BEST PRACTICES GUIDE

Ultimate 10 Step Guide to Boosting Your Microsoft Secure Score

Essential Steps to Improving Office 365 Security

CoreView

Now It's Under Control

One of the most useful features that comes with the Microsoft Office 365 native Admin Center is Secure Score, which shows how your level of security compares with other companies and serves as a basis for improvement.

Microsoft Secure Score awards points for good security practices, such as adopting multi-factor authentication (MFA), using third party solutions to improve security, regularly producing and viewing security related reports, and using and configuring recommended Office 365 security features.

What's Inside

Microsoft Secure Score, formerly Office 365 Secure Score, is one of the best ways to measure your tenant's security posture. Boosting your score is great for your Office 365 – and job security!

Table of Contents

Step One – Get to Know the Score

The New Secure Score

Office 365 Secure, as the name indicates, is focused on Office 365 security. Its replacement, the new Microsoft Secure Score now includes Azure security, and so is a broader measure of Microsoft security. "The Office 365 Secure Score has evolved into the Microsoft Secure Score. This tool assesses the security state of multiple aspects of Office 365 by evaluating which controls are enabled and presenting a score — the sum of the point values for each control. The score is a reasonably meaningful starting point for measuring and improving your Office 365 security posture," Microsoft explained. "To help you devise a plan for a staged rollout of controls, the tool combines recommendations into five categories: identity, data, devices, apps and infrastructure."

Scoring High with Security – Your CoreView Secure Score Results

CoreView takes Microsoft Secure Score a step further by adding a new dimension to Secure Score, giving you a deeper level of analysis and ranking through the CoreView version of Secure Score. To make it easier to understand, we use the same formatting and user interface as Microsoft Secure Score – and simply extend it with greater depth and insight.

As a result of these efforts, CoreView Secure Score turns Office 365 basic security scoring and data into actionable, usable, vital information to protect your SaaS environment. We also add custom policies, workflows and automation to maintain and tighten security.

The CoreView Secure Score also includes a benchmark of the total score compared with:

- All Microsoft Office 365 tenants (using data provided by Microsoft)
- Tenants with similar size to your organization (data also provided by Microsoft)
- Comparisons with all CoreView tenants (with data provided by CoreView)

According to Gartner analyst Neil MacDonald,
“Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities.”

Step Two – Analyze Your O365 Tenant

Discover Weaknesses and Vulnerabilities

The CoreView Office 365 Health Check (a complete scan of your O365 tenant to determine security posture, application usage and license state) shows many ways you can boost your Secure Score. The Health Check is deep analysis, and offers an O365 Security Action Plan based on the findings. It also includes an enhanced version of the Microsoft Secure Score.

Below you see an example of a Security Compliance Check that dives into passwords, MFA status, malware exposure, state of admin privileges (excess rights are a huge security issue), email safety, and data leakage exposure level.

SECURITY COMPLIANCE CHECK	VALUE
Cloud Only Users Password Policy: Expiry	Issue: 6 Set to Never Expires
Cloud Only Users Password Policy: Strong Password	Issue: 1,837 Not Currently Required
Multi-Factor Authentication (MFA): All Users	Issue: 72,380 Not Currently Required
Multi-Factor Authentication (MFA): Administrators	Issue: 77 Not Currently Required
Users with Access Rights to more than Five Mailboxes	Warn: Detected 854 users
Users Send External Emails with Malware	Issue: Detected 183 emails
Litigation Holds	Warn: 11,354 not active
User with Administrative Roles	Warn: 178
Company Administrators	Warn: 7
Users with Auto-Forwarding rules to External Email Addresses	Issue: 408
Users Forwarding Email to gmail.com domain	Issue: 9
Anonymous Links Shared	Issue: 0
Anonymous Links Used	Issue: 0
SharePoint Sharing Activities	Info: 10,708
OneDrive Sharing Activities	Info: 23,602
OneDrive with Multiple Owners	Warn: 0
Number of Sign-ins Failures in Last 30 Days	Info: 44,019
Top 3 Countries with Failed Logins	Info: United States, Canada
Top 3 Departments with Failed Logins	Info: enterprise infrastructure, retailtainment hq, syndicated
Top 3 Attacked Users	Info: doug.robbet@democompany.com, thomas.barrow@ democompany.com, gerry.mordens@ democompany.com

Step Three – Tighten Password Strength

Why Passwords Matter

Passwords are a big deal for any application, service, or environment. They are even more critical for an Office 365 tenant. Whether you have a hybrid or a cloud-only Office 365 environment, you will have cloud users. In this case, Office 365 is the authentication provider for these users. That is why it is so vital to implement the right password policy to protect your users' identities and account security. Once an O365 password is cracked, the hacker has access to everything that end user does.

Doing Passwords Right

The old way of protecting passwords was to demand complexity, and require these complex passwords to be changed regularly, often every 90 days. This causes users to forget their passwords and often put them on Post-It notes to remind them – a security flaw if we ever saw one. The new approach is event-driven password changes. If there is a breach, or other security event, this is when end users should change their passwords.

CoreView tracks these events, and can automatically alert users to update their passwords. We can report on these password changes, and again, automatically alerts users that failed to take.

> *"Strong passwords are achieved by following best practices for character usage and can be enforced through password policies.*
>
> *There are several key points that you should be sure to avoid when selecting passwords:*
>
> - *Don't use a password that is the same as other websites.*
> - *Don't use single words, like "password"*
> - *Avoid commonly used phrases, like "iloveyou".*
>
> *Setting a password policy can enforce the use of stronger password security. Password policies can set minimum password lengths — for example, requiring passwords to be eight characters or longer. The policies can require the use of multiple character sets like a mix of uppercase characters, lowercase characters, numbers, and non-alphanumeric characters like $, !,#, or *."*
>
> – Michael Otey, Petri.com

Step Four – Protect User Identities Through Tough Authentication

Why Multi-Factor Authentication Matters

Multi-Factor Authentication (MFA) is one of the most important security practices you can employ. Fortunately, Microsoft Office 365 has a robust and proven MFA solution built-in. Forward-thinking organizations are implementing MFA to improve user identity security. 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. Also, the United States Department of Homeland security now recommends that all Office 365 users implement MFA.

> *"Based on our studies, your account is more than 99.9% less likely to be compromised if you use MFA,"* said Alex Weinert, Group Program Manager for Identity Security and Protection at Microsoft.

Step Five – Activate MFA!

Don’t Forget to Turn on MFA

MFA only works if it is activated. “Multi-factor authentication for administrator accounts not enabled by default: Azure Active Directory (AD) Global Administrators in an O365 environment have the highest level of administrator privileges at the tenant level. Multi-factor authentication (MFA) is not enabled by default for these accounts,” the NIST guidelines stated.

CoreView shows how many users have MFA activated, have MFA disabled, and how many users with MFA disabled have administrative roles, which presents a substantial security risk. With CoreView, it is simple for you and your administrators to monitor, set, and enforce an appropriate MFA authentication policy.

> *“MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). Your credentials must come from two different categories to enhance security – so entering two different passwords would not be considered multi-factor.”*
>
> – Nist.gov

Step Six – Secure Email – O365's Weakest Link

Button up Email Security

Are you shocked to learn that 94% of all cyberthreats start with email?

Here are more shocking email facts courtesy of the 'Mimecast 'State of Email Security 2020', which finds that:

- "51% of organizations have been impacted by ransomware in the last 12 months
- 58% saw phishing attacks increase
- 60% of organizations have experienced their own employees being responsible for spreading a malicious email"

Mailboxes are the number one way hackers breach systems, steal identities and credentials, and launch phishing and ransomware attacks. One step to take is to set access rights to mailboxes to protect data, mail content and mailbox owner identities. This can include items such as access to more than five mailboxes, auto forwarding, and accessing mailboxes of others.

Fortunately, CoreView can apply key rules for mailbox security, especially in regard to access rights. CoreView, for instance, flags user accounts that have been provided with access rights to more than 5 other user mailboxes. These are not for Room, Shared, or Team mailboxes, but rather actual User Mailbox accounts. Such cases should be investigated to ensure they are being used for acceptable business purposes.

Often, mailbox security can be compromised by spam and malicious malware. CoreView can discover the exact number of instances of malware sent by email from your organization.

Knowing the internal sources of malware is critical to stopping the spread. CoreView keeps IT informed of unusual patterns or targeting, which may be attempts to compromise mailboxes in your organization. CoreView also provides details on potentially compromised accounts and the malware which may have been sent from your organization, enabling your shop to take action to support investigations and remedy issues.

Malware often spreads from mailbox to mailbox – right under IT's nose. The answer is tracking all actions and file movement from mailbox owners hit by malware, and other unusual activity.

Monitoring Email Behavior is Critical

Monitoring employee activities such as their mailbox practices can identify risky behavior and proactively secure business-critical data. Preventing risky activities such as auto-forwarding to external email addresses and limiting access rights to other users' mailboxes can prevent the spread of malware and the leakage of data through emails. In addition, being aware of unusual email activity prevents targeted spam or social engineering tactics common among today's cybersecurity threats.

Step Seven – Don’t Forward Critical Data Away

The Danger of External Auto Forwarding

To the average end user, setting up automatic email forwarding rules is a harmless exercise. But for those whose job it is to prevent data breaches and ensure compliance, email forwarding rules can quickly turn into a nightmare scenario. The indiscriminate forwarding of emails outside of your organizational control is a common vector for information theft, as well as GDPR and similar data protection regulations violations.

CoreView can identify mailboxes that have auto-forwarding to external addresses such as “Gmail.com”. This is a major data leakage concern. These should all be reset to internal e-mail addresses or have the auto-forwarding removed completely.

Autoforwarding Attacks Explode in Wake of COVID-19

“Threat actors are leveraging fear of the current pandemic situation to carry out smishing and phishing attacks. With work from home and remote access via less or unsecured endpoints, it’s easier for threat actors to compromise an organization’s security perimeter. Consider if one gets access to a user’s mailbox, they can then auto-forward the user’s confidential email(s) to an outside address and access the individual’s and/or organization’s proprietary information.”

– CISOmag.com

Step Eight – Limit the Power of O365 Admins

Reducing the Risk of Out of Control Administrative Roles

Ensuring that O365 administrative privileges are limited to those that absolutely need them is critical to a safe Office 365 environment. An internal threat, such as a disgruntled employee, with access to global admin privileges, is a major risk that can be prevented simply by limiting the number of users with admin privileges — and restricting the scope of those permissions.

Unfortunately, Microsoft Office 365 Admin roles have limited flexibility. Microsoft offers some roles that limit administration rights on a specific workload, but these are not available across all workloads. For example, you can configure an operator as an Exchange administrator and another operator as a SharePoint administrator. The major issue with many Office 365 deployments is that administrators have global access to all the company users as well as access to all configuration capabilities for the assigned workload. Unfortunately, this permission model doesn't match with most enterprise organizations' requirements. For example, if you have a local support team in a specific country, you should limit their administrative control to users within their area of work. Or, if you have a tiered support structure, you should limit administrative rights for support staff based on their responsibilities.

Least Privilege Access Vital to O365 Safety

The concept of "least privilege" involves the practice of restricting access rights for users, accounts, and computing processes to only those resources required to perform routine, legitimate activities. This is not a new concept; in fact, adoption of "least privilege" was advanced by the publication of the "Department of Defense Trusted Computer System Evaluation Criteria" in 1985, following the recommendations of a task force dedicated to safeguarding classified data.

Step Eight – Limit the Power of O365 Admins

Get a Detailed View of O365 Admin Roles

CoreView show how many admins your shop has, and their roles. The report to the right is an example of a tenant with 178 total admins, 7 of whom also have a company admin role.

The good news is that by using CoreView, your organization can implement a granular Role-Based Access Control (RBAC) policy. This will enable your organization to assign administrative privileges to operators which appropriately matches their responsibilities.

MEMBERS COUNT FOR ADMINISTRATIVE ROLES

Role Name	Member Count
Service Support Administrator	45
License Administrator	18
SharePoint Service Administrator	17
User Account Administrator	16
Directory Readers	13
Exchange Service Administrator	12
Lync Service Administrator	8
Security Reader	8
Company Administrator	7
Reports Reader	7
Security Administrator	3
Power BI Service Administrator	3
CRM Service Administrator	3
Directory Synchronization Accounts	3
Compliance Administrator	2
Message Center Reader	2
Teams Service Administrator	2
Intune Service Administrator	2
Privileged Role Administrator	1
Teams Communications Support Specialist	1
Billing Administrator	1
Teams Communications Administrator	1
Directory Writers	1
Search Editor	1
Search Administrator	1

Step Nine – Stop Confidential Files from Leaving Your Shop

Data Leakage Through OneDrive and SharePoint Sharing

Whether your organization is large or small, sharing content with users is a powerful capability provided by Office 365 collaboration features. This is especially true when working with clients, vendors, and partners.

With SharePoint and OneDrive, users have multiple choices when they need to share documents externally:

- Shareable: Anyone with the link
- Internal: Only people in your organization
- Direct: Specific people

Shareable, also known as Anonymous Sharing, is the most insecure way to share a document since you cannot track how the link will circulate and be shared outside of your organization, and who will have access to your data.

CoreView can detect OneDrive sharing activities, SharePoint sharing activities, as well as creation and use of anonymous links. Also, with CoreView admins can be alerted when new anonymous links are created or used. You can then immediately address any problems.

Wake Up From Data Leakage Nightmare

In 2017, voting machine maker Election Systems and Software publicly exposed data of close to 2 million voters in Illinois – names, addresses, birth dates and registered party. The data leak, unlike some, was not intentional. Instead, an Amazon Web Services (AWS) cloud container was somehow misconfigured – leaving it wide open.

Data leakage is similar, and in some ways overlaps with IP theft – but instead of the data stolen by an external entity, it is leaked by an insider – either for nefarious reasons or through accident, neglect, poor configuration or lack of security oversight. For instance, a fired employee may post confidential or even damaging data online.

This is a particularly critical issue for Office 365, as a study shows that 58.4% of sensitive data held in the cloud is stored in Office documents. Another issue is mistakes made by admins. *"There has been a notable increase in errors caused by system administrators publishing sensitive data in public cloud spaces open to everyone,"* found the Verizon 2019 Data Breach Investigations Report.

Step Ten – Run a Tightly Configured Ship

Eliminate Misconfiguration and Mismanagement Danger

Gartner argues that *"Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes."* Providing proper configuration, as well as monitoring and enforcing policies, are the responsibility of Office 365 IT professionals, and is a must-do best practice to reduce your breach perimeter.

To reduce mismanagement issues, CoreView implements segregation of your tenants in many critical ways. You can separate your tenant into sub-tenants or virtual tenants. This way you can have local administrators that keep an eye on a smaller, more defined set of users. Specific policies can apply to just these user sets. Moreover, because fewer admins have global rights, end users in these sub-tenants are protected from global admin mistakes or malfeasance.

Stopping Improper Administration and Non-Compliance

With CoreView, you can monitor your configurations and usage policies, and report and alert on account and device misconfiguration. If a misconfiguration or a misusage has been detected, you can immediately remediate it as well as enforce those policies using the CoreView workflow automation capability. Moreover, with CoreView, policy management moves from a manual and error-prone process to one that is intuitive, easy and automated.

Make Misconfiguration a Thing of the Past

For enterprises, correctly defining configurations and appropriate user behaviors are best practices. However, misconfiguration is still possible due to operator workarounds or operator error. That is why it is so important to monitor and enforce your configuration best practices including policies and baselines, and that way fully secure your Microsoft SaaS environment.

CoreView defines administrators that are specific to a location, functional sets of users, or other attributes. This means admins know who their users are, and have a manageable set of end users to handle.

At the same time, CoreView tracks application usage, so you know which applications handle the most work, and when end users are misusing the system. The 'single pane of glass' CoreView console offers deep insight into how end users are configured, and where they might be misconfigured.

About CoreView

CoreView cuts the chaos and gets Microsoft 365 under control. The CoreView Microsoft 365 Management Platform helps IT teams get full value from their Microsoft 365 investment, gain full oversight of their environment, and move at full speed. More than 10 million users and the world’s largest organizations rely on CoreView to craft perfect privileges, eliminate wasted licenses, drive adoption, and automate repetitive tasks. A Microsoft Gold Partner, CoreView is Co-Sell Prioritized and available on the Azure Marketplace. CoreView | Now It’s Under Control.

CoreView
Now It’s Under Control

sales@CoreView.com
+1 (800) 436-8183
www.CoreView.com