CoreView

SaaS, Mastered.

M365 Application Security, Data Governance and Shadow IT Report

CoreView Research Indicates 50% of M365 Users are Not Managed by Default Security Policies

Introduction

MIT Center for Information Systems Research (CISR) defines IT governance as, "a framework for decision rights and accountability to encourage desirable behavior in the use of IT." MIT CISR has also found that firms with effective IT governance strategies have 20% higher profits than their competitors.

Simple enough, right?

Many businesses underestimate the security and governance responsibilities they take on when they migrate to Microsoft 365 (M365). In theory, it's easy to establish a framework for critical IT-related decisions, such as data governance, securing business applications, and prioritizing IT investments and principles. However, many organizations struggle with these fundamental tasks due to three common mistakes:

1. Failing to implement basic security practices;
2. Giving administrators excessive controls, resulting in increased access to sensitive information; and,
3. Investing in productivity and operation applications without considering security implications.

With today's modern workforce increasingly working from home, it's more important than ever to prioritize security and data governance in M365.

Methodology

To understand how enterprises are employing application security and data governance initiatives, CoreView analyzed more than five million workers from enterprises that are actively using its SaaS Management Platform (SMP); have undergone a complimentary CoreView Office 365 Health Check analysis; or are using the free CoreDiscovery solution that discovers opportunities to strengthen AppSec and data governance. Read on for a breakdown of the full report, including three core findings.

Finding #1: Global enterprises aren't widely implementing basic security practices in their M365 environments

97%

of total M365 users do not use MFA

Cyberattacks on M365 often manifest as email-based phishing or spear phishing attacks, automated credential stuffing, or guessing attacks. Multi-factor authentication (MFA) is one of the best ways to prevent this type of unauthorized access to M365.

Unfortunately, CoreView's data indicates that approximately 78% of M365 administrators do not have MFA activated. This is a huge security risk – particularly during a time where the majority of employees are remote – that IT departments must acknowledge and address in order to effectively deter cyberattacks and strengthen their organization's security posture.

Breaking basic security practice data from CoreView down further, we find:

- 97% of total **M365 users** do not use MFA. This is unfortunate given research from SANS Software Security Institute indicates that 99% of data breaches can be prevented using MFA.
- 50% of enterprise **M365 users** are cloud users, meaning they are not managed by on-prem policies. Well-defined, cloud-based policies for passwords, authentication, etc., must be established and maintained as business continue their acceleration to the cloud.
- 1% of **M365 amins** don't use strong passwords. While this may seem like a small percentage, medium-sized **enterprises** have 50 to 249 employees on average and large enterprises employ 250 or more people. Meaning, these organizations have between eight and forty-two employees that are leaving the business vulnerable to attacks.
- 1 in 5 users on enterprise M365 environments are a **guest user**.
- **70% of guest users are inactive**, which creates unnecessary risks and costs to the organization, and should be removed.

Finding #2: Administrators have excessive permissions, resulting in increased access to sensitive information

57%

of global organizations have M635 administrators with excess permissions to access, modify, share critical data

Research indicates that roughly 80% of data breaches involve privileged credentials, so setting appropriate admin controls should be IT's first job when giving access to employees.

Unfortunately, there is a gap in security controls regarding Microsoft 365's Azure Active Directory (AD). In enterprise organizations with hybrid environments, Azure AD's policies are dictated, by default, by on-prem rules. This creates a huge security threat for the organization, as cloud user identities (16% of users in this case) are not managed by on-prem policies. Organizations must implement well-defined, cloud-based policies for Azure AD to protect all of its user identities.

CoreView's data also shows that some users are forwarding internal communications, including email and additional resources and documents, outside of their organization. While collaboration with external partners is an ordinary business function, most organizations don't have any visibility into who their employees are communicating with and what their employees are sending. This is huge data breach risk since the organization immediately loses ownership of its data.

Breaking data from CoreView down further, we find:

- 57% of global organizations have **M635 administrators with excess permissions to access, modify, share critical data**
- **17% of M365 admins are Exchange admins**, meaning they can see and do whatever they want on any employee's inbox, including the CEO's
- **36% of M365 admins are Global Admins**, meaning these admins can essentially do whatever they want in M365. Microsoft suggests limiting the number of Global Admins to two to four operators max per business.

Finding #3: US companies are investing in productivity and operations applications more than any other area of business, which opens the door to preventable cyber-attacks

Shadow IT is clearly ripe for attack, as Gartner researchers predict that 1/3 of all successful attacks on enterprises in 2020 will be against Shadow IT resources.

To ensure productivity in the workplace (remote or on-prem) it's crucial that organizations offer innovative technology that empowers employees to communicate, collaborate, and produce with agility. In recent months we've experienced an unprecedented surge in the adoption of digital technologies which are transforming every aspect of business. This proliferation has greatly impacted the rise of Shadow IT, otherwise known as the (mostly) SaaS applications that employees use, typically without IT permission or even knowledge.

CoreView data shows that US enterprises collectively utilize more than 1,100 different productivity and operations apps, which indicates a strong dedication to the growing needs of business across departments, locations, and time zones.

While increased access to productivity and operations apps helps fuel productivity, unsanctioned shadow IT apps have varying levels of security unsanctioned apps represent a significant security risk. Shadow IT is clearly ripe for attack, as Gartner researchers predict that this year, 2020, one-third of all successful attacks on enterprises will be against Shadow IT resources.

At a basic level, malicious apps can siphon off critical data. Users could also potentially be sharing sensitive company information through these apps to compromised parties, putting organizations at a substantial risk of a data breach. It's vital that organizations properly monitor these apps for potential security gaps.

Conclusion

CoreView helps organizations properly manage and secure M365 by identifying gaps in app security, data governance and Shadow IT best practices.

In today's modern work environment, where supporting remote work is a must, CoreView's data indicates that the missing ingredient in deploying and using M365 effectively is often data governance, application security and Shadow IT oversight. Enterprises must ensure they have the processes and tools, including CoreView, to help securely migrate and operate the world's leading SaaS productivity platform.

CoreView provides actionable insights, detailed forensics, and governance controls that help businesses not only set policies for rollout and usage, but also to counter security risks. CoreView can instantly identify and fix common security issues that account for most breaches, including alerts and reports of breach attempts, email forwards, external file sharing, mailbox security risks, and more.

CoreSaaS enables enterprise IT teams to discover Shadow IT products in the cloud, manage costs and renewals, increase security and compliance, and automate processes. Currently, CoreSaaS offers 26 native integrations for advanced management and monitoring.

CoreView helps organizations properly manage and secure M365 by identifying these types of app security, data governance and Shadow IT gaps. For more information on how to improve security of your organization's M365 instance, please visit www.coreview.com.