Office 365 Security Pain Points – The People Problem

Eight Ways People Threaten Your O365 Environment, and What to do About it

PART FOUR IN A FOUR PART SERIES

CoreView

Office 365 Security Pain Points – The People Problem

People come in all sorts: Most are good, but others have bad intentions, or are just plain negligent.

Protecting your Office 365 tenant means safeguarding it from bad internal and external actors, and insuring that simple thoughtlessness doesn't turn into a security disaster.

Here are eight ways people wreak Office 365 havoc, and how to handle negligence and block malfeasance.

If your future involves the Cloud and SaaS, you really should talk to CoreView.

We offer delegated administration and role-based access control built for your network today – and tomorrow.

The People Problem

1. The Pain: Poor O365 Identity Management

Credential cracking and elevation of privilege attacks demonstrate that we must treat identity as a primary security perimeter. This is a shift from the traditional focus on network security. Network perimeters keep getting more porous, and that perimeter defense cannot be as effective as it was before the explosion of BYOD devices and cloud applications.

Both types of attacks exploit the risk of granting too many global privileges. In fact, CoreView has rewritten the rules for RBAC in the Office 365 world. The new best practice is to segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Office 365 tenant, allow only certain actions at a particular scope.

There are other identity management issues, many of which were settled in the on-premises world but have to be readdressed in the world of SaaS and hybrid networks.

If your future involves the Cloud and SaaS, you really should talk to CoreView. We offer delegated administration and role-based access control built for your network today – and tomorrow. Our user provisioning and lifecycle management of identities are built for modern cloud and hybrid environments.

While we serve your user management and identity needs, we go far further. There is so much we do that Azure AD doesn't – such as finding malicious log-in attempts, sign-ins from infected devices or from out of the norm geographies. We also track end user activities relative to Azure, and provide rich auditing and reporting.

That is the tip of the CoreView end user and identity management iceberg. At the same time, CoreView offers deep Office 365 management, security and helps your end users more fully adopt O365 services.

CoreView has rewritten the rules for RBAC in the Office 365 world. The new best practice is to segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

Instead of giving everybody unrestricted permissions in your Office 365 tenant, allow only certain actions at a particular scope.

The People Problem

2. The Pain: The Problem With Ex-Employees

There is little more dangerous than an ex-employee – except an employee who is soon to leave and wants to create damage or take confidential competitive information with them when they go.

An all too common scenario is to have a current employee planning to go work for a rival company. The key is their knowledge and experience of the market, but also any of your confidential data they can steal such as customer lists, contracts and product plans. An active employee may be forwarding all their emails to personal accounts and share files externally to themselves and new business partners. If you were tracking email forwards and external data sharing, you would spot this data theft before it gets out of hand.

If IT learns an employee is leaving, and has given, say, two weeks' notice, the antenna should go up. This is the time to make sure there is no external sharing of confidential data, or other sketchy activity.

Once a worker leaves, forensics should kick in to insure nothing untoward has happened, and if it did, action can be taken. With CoreView, every time an employee leaves the organization, IT can run an audit report of every file accessed for the past whatever number of days, email forwarding to non-company accounts, and sharing data such as OneDrive volumes externally.

3. The Pain: Stale Mailbox Rights

A common scenario is sharing calendar or mailbox access with other colleagues, the problem is that no one is taking care of removing this access — if this is not done by the owner of the shared resource.

Access to resources is usually needed for a limited amount of time, and you should ensure that this principle is applied. When access is granted to final users and it's removed only when a person leaves the company or reminds IT to remove it – this potentially opens security breaches which are not monitored by anyone.

CoreView helps governance of this process through a workflow, where a user can ask for resource access to target users for a limited amount of time and the workflow will remove it automatically after it expires.

With CoreView, every time an employee leaves the organization, IT can run an audit report of every file accessed for the past whatever number of days, email forwarding to non-company accounts, and sharing data such as OneDrive volumes externally.

The People Problem

4. The Pain: Stale External Users

Digital interactions between different companies is the core of productivity. Employees share files with external users, invite them to share in Teams chat or meetings, and add them to distribution groups every day.

Usually these interactions are limited in time, and the external user accesses a resource for a specific project or moment in time and then goes back to his normal activity. Unfortunately, this guest account is still active in the tenant and he can log-in whenever he wants.

What happens if his account is breached several months after invitation? The attacker will be able to access shared resources, read emails exchanged, and act on behalf of the real users.

What happens if the employee who invited him leaves the company? Who is responsible for removing the guest user from the tenant? Probably it will remain there forever.

CoreView addresses all these problems through a workflow that can be used to force users to add detailed information when an external user is invited such as department, company, manager, country and a validity. CoreView will take care of removing the invited user or renew it based on a customizable approval process.

CoreView automation can also be used to identify external users inactive in the last 60 days and automatically start a process of cleanup with approval.

Any external user is an additional endpoint to your tenant – keeping them active indefinitely is a common bad practice that can be easily addressed with CoreView.

CoreView automation can also be used to identify external users inactive in the last **60 days** and automatically start a process of cleanup with approval.

5. The Pain: Weak Authentication

Hackers have raised password cracking to an art form. With so many weak passwords, it doesn't take a rocket scientist to break them. The answer is multi-factor authentication (MFA). In fact, US government Office 365 security guidelines strongly advise MFA, especially for admins.

"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 advisory stated.

Locking down end-user accounts through secure passwords and rigorous authentication is also essential. MFA requires at least two forms of personal user identification and is recognized by the National Institute of Standards and Technology (NIST) guidelines for password security. The United States Department of Homeland Security now recommends that all Office 365 users implement MFA. Microsoft provides tools such as Microsoft Authenticator for users to install on their smartphones, as well as Smartcards, to work in combination with pass worded logins. Multi-factor authentication is a surefire way to prevent unauthorized logins, and there is little excuse not to use it.

The United States Department of Homeland Security now recommends that all Office 365 users implement MFA.

Microsoft provides tools such as Microsoft Authenticator for users to install on their smartphones, as well as Smartcards, to work in combination with pass worded logins.

The People Problem

6. The Pain: Too Little Attention Paid to Azure AD Security

Azure is the host to Office 365 and a key way end users are identified in the cloud. This also makes Azure and Azure AD the main thoroughfare for cybercriminals making their way into the network.

A piece by Microsoft: Azure Identity Management and Access Control Security Best Practices, lists a handful of tips, including:

- "Treat identity as the primary security perimeter
- Centralize identity management
- Manage connected tenants
- Enable single sign-on
- Turn on Conditional Access
- Plan for routine security improvements
- Enable password management
- Enforce multi-factor verification for users
- Use role-based access control
- Lower exposure of privileged accounts"

Fortunately, this checklist is a roadmap of many CoreView security features. One key item is CoreView's Azure Activity Reports, which include:

- Application usage: summary and detailed reports
- Application dashboard
- Detailed audit logs
- Account provisioning errors
- Individual user devices and activity
- Groups activity reports
- Password reset activity

One key item is CoreView's Azure Activity Reports, which include:

Application usage: summary and detailed reports

Application dashboard

Detailed audit logs

Account provisioning errors

Individual user devices and activity

Groups activity reports

Password reset activity

The People Problem

With Azure monitoring and reporting, customers audit and report on suspicious login activity, different device access methods and DLP activities, and perform security and compliance auditing, all from a common management interface. These capabilities also allow customers to configure automated alerts to notify administrators when security compliance issues with Azure AD are identified. In total, CoreView now allows auditing and alert notifications based on over 500 actions in Office 365 and Azure AD.

One of the biggest items is tracking AD suspicious sign-in activity. The Azure AD security monitoring and auditing reports available in CoreView provide the proactive, bloodhound type trail to sniff-out suspicious activities for user account log-ins. Many security breaches come from botnet driven brute-force attacks on user accounts by trying different password combinations until they gain access over time. This was the method used by the "KnockKnock" attack which targeted Office 365 system accounts. Add to this the ShurL0ckr type attacks in 2018 that are still ongoing and infect OneDrive collaborate storage folders, and you can see how IT admins have their hands full with monitoring security breaches and infestations.

Monitoring suspicious sign-in activities on user accounts has quickly become a critical security task for IT administrators responsible for managing Office 365. The customizable reports from CoreView enable IT admins to easily monitor these suspicious activities, identify who performed the sign-in, when it happened, and from what geographic location (which IP address). The anomalous AD activity reports combine suspicious sign-in details from the following categories:

- Sign-ins from unknown sources
- Sign-ins after multiple failures
- Sign-ins from multiple geographies in the same days/weeks
- Sign-ins from IP addresses with suspicious activity
- Sign-ins from possibly infected devices
- Irregular sign-in activity

The anomalous AD activity reports combine suspicious sign-in details from the following categories:

Sign-ins from unknown sources

Sign-ins after multiple failures

Sign-ins from multiple geographies in the same days/weeks

Sign-ins from IP addresses with suspicious activity

Sign-ins from possibly infected devices

Irregular sign-in activity

The People Problem

In fact, CoreView can easily establish and manage AD identities, and have this work automated in a pre-set, serial workflow process with full auditing implemented by default. Here are the steps that can be automated, and done without error:

1. **Import New User List** – into CoreView processing queue using a CSV file
2. **On-Premises Account Creation** – in the on-premises Active Directory using the CoreView Hybrid management functionality
3. **Azure AD Account Creation** – setup synchronized accounts in the cloud
4. **O365 License Assignments** – based on department and job role profile
5. **Addition to Office 365 Groups**
6. **Policies Assignment for Various Services**
7. **E-Mail Sent to Manager With Temporary Password**
8. **Preconfigured Welcome Message Sent to New User** – containing links to onboarding materials and training portal
9. **New User Account Included in Virtual** – Tenant for Associated Business Unit

CoreView can easily establish and manage AD identities, and have this work automated in a pre-set, serial workflow process with full auditing implemented by default.

7. The Pain: Not Monitoring Suspicious Sign-in Activity for Office 365

Knowing how many suspicious sign-ins attempts are happening, where they are coming from, and what they are targeting is a key security best practice. Unfortunately, this is difficult work if all you have is the native O365 Admin Center from Microsoft.

Many breaches come from botnet driven, brute-force attacks on user accounts by trying different passwords combinations at segmented intervals until they gain access over time. This was the method used by the "KnockKnock" attack, which successfully targeted Office 365 system accounts. The Azure AD security monitoring and auditing reports available in CoreView provide the type of proactive, fast analysis capabilities to quickly sniff-out suspicious activities for user account sign-ins. *Identifying those hackers early on allows IT teams to quickly block those IP addresses and enable extra security to any of the accounts that are being targeted.*

This is extremely helpful for distributed organizations with multiple sites and geographic locations. One enterprise organization we talked to said that they have improved their response time to block remote hacker attempts by over 500%. One customer based in the mid-western US said that they used to spend approximately 80 hours/month running their own PowerShell scripts and sifting through the piles of data to search for anomalous sign-ins across their different geographic locations. Now they spend about 10 hours/month monitoring for suspicious sign-ins and can take immediate action when they find an issue.

> Identifying those hackers early on allows IT teams to quickly block those IP addresses and enable extra security to any of the accounts that are being targeted.

The People Problem

Here are suspicious sign-ins tracked by CoreView:

Sign-Ins From Infected Devices

This report showcases the account logins that were performed from infected devices that are now part of a botnet. We correlate IP addresses of user sign-ins against IP addresses that are known to be in contact with botnet servers. These are important to quickly identifying users infected with malware or other infestations that need immediate remediation. These reports are completely customizable.

Sign-Ins From IP Addresses With Suspicious Activity

This report shows sign-ins from IP addresses where suspicious activity has been detected. Suspicious activity in this case is defined as an unusually high ratio of failed sign-ins to successful sign-ins, which may indicate that an IP address is being used for malicious purposes.

Sign-Ins From Multiple Geographies

This report includes successful sign-ins for the same account where two sign-ins appeared to originate from different geographical regions during a specific timeframe. The report takes into consideration the time difference between the sign-ins to provide more details to the administrator so they can determine whether it was possible for the user to have traveled between those regions.

Impossible Travel Sign-Ins

These types of questionable sign-ins are identified on the basis of an "impossible travel" condition combined with an anomalous sign-in location and device. This means that a successful sign-in occurs from a single account over multiple geographic locations in overlapping time sequences. This may indicate that a hacker has successfully signed in using this account.

Here are suspicious sign-ins tracked by CoreView:

Sign-Ins From Infected Devices

Sign-Ins From IP Addresses With Suspicious Activity

Sign-Ins From Multiple Geographies

Impossible Travel Sign-Ins

8. What the Chief Security Officer Does Not Know – Hurts

So what do security IT executives need to know about security that they don't already? "It is a delicate conversation. How do you tell them? – 'You have been operating unsafely for four years and should have been examining every file that got touched after a malware event.' It is going to happen. If it happens to the US Department of Defense, you will be hacked too. Somebody will get a virus. Somebody will leave the organization and not be 100% happy that they are leaving. Some administrator will do something they should not. Why haven't they turned on all these controls?" said Matt Smith, solution architect for CoreView.

The best advice for an Office 365 environment of any size is to get a free CoreView Office 365 Health Check today. At the same time, make sure you have enabled all the data Microsoft has to offer for detecting and correcting a security event. Then subscribe to the CoreView solution so you can rationalize all that information into actionable reports.

"A huge benefit of having a CoreView Office 365 Health Check scan and analysis performed on your entire O365 environment is that auditing is not turned on by default by Microsoft. Many people do not realize this. When we do an Office 365 Health Check, we flip on auditing for every single workload. Even if they do not buy CoreView, it is a value add in that at least all that data is there," Smith concluded.

Office 365 Specific Security Essentials

Every IT shop worth its salt has at least a few layers of security – anti-virus/anti-malware, firewalls, maybe some intrusion detection and prevention systems. However, Office 365 adds an array of SaaS-specific openings that hackers are more than happy to exploit.

Key Office 365 security best practices include password policy, multi-factor authentication, mailbox security, and file storage security. Proactively establishing best practices in these areas dramatically reduces security risks.

Ensuring that 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.

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.

Learn How CoreView Protects Your Environment, and More

Get Started with CoreView – for Free

Our new CoreDiscovery solution will help admins understand, manage, secure, and drive application adoption for their O365 tenant. Learn more on the CoreDiscovery product page: https://www.coreview.com/corediscovery/.

Get your free software at the CoreDiscovery sign up page: https://www.coreview.com/core-discovery-sign-up/.

Want to learn how CoreView prevents overspending on licenses, underusing applications, or mismanaging security and configurations? Our free CoreView Office 365 Health Check diagnoses all your Office 365 problems. Sign up for an Office 365 Health Check and we will build a detailed 20-page report to cure all your Office 365 ills.

Not ready for a full custom report? You can still take a look at a Health Check sample report.

Want to see firsthand how CoreView solves Office 365 problems and tightens security, just request a demo.

Sign up for an Office 365 Health Check and we will build a detailed 20-page report to cure all your Office 365 ills.