CoreView

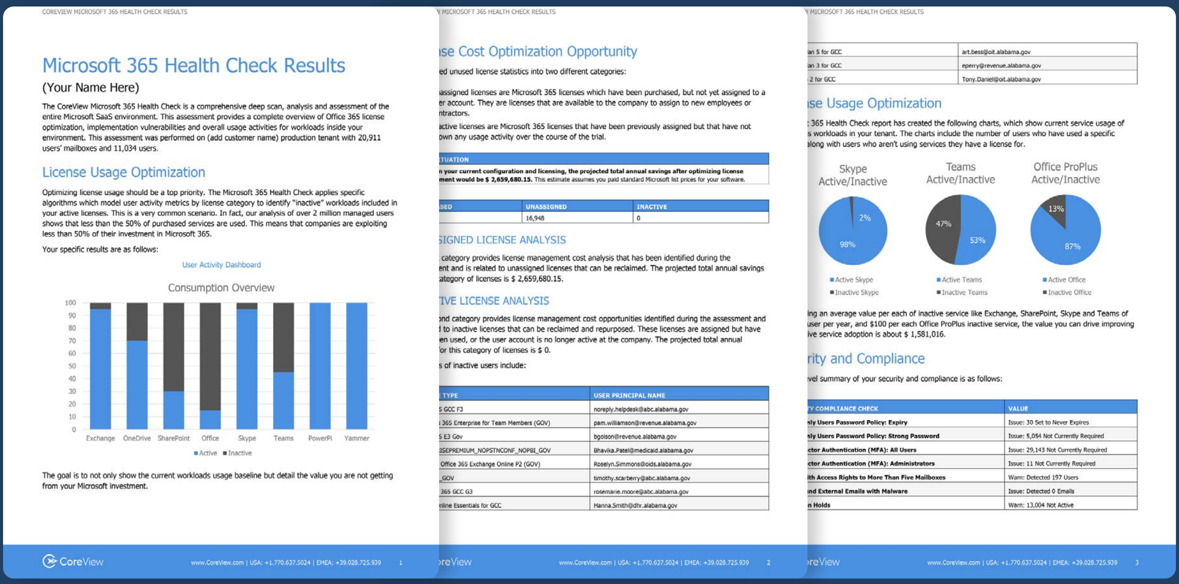
Microsoft 365 security: A Deep Dive Into The Challenges of Governance & License Management

Introduction

In the past few years, online collaboration has catapulted from a nice-to-have to mission critical, as more employees work remotely and for many organizations, "Office 365" is now a stand-in for a brick-and-mortar office. But with skyrocketing usage has come increasing complexity. Today, what is now called Microsoft 365 includes 25 different apps and 17 different admin panels – with new apps being added all the time. Combined with skyrocketing usage, this complexity means many IT teams are struggling just to keep up – let alone to get ahead with proactive activities like security monitoring, governance, and attestation.

But what's making managing Microsoft 365 (M365, for short) so complicated, and how can IT teams break out of the day-to-day management headaches to truly take control of their M365 instance?

To find out, CoreView studied more than 1.6 million M365 users to identify the most common problems, understand what organizations are doing well, and reveal gaps in IT management strategies.



COREVIEW MICROSOFT 365 HEALTH CHECK RESULTS

Microsoft 365 Health Check Results

(Your Name Here)

The CoreView Microsoft 365 Health Check is a comprehensive deep scan, analysis and assessment of the entire Microsoft SaaS environment. This assessment provides a complete overview of Office 365 license optimization, implementation vulnerabilities and overall usage activities for workloads inside your environment. This assessment was performed on (add customer name) production tenant with 20,911 users' mailboxes and 11,034 users.

License Usage Optimization

Optimizing license usage should be a top priority. The Microsoft 365 Health Check applies specific algorithms which model user activity metrics by license category to identify "inactive" workloads included in your active licenses. This is a very common scenario. In fact, our analysis of over 2 million managed users shows that less than the 50% of purchased services are used. This means that companies are exploiting less than 50% of their investment in Microsoft 365.

Your specific results are as follows:

User Activity Dashboard

The goal is to not only show the current workloads usage baseline but detail the value you are not getting from your Microsoft investment.

CoreView www.CoreView.com | USA: +1.770.637.5024 | EMEA: +39.028.725.939 1

V MICROSOFT 365 HEALTH CHECK RESULTS

ıse Cost Optimization Opportunity

ed unused license statistics into two different categories:

ıassigned licenses are Microsoft 365 licenses which have been purchased, but not yet assigned to a er account. They are licenses that are available to the company to assign to new employees or ntractors.

active licenses are Microsoft 365 licenses that have been previously assigned but that have not own any usage activity over the course of the trial.

TUATION
n your current configuration and licensing, the projected total annual savings after optimizing license ment would be $ 2,659,680.15. This estimate assumes you paid standard Microsoft list prices for your software.

SED	UNASSIGNED	INACTIVE
	16,948	0

SIGNED LICENSE ANALYSIS

category provides license management cost analysis that has been identified during the ent and is related to unassigned licenses that can be reclaimed. The projected total annual savings ategory of licenses is $ 2,659,680.15.

TIVE LICENSE ANALYSIS

ond category provides license management cost opportunities identified during the assessment and d to inactive licenses that can be reclaimed and repurposed. These licenses are assigned but have en used, or the user account is no longer active at the company. The projected total annual for this category of licenses is $ 0.

s of inactive users include:

E TYPE	USER PRINCIPAL NAME
5 GCC F3	noreply.helpdesk@abc.alabama.gov
365 Enterprise for Team Members (GOV)	pam.williamson@revenue.alabama.gov
5 E3 Gov	bgolson@revenue.alabama.gov
ISEPREMIUM_NOPSTNCONF_NOPBI_GOV	Bhavika.Patel@medicaid.alabama.gov
Office 365 Exchange Online P2 (GOV)	Roselyn.Simmons@oids.alabama.gov
_GOV	timothy.scarberry@abc.alabama.gov
365 GCC G3	rosemarie.moore@abc.alabama.gov
nline Essentials for GCC	Hanna.Smith@dhr.alabama.gov

oreView www.CoreView.com | USA: +1.770.637.5024 | EMEA: +39.028.725.939 2

V MICROSOFT 365 HEALTH CHECK RESULTS

an 5 for GCC	art.bess@oit.alabama.gov
an 3 for GCC	eperry@revenue.alabama.gov
2 for GCC	Tony.Daniel@oit.alabama.gov

ıse Usage Optimization

365 Health Check report has created the following charts, which show current service usage of s workloads in your tenant. The charts include the number of users who have used a specific along with users who aren't using services they have a license for.

ing an average value per each of inactive service like Exchange, SharePoint, Skype and Teams of user per year, and $100 per each Office ProPlus inactive service, the value you can drive improving ive service adoption is about $ 1,581,016.

rity and Compliance

vel summary of your security and compliance is as follows:

Y COMPLIANCE CHECK	VALUE
nly Users Password Policy: Expiry	Issue: 30 Set to Never Expires
nly Users Password Policy: Strong Password	Issue: 5,054 Not Currently Required
ctor Authentication (MFA): All Users	Issue: 29,143 Not Currently Required
ctor Authentication (MFA): Administrators	Issue: 11 Not Currently Required
ith Access Rights to More Than Five Mailboxes	Warn: Detected 197 Users
nd External Emails with Malware	Issue: Detected 0 Emails
n Holds	Warn: 13,004 Not Active

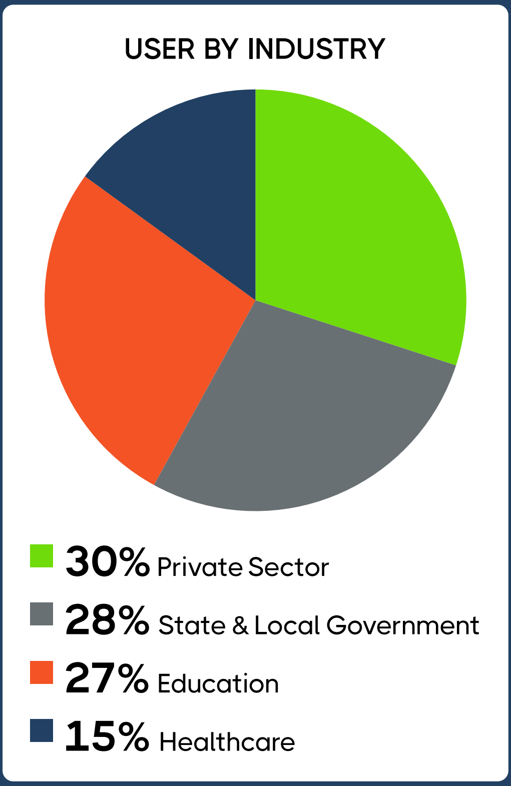
oreView www.CoreView.com | USA: +1.770.637.5024 | EMEA: +39.028.725.939 3

As a part of our normal business, CoreView runs "Health Checks" on Microsoft 365 tenants to help organizations understand what's lurking in their tenants that they might not be aware of. This report is the compilation of the last two years of Health Checks, bringing together all of the most common issues we discover and helping Microsoft 365 admins identify what issues they should be looking for.

Who We Studied

We pulled anonymous data to see what's trending now, what people are still struggling with, and where to find the most common problems. In total, these Health Checks included 1,629,442 users across a variety of industries. On average, the organizations we studied had 40,736 employees, and ranged from 1,000 up to nearly 400,000 users. 30% of these users were in the Private Sector, 28% from State and Local Government, 27% from Education (including both K-12 and Higher Education), and 15% from Healthcare.

We studied organizations across North America, EMEA, as well as a handful in other regions as well. In total, there were 1,018,705 users in the United States, 319,281 in Canada, 232,302 in Europe, and 58,543 in Australia.



1,018,705 users
in the United States

319,281 users
in Canada

232,302 users
in Europe

58,543 users
in Australia

How can IT teams break out of their day-to-day management headaches to truly take control of their M365 instance?

Security Governance

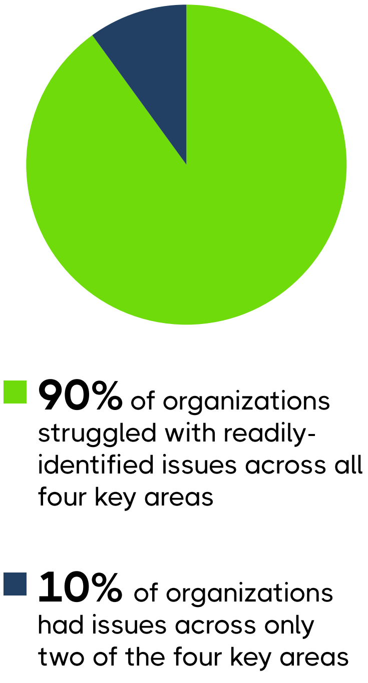
What is Security Governance?

According to the UK's National Cyber Security Centre[1] *"Security governance is the means by which you control and direct your organisation's approach to security."* Gartner tells us that Security Governance[2] "...governs the interplay of mitigating identified business risks, addressing internal and external threats, and dealing with compliance." In other words – it's how you implement security controls, and how you ensure ongoing review of key segments of your security strategy.

Why It Matters

In most organizations, Microsoft 365 contains nearly all of the organizations' important data – from HR files to financials to constituent information to competitive advantages. It's also where employees spend a large portion of their day, and therefore fraught with potential for security threats and attacks.

Perhaps most glaringly, among the organizations we studied, almost all – 90% — were still struggling with readily-identified issues across all four key areas – **Password Policies**, **Multi-Factor Authentication**, **Email Security**, and **Failed Logins**. The remaining 10% of organizations had issues across only two of the four key areas. Not a single organization had fully addressed these key aspects of security.



These aren't new security areas in the industry – in fact, they've been hot topics of discussion, and played heavily in key security recommendations, for years - if not decades. Yet almost everyone we studied still struggled to maintain strong security policies in these areas.

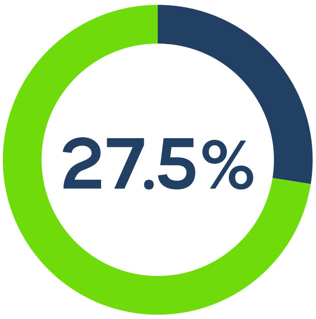
So why are IT teams still struggling to enforce the most basic security policies? These are conscientious IT teams with strong policies in place, and yet, at the end of the day, they're failing to effectively protect their organizations from ever-present and well-known risks.

The answer isn't in stronger policies, or improved employee awareness. Day in and day out, we talk to IT teams that are overwhelmed, understaffed, and struggling to keep up with employee demands. They're not missing key security aspects because they're not aware; they're missing them because they get lost in the mountain of manual work to do each day, and security governance – meaning stronger enforcement, mitigating risks, addressing internal and external threats, and dealing with compliance – gets pushed to the bottom of the pile.

The Challenge of Microsoft 365 Administration

One key trend that came up over and over during the study was the challenge of Microsoft 365 administration, and the heavy burden facing M365 admins. In total, there were 8,992 admins studied, representing not just Global Admin roles but also everything from Intune Administrator to Printer Admin. On average, each organization had 12 Global Admins. This is already higher than Microsoft's recommended 3-4 Global Admins per organization; but is actually just a small number of the overall admins required to keep Microsoft 365 running.

Interestingly, even organizations with higher numbers of admins (the top 40% of those studied) struggled to ensure consistent security policies. In fact, among those with more admins, there were also more admins without MFA enabled (27.5% of admins, versus 26% of admins among organizations with fewer admins). They were also more likely to experience malware issues, with nearly 10x the number of infected emails sent among organizations with more admins. Some of this is to be expected – larger organizations have more admins but also more potential issues. But throwing more employees at the problem isn't solving it. Even with all these various types of administrators, they still struggled to keep up with enforcing the most common security strategies. As Microsoft 365 becomes more and more complex, it becomes even harder to keep up with everything that's occurring in an M365 tenant (or tenants!).



Of admins without MFA enabled

Even with all of these various types of administrators, they still struggled to keep up with some of the most common security strategies. As Microsoft 365 becomes more and more complex, it becomes even harder to keep up with everything that's occurring in an M365 tenant (or tenants!).

Password Policies

Having strong password policies is a cornerstone of any good security strategy. During our Health Checks, we identify the number of:

××××

Users with password expiration date set to 'never expire'

××××

Administrators with password expiration date set to 'never expire'

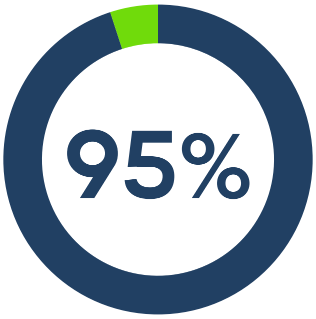
××××

Users with strong password requirements disabled

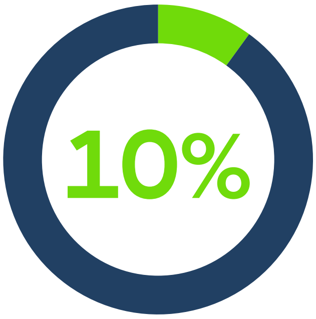
××××

Administrators with strong password requirements disabled

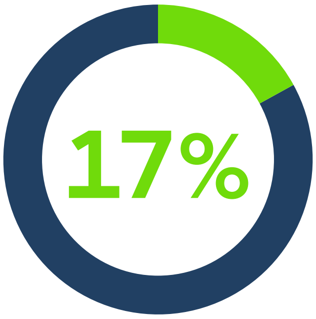
Across the entire group we studied, only a single tenant had neither users nor administrators without a password expiration date, or without strong password requirements. 95% of organizations studied had identified security issues in both areas, while only 10% of organizations avoided password expiration weaknesses and 17% had strong password requirements across the organization.



Of organizations had identified security issues in both areas

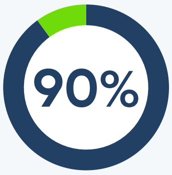


Of organizations avoided password expiration weaknesses

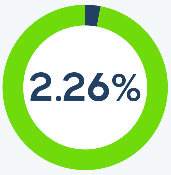


Of organizations had strong password requirements across the organization

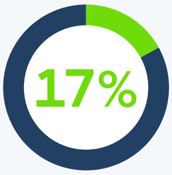
Other key findings:



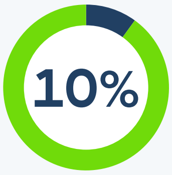
90% have at least one user without a password expiration policy in place; **32%** have more than ten users without one.



Overall, **2.26%** of users don't have a password expiration policy – for a total of 36,780 users. This represents an average of more than 900 users in each organization we studied.



Only **17%** of organizations required strong passwords for ALL users.



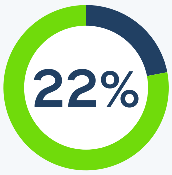
10% of organizations have thousands of users without strong password requirements.

Overall, nearly every organization is leaving the door open for cybersecurity threats due to weak credentials, particularly for administrator accounts.

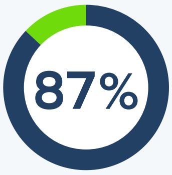
Multi-Factor Authentication

Multi-Factor Authentication (MFA) is one of the most important security practices you can employ. Better yet, Microsoft 365 has a robust and proven MFA solution built-in. MFA has become so recognized that the National Institute of Standards and Technology (NIST) guidelines on password security now specifically recommend the implementation of MFA. The United States Department of Homeland Security recommends that all Office 365 users implement MFA.

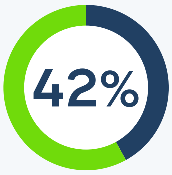
Yet when reviewing the data, we found that:



22% of organizations have MFA disabled for at least 1/3rd of their users - but are not using a third-party solution



87% of organizations have MFA disabled for some or all of their admins



42% have MFA disabled for at least 1/3rd of their admins

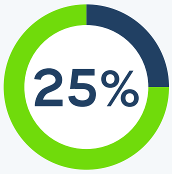
MFA can be particularly critical for users with administrative roles which present a substantial security risk. Yet 28.3% of the admins studied had MFA disabled, as well as 6.5% of all users. In other words – admins, the most critical accounts to protect, are more than four times more likely to have MFA disabled.

Email Security

The average IT team is well aware of the need for good email security strategies. During a Health Check, we look for a variety of potential email security issues, including:

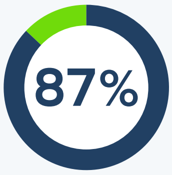
- User accounts that have access to more than 5 other user mailboxes, which could represent a security loophole
- Malware being sent from mailboxes within the organization
- Users auto-forwarding emails to external email addresses or freemail providers, which could indicate data leakage

Overall, among the organizations we studied:

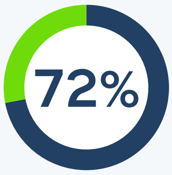


25% had at least one detectable email containing malware sent within the last 7 days

10% had more than 25 detectable malware events



87% had users auto-forwarding emails to external addresses



72% had users auto-forwarding emails to Gmail or other freemail providers

Some of this activity may be legitimate – such as users auto-forwarding emails to an external vendor or contractor; but these practices can be dangerous and should be regularly evaluated to ensure that nothing suspicious is occurring.

Failed Logins

Large-scale security incidents, where access was gained through illicit logins, hit the news all the time. With these types of events so prevalent, most organizations should be taking action, such as:

- Tracking attempting logins from known hacker “hot spots” to harden security
- Malware being sent from mailboxes within the organization
- Users auto-forwarding emails to external email addresses or freemail providers, which could indicate data leakage

In reality, every organization we studied is being attacked with illicit attempted logins constantly. The volumes of attempted logins were quite a bit higher than expected. In a normal organization, there are some legitimate failed logins, due to employees forgetting their information, devices with old login information, and similar events. Even assuming that one in every four users forgets their login every week, it would still be a fairly small number of overall failed logins.

In reality, the organizations we studied experienced 3.5 failed logins per user every 7 days, for a total average of 140,433 failed logins per organization each week, or around 14x the number of failed logins we can assume to be legitimate. In other words – for every employee who forgets their password, there are 13 additional attempts to hack into their account. How many of those failed login attacks are resulting in successful access?

140,433
failed logins

PER

Organization
each week

In fact, the top 5% of organizations experienced more than a million failed logins each week. Combined with weak password requirements being so prevalent, this is a huge potential risk – and one that is being missed in every organization we studied.

Every organization we studied is being attacked with illicit attempted logins constantly.

License Optimization

Why License Optimization?

For our purposes, license optimization is the process of ensuring that employees have the licenses they need to do their jobs effectively, without spending more than is necessary or having an excessive number of licenses sitting on the shelf unused.

Due to the complex nature of Microsoft 365 licenses, for some organizations license management is a full-time job in itself. Getting the right licenses requires balancing considerations that are constantly changing, such as:

- Microsoft price changes
- Employee growth
- “Free trial” licenses that were previously complimentary but may convert to paid licenses
- Strategic changes in desired license mix – such as upgrading all executives to E5 licenses for security reasons
- Licenses currently unassigned – including those purchased in anticipation of future growth, unassigned due to normal employee turnover, and other needs
- Licenses currently inactive – including those assigned to employees currently on leave or otherwise explained by normal business activities

License management is
a full-time job in itself.

In the absence of a dedicated person or team to focus on these issues, it’s all too common for the pile of unassigned and inactive licenses to grow over time, and include license waste in excess of the amounts needed due to normal business activities such as turnover and anticipated growth. It’s worth noting that, for many organizations their Microsoft contract is a multi-year, complex agreement that cannot be easily modified during the term of the agreement, and that in many cases we identify opportunities to avoid future costs, or avoid purchasing additional licenses, as opposed to a direct reduction in current costs.

License Optimization Opportunities

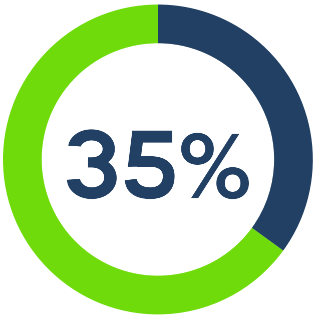
On average, the organizations we studied purchased 59,617 licenses – but only have 40,736 users. Now, some of this is totally normal, because a given user may have a primary Microsoft 365 license, as well as a separate Power BI license, for example. And even in that scenario, buying separate licenses may be less efficient and end up costing more than buying a single combination license, depending on the situation. But upon further review, we see that:

- The average organization had 12,922 licenses unassigned (21.6%) and sitting on the shelf, and another 6,134 inactive licenses (10.2%), for a total savings opportunity of 31.9% on average.
- 17% had more than 10,000 unassigned licenses sitting on the shelf, while 10% had more than 10,000 inactive licenses.

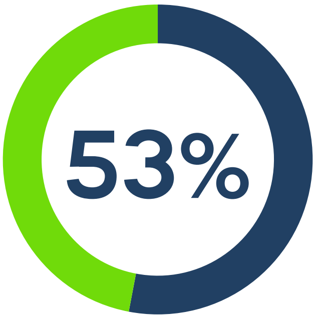
Inactive licenses also represent a potential security risk, in that users who may have left the organization may still have access, or may have poor password security and be easily hacked. They may also be a reflection of overpurchased licenses, where users don't need the capabilities that were purchased.

License Usage

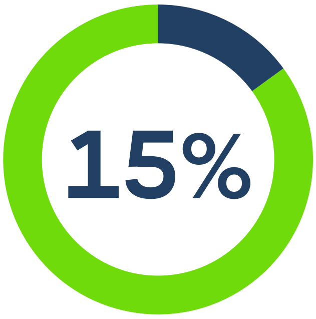
One of the key findings from the study was the extent of disuse by application. In other words – the extent to which users don't use the apps for which they have licenses. For example, among those with Microsoft Teams licenses, on average 35% of users didn't access Teams in the course of a week. For OneDrive, it's even higher, with 53% of users inactive in a given week. On average, 15% of users were not even active in Exchange during the preceding week.



Of licensed users didn't access Teams



Of licensed users didn't access OneDrive



Of licensed users didn't access Exchange

These usage statistics will vary dramatically from organization to organization, depending on industry, employee types and mix, other tools available, and other factors. What's important, however, is that IT teams have a strategy for monitoring usage, and reacting accordingly – whether it be to cut back on licenses that don't make sense, eliminate other tools, or roll out additional training on specific apps.

Summary

As this study clearly indicates, IT teams can't keep up with industry-standard best practices, let alone the myriad of industry and region-specific compliance requirements, without a cohesive strategy for governance, enforcing internal and external policies and continually ensuring compliance with these policies. IT leaders and teams that are still monitoring and enforcing security policies manually are falling behind, becoming more and more unable to keep up with the demands facing them.

Instead, leading IT teams are increasingly choosing to automate and delegate critical security, license optimization, and other management tasks, offloading an estimated 30-40% of their workloads and allowing them to focus on important tasks instead of repetitive manual work. CoreView has had the privilege of helping many of these leading IT teams change the game, from one of chaos and overwhelm to confidence and control. If you're interested in seeing what's really going on in your own tenant, please let us know. We look forward to helping you get Microsoft 365 under control.

About CoreView

CoreView is the #1 Microsoft 365 management platform for IT teams who are transforming the way they run their Microsoft 365 stack. CoreView delivers a unified approach to configuration management, delegated administration, and automated governance with capabilities far beyond native tools or point products. Organizations of all sizes choose CoreView to command their operations, optimize tasks, refine governance strategies, and empower their workforce.

We are proud to be a Microsoft AI Cloud Partner and available in the Azure Marketplace. We are committed to working exclusively with the global network of Microsoft resellers, solution integrators and managed service providers. CoreView | Because Microsoft 365 is at the core of your business.

For more information,
please visit coreview.com.

1. Introduction to security governance. (n.d.). Retrieved September 22, 2022, from https://www.ncsc.gov.uk/collection/risk-management-collection/governance-cyber-risk/security-governance-introduction
2. Definition of Security Governance - Gartner Information Technology Glossary. (n.d.). Gartner. Retrieved September 22, 2022, from https://www.gartner.com/en/information-technology/glossary/security-governance