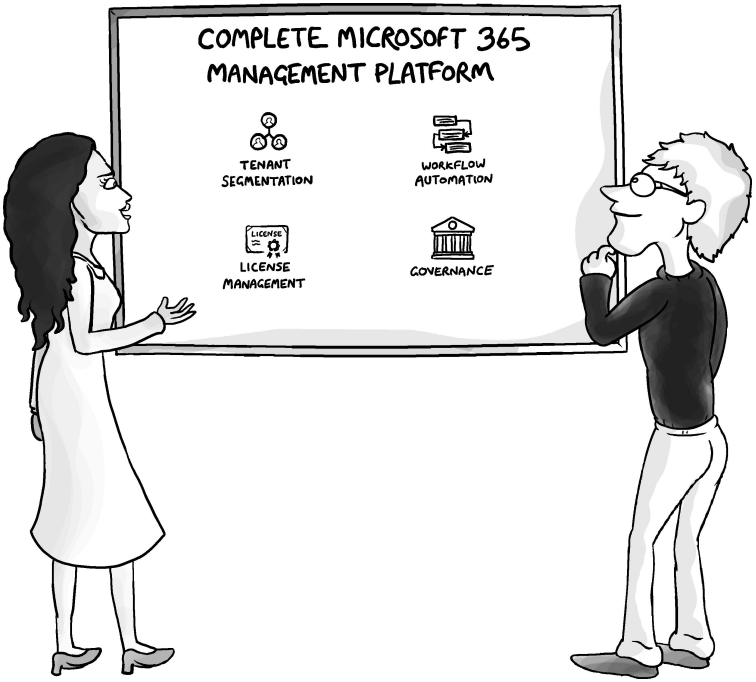
Legacy dashboards that display as reporting silos and do not provide a single pane of glass may not be super confusing for seasoned on-prem admins, but, with next-gen admins or non-IT admins being thrust into administrative roles, it can be challenging. We see Microsoft working to create new dashboards that combine stories across solutions (for security and compliance needs, as an example).

Additional "battlefield" issues revolve around provisioning and deprovisioning of users. Since some of the core solutions for Microsoft 365 were siloed and users were provisioned per service, it's been a challenge to ensure you can spin up a user with multiple services upon entry into an organization and deprovision those same services smoothly upon exit.

License management and license right-sizing is yet another factor to ponder either from a cost or adoption perspective. And then there are the nitty gritty administrative aspects that require admins use the command-line PowerShell remote connection options to configure, which is an added complexity with added room for user error.

The result is a need for a bolt-on Microsoft 365 management platform that assists in Microsoft 365 administration by providing the missing gaps of the story. A single-pane-of-glass dashboard to fill those gaps.

Vendor Sponsor: CoreView



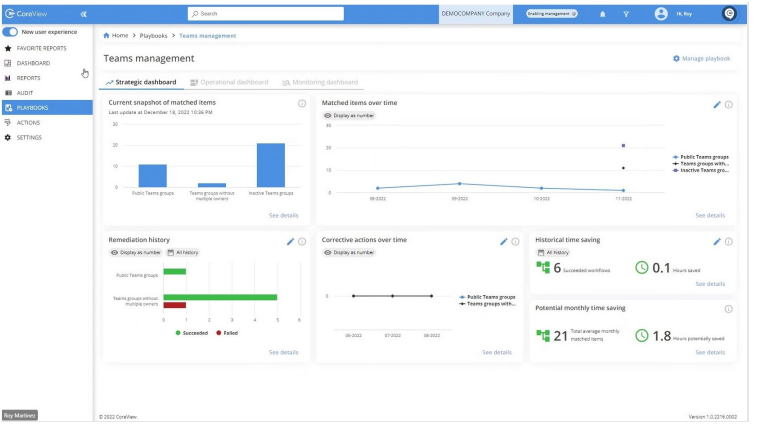
CoreView is a leading Microsoft 365 platform supplier that provides organizations with a security, governance and administration platform solution focused on tackling what Microsoft 365's native management is lacking.

Their primary offering is a suite of CoreView tools that puts all your Microsoft 365 administration in one unified space.

Let's dive in!

Overview

The CoreView dashboard takes the gaps discussed in the previous section revolving around issues with license over/under commit, Role-based Access Control (RBAC), and such, and offers mitigation through license lifecycle management, virtual tenants, and other features.



Microsoft 365 has an endless number of license and service configurations thanks to set plans and a la carte combinations. It can become convoluted and expensive, especially with larger, distributed organizations and/or government entities. With CoreView, you can spot unused, unassigned or underused licenses, and enjoy an average saving of 30% on license costs.

We mentioned the stress with having multiple admin consoles in Microsoft 365 instead of a single source of truth, but CoreView provides that single pane, replacing multiple admin center interfaces.

Additionally, you can set up license pools for better management, tracking, chargebacks, etc. The license pools allow you to delegate to different business units through

virtual tenants (aka tenant segmentation). This proactive license management helps you to control the assignment of licenses better (and who is paying for those licenses). In addition, it provides license usage reporting on the use of those accounts broken down by group. The goal is to optimize the licenses you have.

Using Microsoft Graph APIs, another key part of the CoreView options is the Teams dashboard that can help you see user activity, call quality and other telephony elements, inactive users and more. This kind of data can assist with the adoption side to management. And it's important to mention that the reporting is actionable immediately from within the report. You can run actions from within the report or string those actions together into automated workflows.

Automation

It's great to be able to see information and reports, but it's even better to be able to fix problems or change things from the report itself. Workflow automation, another important aspect of CoreView, helps optimize execution of common, repetitive tasks while removing human error with automated functions like user provisioning and de-provisioning. Combine that with auditing, so you know who is doing what, when, where and why.

Pre-Built Playbooks

It's easy to tell folks to establish compliance standards with KPI metrics that lead to automated response. It's not quite that easy to make that happen, especially with the standard Microsoft 365 tools. CoreView has pre-built playbooks with out-of-the-box and/or custom designed compliance standards. Standard Key Performance Indicators (KPIs) with metrics tied to remediation and automation pulls it all together to provide much more control over your environment, whether it be

security-based, performance-based or adoption-based, it's all about control.

Through the playbooks feature you can build out playbooks to adhere to specific compliance scenarios and view it all through a single dashboard.

Continuance Compliance Modelling and Remediation

This will also help to cut down on escalations, which means fewer help desk tickets. That follows the same thinking we mentioned earlier from Satya Nadella in helping customers "do more with less".

Playbooks let you implement governance policies automatically, so those often-forgotten tasks get done. For example, how often in Teams do we have abandoned, headless teams? The original owner is gone. Manually searching and resolving these types of situations can be a time waster. Instead, use a playbook to find them, and tie the action to finding a new owner for them. That's just one of many examples of how playbooks can help resolve issues whether it be Teams management, governance issues, cyber security concerns, and more.

Custom Actions is a feature that allows you to use your existing PowerShell commands and scripts within the CoreView solution as either a one-off or part of a workflow. There are some fun things you can do here regarding your PowerShell scripts to make them available to non-experts within the organization (aka democratized PowerShell). You can turn

those scripts into buttons and assign them to admins for ease of use.

A friend of mine refers to CoreView as a makeshift repository of all your PowerShell scripts allowing for better change control without having to go full bore into a Git scenario.

Delegated Administration

CoreView allows you to break up your Microsoft 365 tenant into smaller sub-tenants or virtual tenants (v-tenants). The granular, easy-to-use aspects of role-based access control options are valuable; they help fill the gaps of Microsoft 365 administration by giving admins specific permissions to perform only those tasks they're assigned and only over those users they're assigned. So, you're able to have local admins, or assign admins to departments, and limit who the admin manages, and what management functions they can perform. Wait… that sounds like… you've got it… real RBAC. This is in stark contrast to the global permission allowances given to IT admins because it's a bit of a nightmare to try and box them in using the built-in roles provided.

Allowing autonomy based on geographic location and/or departments not only helps with segmenting users for management, but also adds another security control angle. Each agency has independent siloed jurisdiction which allows you to enforce the security boundaries you map out for your organization while also providing autonomy to those boundaries through the permission sets and augmentation of RBAC.

Security

With millions of users, Microsoft has a tremendous amount of threat intel that can be of benefit to them, and to your organization. CoreView provides forensic analysis and auditing with long-term, full-year storage of activity logs. Data can be mined and surfaced back in compliance reports that can be analyzed by department, business unit, country, and so on. This will help you see where breaches are occurring. You're able to create custom, real-time alerts to allow for faster response times for your IT staff (which is great for inappropriate file access or sharing and false log-in attempts).

File auditing and data analysis can really help an organization to see user behavior throughout their Microsoft 365 environment. CoreView has 200+ customizable reports to assist you with monitoring usage and end-user activity to ensure you're fully compliant with company policies and governmental regulations.

CoreView calls their audit logs "human readable", which is rare, as you know if you're ever seen some of the log data IT folks need to parse through. Very human unreadable most of the time.

There is a health check service that provides a full report back on license utilization, vulnerabilities, security and compliance risks, and usage activities. The results are organized into four categories: license management, security and compliance, change management and adoption, and an action plan.

For example, the assessment might report that you are not using multi-factor authentication (MFA) within your environment (or perhaps it hasn't been enabled for all users to take advantage of). Through CoreView, you can easily set and enforce MFA policies. The same is true of password policies.

You can also monitor and enforce appropriate password policies for your organization.

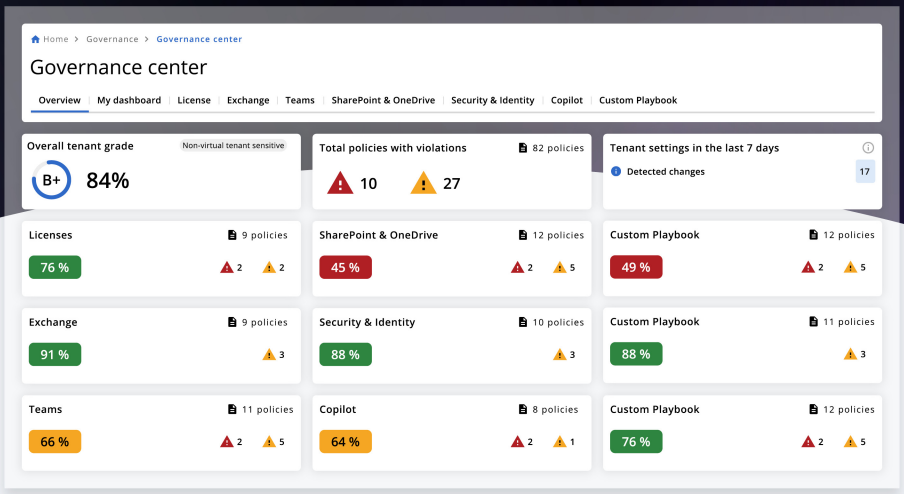
That's not to imply that CoreView is an intrusion detection system. Rather, it provides insight into dangerous user behavior and misconfiguration of your Microsoft 365 portal.

In Conclusion

CoreView is an enterprise-grade Microsoft 365 Security, Governance and Administration Platform with a heavy focus on improved administration, RBAC, policy management, license insights, workflow automation, reporting, and more. Through its centralized approach to managing Microsoft 365, it provides organizations with an ability to simplify the work of increasing the overall adoption of Microsoft 365, improving end-user productivity, centralizing IT's control, and enhancing the organization's security and compliance stance – all while lowering the overall cost of owning Microsoft 365.

Find and fix hidden risks in Microsoft 365 — *before they cost you.*

Get full visibility and control with **CoreView ONE**.



End-to-end Microsoft 365 has never been easier.

- Misconfigurations? **Fixed.**
- Security policies? **Enforced.**
- Entra identities? **Secured.**
- Tenant configurations? **Backed up.**
- User licenses? **Governed.**
- Provisioning? **Automated.**

See CoreView in action.

www.coreview.com/product-tour

CoreView

Quickly become conversational about Microsoft 365 Management in any setting

With Microsoft 365 reaching global dominance, enterprise organizations need help to manage, secure and optimize their Microsoft 365 tenants. Disparate admin centers, cumbersome workflow process automation, simplistic RBAC, license bloat, and other management issues are causing some to be frustrated by Microsoft 365. In this book, we will discuss the challenges of managing Microsoft 365 and look at the value of a Microsoft 365 Management Platform to assist with these frustrations.

About Heather Severino

Heather Severino is a Microsoft MVP, Microsoft Certified Trainer (MCT) and owner/full-time author and trainer for TeachUTech, specializing in Microsoft Office, presentation and instructional skills training, instructional design, and authoring training videos.

ConversationalGeek®

For more content on topics geeks love, visit

conversationalgeek.com