Office 365 Security Pain Points – Data Protection and Data Breaches

Six Data Disasters Waiting to Happen

PART ONE IN A FOUR PART SERIES

CoreView

Office 365 Security Pain Points – Data Protection and Data Breaches

Many novice Office 365 shops do not know where O365-specific security vulnerabilities lie, or that they even exist. These threats do not cause pain until they rise up and bite – then the agony is fierce.

More experienced organizations know threats exists, but not exactly where they are or how to address them. The results can be disaster. A survey of 27 million users across 600 enterprises found that 71.4% of Office 365 business users suffer at least one compromised account each month.

Virtually all organizations have some basic forms of security protection, such as anti-virus and firewalls – but nothing for Office 365-specific security issues. The basic tools they have make them feel safe. Meanwhile, larger shops likely have defense-in-depth for general security and compliance and regulatory controls and solutions – but again, nothing for Office-365 specific security and compliance concerns.

This is a thorn in the side of Office 365 IT pros. Osterman Research surveyed Office 365 IT managers and found these pain points and areas of administrative weakness:

- "Monitor for and block access from compromised accounts 80% responded yes
- Audit, manage and control privileged access into Office 365 applications 71% responded yes
- The ability to centrally manage security policies across all communication channels, both within Office 365 and on other platforms 57% responded yes"

While Office 365 does come with some security features and configuration options – and all O365 shops should take advantage of them, native or built-in tools do not address many vulnerabilities and issues such as those raised by Osterman.

The good news is that CoreView solutions handle all of Osterman's concerns – and more. CoreView manages well over 7 million Office 365 end points, and knows exactly where the pain and problems lie, and how to neutralize threats and achieve compliance.

Here are six Office 365 data protection and data breach pain points – and how to relieve the discomfort.

Osterman Research surveyed Office 365 IT managers and found these pain points and areas of administrative weakness:

"Monitor for and block access from compromised accounts **80%** responded yes

Audit, manage and control privileged access into Office 365 applications **71%** responded yes

The ability to centrally manage security policies across all communication channels, both within Office 365 and on other platforms **57%** responded yes"

Data Protection and Data Breaches

1. The Pain: Sensitive Files are Shared Externally

With native Office 365 security, intercepting the sharing of sensitive and confidential files is nearly impossible. IT can create alerts on a per file basis or per user basis and notify IT or a group of users – but this approach is ineffective. IT receives thousands of alerts per day: these new alerts are just extra noise in an already loud world.

In a CoreView world, when a user from the sales department, for instance, (CoreView's unique enriched audit log grants the capability to identity users by location or department) shares a file with an external user, a workflow starts. This notifies the user sharing the file, his/her manager, and the external user that this activity has been logged, and any following activities on the file will be audited. In this case, IT is not even involved, responsibility is shared among all actors involved and security is increased.

OneDrive being shared with external users is a particular pain point and security threat, and is something CoreView easily addresses.

2. The Pain: Intellectual Property (IP) Theft

Companies that develop products, conduct research, or have leading edge business practices rely on critical intellectual property. Your competition, and a good many hackers – even foreign entities, would love to steal this hard-won information.

CoreView blocks IP theft, and if it does somehow occur, helps IT figure out what the heck happened by performing forensics on IP theft.

IP theft events occur for two main reasons – either an external threat or an internal threat. To CoreView, external and internal threats are the same. The solution logs internal threats the same way it does external threats – and treats them with the same level of security.

When it comes to IP theft prevention, one CoreView report is particularly critical – sign-in fails. CoreView builds a map that displays where sign-ins are coming from across the globe. A customer may have people in North America and EMEA, but nobody in Southeast Asia – so sign-ins from that region are clearly suspicious and need to be flagged. CoreView also has long-term maps – such as showing 90 days' worth of failed sign-in data. "Security professionals tell me they know people are trying

CoreView blocks IP theft, and if it does somehow occur, helps IT figure out what the heck happened by performing forensics on IP theft.

IP theft events occur for two main reasons – either an external threat or an internal threat. To CoreView, external and internal threats are the same. The solution logs internal threats the same way it does external threats – and treats them with the same level of security.

to sign-in from China, Indonesia, India, and so forth," said Matt Smith, solution architect for CoreView. "They are telling the truth – they do. Where we are different, is CoreView shows precisely what accounts they are targeting from the application perspective, not just the network perspective. CoreView, thanks to its unique enrichment capability, shows what users, departments or even privileged accounts, hackers are targeting. In addition, what measures have been put in place, such as if they have multi-factor authentication or not, as well as conditional access policies that were utilized to try to block them from gaining access. And, at the end of the day, what was the actual sign-in failure reason?"

With CoreView, IT can block these breaches by only allowing log-ins from allowed locations. If a user account is attacked this way, CoreView will know it and can investigate. Moreover, a CoreView-equipped Office 365 administrator can reach out to the user that was targeted, perform a workstation refresh, find out what other devices they are using, and what licenses they have on other devices, among other items.

These insights and reports are schedulable. "What we are trying to do from a security standpoint is operationalize these reports and create daily, weekly, monthly and quarterly touchpoints. The daily touchpoints are items we surface through the CoreView management console. Items like devices with malware. IT can get a daily report showing if a device shows up with malware. You can then run an additional report that shows the files that user accessed since malware was detected on their account," Smith explained.

For full IP protection, IT needs reports showing who was provisioned incorrectly so it can perform proper configuration management, if there are mobile devices that did not have an MDM policy applied, or which members of a department's executive team did not get litigation hold enabled. "That is how we apply both the forensic capability and the blocking capability to our data repository to give you insights into exactly what is going on, and reduce the number of signals so they are actually consumable by O365 administrators," Smith said. "Plus, if CoreView finds a sign-in from an infected device in our report, you can link that to an audit report that shows that particular user and everything that they have accessed since that malware was detected."

> "CoreView, thanks to its unique enrichment capability, shows what users, departments or even privileged accounts, hackers are targeting.
>
> In addition, what measures have been put in place, such as if they have multi-factor authentication or not, as well as conditional access policies that were utilized to try to block them from gaining access.
>
> And, at the end of the day, what was the actual sign-in failure reason?"

3. The Pain: Data Leakage and Poor Data Prevention (DLP)

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 are 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.

Users who normally have access to data as part of their jobs, such as client account spreadsheets, aren't triggering DLP rules. Fortunately, CoreView records this access for review at critical events such as legal requests and HR events such as separation.

CoreView knows where sensitive data rests, who has access and what they do with it. "The first thing I show about security is the landing page in the CoreView dashboard, and explain how we collect security-related data. The real power of the platform is not that we have pretty charts and graphs, it is the security data we collect in a unique way that nobody else can do," Smith said. "We connect to Office 365 via every available API. There is a Graph API, most IT professionals working with Office 365 know about that. We also take the audit log push from Microsoft and that allows us to gather and analyze the same data as Splunk and the new Microsoft Azure Sentinel."

CoreView dives into every one of the application APIs. Exchange has Exchange web services for example. Skype has activity logs, and SharePoint and Teams all have their own APIs. Finally, CoreView gets data from Azure Active Directory (Azure AD). All this data is stored externally in a Microsoft Azure subscription. "The data never leaves the Microsoft platform. You are not pulling it across the internet, not pulling it down to the desktop, not sending it over to Amazon Web Services. It all stays within Azure. Because Office 365 runs on Azure, and CoreView runs on Azure, it stays in the Microsoft data centers.

Users who normally have access to data as part of their jobs, such as client account spreadsheets, aren't triggering DLP rules. Fortunately, CoreView records this access for review at critical events such as legal requests and HR events such as separation.

With CoreView, IT knows every single transaction that occurs within the Microsoft platform, and the configuration information. That means IT knows when a document is created, when it is replicated to Office 365, when it is accessed, and when it is changed.

Data Protection and Data Breaches

"You can store that data for as long as you want, and enrich the data as it comes in. Since you have data from all these different sources, you can use the audit log to get a deep view. For instance, you will not just know that it was 'Joe User' who accessed a file in OneDrive, but understand the complete path to the file – how he accessed it, with what mobile device, and what MDM policy his mobile device had, including who 'Joe User' was: department, country, company as well as administrative roles in the tenant. Also when did he it, and from what IP address," Smith said.

With CoreView, IT knows every single transaction that occurs within the Microsoft platform, and the configuration information. That means IT knows when a document is created, when it is replicated to Office 365, when it is accessed, and when it is changed. CoreView stores all of that information externally in an immutable (meaning it cannot be changed) database. That, in essence, is the complete block chain information for every single transaction in Office 365.

4. The Pain: Cannot Stop Data Breaches

Ponemon's 'Cost of a Data Breach' Survey sponsored by IBM explains the damage of data breaches best. What is the cost of losing a file? They say $141. The average cost to an enterprise of a breach – $3.62 million. It is about 191 days on average to figure out that you have had a data breach.

The best defense is stopping breaches before they happen. Finding and retaining trusted IT talent is a critical security component. "An IT study says over 50% of the data breaches are because we did not configure things correctly. That leads to the two poor IT people in the basement who have to do everything. Alternatively, we had to give out global administrative rights to 167 people and just pray they do not press the wrong button," Smith said.

From a prevention standpoint, CoreView takes the signals that Microsoft provides and greatly enriches them. For instance, CoreView has a global suspicious sign-in attempt map showing not only what IP address hackers were attacking from and failed, but also what accounts they went after. It also shows if the configuration included multi-factor authentication or not, and whether or not conditional access policies were effective for a specific attempt. Finally, it details the end-result of the sign-in attempt.

The average cost to an enterprise of a breach – **$3.62 million**. It is about **191 days** on average to figure out that you have had a data breach.

5. The Pain: Cannot Figure Out Why a Data Breach Happened

Let's face it. Breaches sometimes bust through the best barriers. And most IT shops discover the incursion months or even over a year after it happened. How then do you figure out how and why it happened?

The answer is forensics that rely on long-term log data quality and retention so you can perform a proper security audit. Here you discover what happened so you can minimize ongoing damage, and by finding the source, stop it from happening again.

This point speaks directly to CoreView's auditing capabilities. "If I do not know what is going on, then how on earth do I investigate issues? One core security pillar is 'know thyself'," said CoreView's Smith. "From a Microsoft perspective, they keep application data for 30 days, and just announced that they will increase this to one year, but only for E5 licenses. How can I be effective if I cannot even tell you who signed in a year ago?" The answer is that IT should keep records on access attempts for as long as they have the O365 platform.

Once a data breach or malware infection occurs, you need to find out everything about it. That is where basic security tools fall short. "From a forensic standpoint, anti-virus will tell you that Joe's PC had a virus on Monday. However, there is no anti-virus platform in the world that shows exactly what he touched since he got that virus," Smith said.

CoreView, though, quickly gets to the heart of the matter. A CoreView-enabled administrator can choose 'file access' and see all the files, the names, and the paths to the files that were accessed after the breach or malware attack. "CoreView can save off these reports as well. The next step is to track where the malware may have spread. For instance, you can see all the files people have accessed within the OneDrive platform where the malware may have landed. These people are now suspected of having malware because one particular user touched this file after he was reported as having malware. The last thing an admin can do is look at OneDrive reports and then external invitations," Smith argued.

A CoreView-enabled administrator can choose 'file access' and see all the files, the names, and the paths to the files that were accessed after the breach or malware attack.

Data Protection and Data Breaches

6. The Pain: E-Mail Hacks

E-mail is the most common way hackers breach your systems, so insecure mailboxes and poor e-mail user practices are perhaps your biggest security exposure. Mailboxes are made vulnerable through insecure, weak and never expiring passwords, as well as a lack of multi-factor authentication (MFA).

Meanwhile, 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 user's 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.

Key rules applied to mailbox security relate to access rights. CoreView flags user accounts with anomalous permissions such as with access rights to more than five other user mailboxes, accessing mailboxes of other departments, disabled accounts able to access mailboxes and more. These are not for Room, Shared, or Team mailboxes, but rather actual User Mailbox accounts. Users who have this type of advanced access rights to other users' mailboxes 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 instances of malware sent from your organization via e-mail – and track this spread in minute detail.

Seven Ways to Know You Are On Top Of Office 365 Security

1. You can produce a log in seconds for every administrative action taken in Office 365 since the platform was initiated. (If a bank teller has a transaction log of every deposit and withdrawal, why don't we have this for O365?)

2. Every time an employee leaves the organization, IT runs an audit report of every file accessed for the past x days. And...

3. Whenever malware or leaked credentials are detected on an employee device, IT runs an audit of every action taken by that user in O365 since malware was detected, which also checks for Trojan horses/ransomware/configuration changes.

4. IT not only knows where O365 attacks are coming from, but whom they are targeting, how the targets are configured, and if successful, all actions that were taken.

5. IT has a fully-deployed least privilege access model for Office 365. And IT can describe precisely what functions those operators can perform, and how they are scoped.

6. IT can perform (report/alert/fix) desired configuration management at the account/device level in Office 365.

7. IT knows how their O365 configuration security posture compares with their peers, and how their Secure Score is trending over time.

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.