ActZero

Securing the Microsoft Cloud

from Azure to M365

CONTRIBUTORS:

Adam Mansour
Virtual CISO &
Head of Sales Engineering

Jerry Heinz
Head of Engineering

1 Introduction:
Popular with businesses & cybercriminals alike

Microsoft offerings are an increasingly common component of many organizations' transition to the cloud. A 2021 analysis by Forbes on the global market shows Microsoft steadily gaining ground on the competition, reaching a 20 percent share of the worldwide cloud market for the first time in 2020. Forbes reports that "63 percent of enterprises are currently running apps on Microsoft Azure," and that "6 percent of enterprises are spending at least $1.2 million annually" on Azure.

This ubiquity makes Microsoft 365 (formerly Office365 or o365) and Azure especially attractive vectors for threat actors, in both widely targeted and surgically specific attacks. Not to mention lucrative: Microsoft says that 95 percent of Fortune 500 companies "rely on Azure for trusted cloud services." Add this financial motivation to the typical challenges of SaaS and IaaS — plus an increasingly distributed workforce and network — and we see a "perfect storm" for threat actors to take advantage of, as evidenced by recent attacks making news headlines.

In late 2019, a sophisticated phishing campaign targeted corporate 365 users, giving bad actors "full access to a user's data stored in the cloud without actually stealing the account password" — all through an official Microsoft login page. In December 2020, Reuters reported that an unusual "cybersecurity advisory" was issued by the U.S. National Security Agency, detailing "how certain Microsoft Azure cloud services may have been compromised by hackers and directing users to lock down their systems."

As Gartner put it in a 2019 report, “CIOs must change their line of questioning from ‘Is the cloud secure?’ to ‘Am I using the cloud securely?’” This is just as true today, and is the focus of this white paper. How can you harden your cloud security posture? How will you ensure that you can detect and respond to compromises? How are you parsing security logs and alerts from cloud applications or infrastructure? **This paper is intended for technical stakeholders across IT**, such as cloud/datacenter architects, frontline service desk personnel, security analysts consuming logs from cloud sources, and CISOs formulating policy and security controls around 365 and Azure. We will discuss the following topics from ActZero’s area of expertise, detection and response:

- **HOW** cloud compromises serve as effective stepping stones to other parts of one’s environment.
- **WHY** the cloud is so challenging to secure, and how this makes your detection and response capabilities more important than ever before — especially when it comes to remote employees.
- **SPECIFIC EXAMPLES** of threats and exploits targeting your Microsoft investments, and use-cases for securing them.

2 Microsoft cloud compromises serve as stepping stones

"Every day, we see attackers mount an offensive against target organizations through the cloud and various other attack vectors with the goal of finding the path of least resistance, quickly expanding foothold, and gaining control of valuable information and assets," writes Microsoft.

In March 2021, hackers compromised the California State Controller's Office — an agency that administers over $100 billion a year — after a single employee was tricked into inputting their login credentials via a phishing link. KrebsOnSecurity reports the criminals responsible gained system access for 24 hours, and in addition to stealing thousands of Social Security numbers, they used the time inside to direct targeted phishing attempts at thousands of other employees. "Intruders also had access to the phished employee's Microsoft Office 365 files — and potentially any files shared with that account across the state network."

This breach demonstrates how **one mistake by one user** can rapidly compromise countless others, enabling rampant spread across the organization. And such phishing attacks are growing in sophistication, to the point that even trained and alert employees can fall victim to them. Now, phishing emails don't just look like they come from seemingly verified users — they can literally come from reputable sources within your 365 environment, but with malicious hackers behind them.

Microsoft itself warns of this risk in a post from March 2021. The company explains how a single compromised 365 email account can snowball into a larger problem: "The attacker can sign in as the original user and perform illicit actions. Using the stolen credentials, the attacker can access the user's Microsoft 365 mailbox, SharePoint folders, or files in the user's OneDrive. One action commonly seen is the attacker sending emails as the original user to recipients both inside and outside of the organization." (See our post "The Perfect Phishing Email" for more on this developing threat.)

3 Why the cloud is so hard to secure

According to CSO, cloud usage data from the first four months of 2020 shows that Microsoft Teams — a communications tool part of 365 — saw a 300 percent increase in use. In April 2020, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an official alert specifically to organizations migrating to the 365 cloud. "Due to the speed of these deployments, organizations may not be fully considering the security configurations of these platforms," wrote CISA. "CISA encourages organizations to implement an organizational cloud strategy to protect their infrastructure assets by defending against attacks related to their 365 transition and better securing 365 services." ActZero has previously written about how the unexpected shift to WFH meant, in many cases, a rushed implementation of tools to support an army of now-remote workers — and these initial hasty solutions have settled in as standard operating procedures.

Even prior to the new challenges posed by the rise of remote work, it's proven difficult for Microsoft itself to secure its cloud. In 2019, "misconfigured Microsoft cloud databases containing 14 years of customer support logs exposed 250 million records to the open internet for 25 days," as Threatpost reported. The cause for this potentially catastrophic lapse? According to Microsoft's own blog post, "a change made to the database's network security group on December 5, 2019 contained misconfigured security rules that enabled exposure of the data." If even Microsoft struggles with its own cloud security configurations, we can be sure it will be no simple matter for the rest of us.

Last year, a post by Azure Security Center promoted various improvements to securing customers' data and detecting threats like malware. However, the post also suggested companies shouldn't rely solely on Azure's defense features to keep themselves safe: "Even with all these capabilities, it's still essential to bolster cybersecurity, especially with the growing complexity and sophistication of cyberattacks," wrote the Azure product manager.

Microsoft 365

Adam Mansour, ActZero's Head of Sales Engineering and a cybersecurity expert with over 15 years of experience, views Microsoft 365 as a particular challenge to secure for small and medium-sized enterprises (SMEs). “Why is 365 such a nightmare? In a word, data. The day you start using 365, you acquire dozens of native apps, and every single one is largely unsecured by default.” You're likely familiar with apps like Teams, Word, and Excel. But how about Delve, Yammer, and Sway, to name a handful of the offerings included with 365? Whether or not you've even heard of them, you now own all of them — and must secure all of them.

This is a major virtue of 365: in just 10 minutes, you can enable an entire data center, and have a whole enterprise ready to go. This is incredible, especially when you consider it might have taken 10 years to set up this amount of IT infrastructure in 1995. There's a catch, though: to secure all the 365 infrastructure from its default state after you've set it up is a massive undertaking. Now, your entire data center is facing the internet, and malicious actors can potentially launch attacks at any one of these vectors, spreading easily between them once they land. There are countless exploits facing this configuration, and the logs produced are vast — there is far too much raw data for humans to comb through it by hand in order to identify suspicious behaviour and abnormal activity.

Azure Active Directory (AD)

Every organization using Microsoft 365 also has Azure AD enabled by default — although some are not even aware of it. Azure AD is Microsoft's cloud-based identity and access management service, allowing employees to access external resources “such as Microsoft 365, the Azure portal, and thousands of other SaaS applications,” along with internalresources“suchasappsonyourcorporatenetworkandintranet.”

This is convenient but also poses considerable risk. Mansour points to Teams as one example. “By default, there are multiple APIs that just let you access Teams — and what's behind Teams: every file you've ever shared, every single username and password, and all your customer data. All of it is open to other apps through APIs. If you share a file on Teams, it's really being posted to SharePoint, and if you connect an app to Teams it potentially connects to both.” The configurations that allow access to these various enterprise apps are poorly understood by many users.

Microsoft Azure

Microsoft describes its Azure platform as “more than 200 products and cloud services designed to help you bring new solutions to life… Build, run, and manage applications across multiple clouds, on-premises, and at the edge, with the tools and frameworks of your choice.” The platform delivers on this claim, providing myriad ways to do things — far more options than an enterprise would have traditionally had on-premise. Jerry Heinz, a cloud computing veteran and ActZero’s VP of Engineering, identifies the versatility offered by Azure as a major hurdle to securing it.

“Windows machines in the cloud are as flexible as any other Windows machine. They can be remote, they can be an application server, they can be a web server. You can choose how to stitch together the services to form an offering. Platform-as-a-Service, Database-as-a-Service, SaaS — all of these services expose many different APIs at different layers, and how you wire those things together will uniquely define what security problems you actually have, and what your threat model looks like.” Heinz says life has gotten far more complicated for the in-house IT admin, who previously worked with standard building blocks of network infrastructure that fit together in predictable ways — and is now faced with potentially limitless configurations.

In the event that the inherently challenging-to-secure nature of the Microsoft cloud is making you rethink your transition, let’s not forget that on-premise infrastructure is also at risk of different types of attacks. Rather than delaying your migration skyward, here are actions you can take to configure and use Microsoft’s cloud more securely.

4 Steps you can take for hardening your Microsoft cloud

With nearly infinite ways of putting things together, there is no "one-size-fits-all" approach to cloud security. However, there are best practises to minimize your risk. We've seen how a single compromised credential can serve as a beachhead for larger attacks, so securing your 365 accounts should be a high priority.

The top three threats to 365 accounts are password-based attacks, credential phishing, and consent phishing. Here's a brief look at each, and how to fortify yourself against them. (For a detailed and technical look at these attacks, and how we are producing detections for them, check out our post "Protect Your Office 365 Accounts from Takeover.")

THREAT 1

- **PASSWORD-BASED ATTACKS:** The three most common password-based attacks for 365 are credential stuffing, brute-force, and password spray. The most important things you can do to protect your 365 accounts from password-based attacks are to turn on Multi-Factor Authentication (MFA) and turn off Legacy Authentication for all user accounts (use long complex passwords for service accounts). Both can be configured through "Properties > Enable Security defaults > Manage Security defaults" in the Azure Portal.

THREAT 2

- **CREDENTIAL PHISHING:** Phishing attempts often appear as a pop-up or an email indicating that account credentials are "suspended," need to be "verified," or "reset." Unsuspecting users follow the prompts, landing on a well-crafted page where they are prompted to enter credentials — and inadvertently give attackers access to the account. In addition to turning on MFA as mentioned above, there are features available in Premium editions of Azure AD that help protect against credential phishing. For example, conditional access policies can block access by location or IP address, and Azure AD identity protection can be used in conjunction with conditional access to create risk-based policies.

THREAT 3

- **CONSENT PHISHING:** Sometimes known as "App Attacks," OAuth attacks occur when threat actors leverage a 365 app created using information stolen from a legitimate organization. The attacker sends an email, text, or other communication purporting to be from Microsoft asking users to complete an action. After the user signs into their 365 account, they're redirected to the official 365 consent process that prompts them to grant permissions to the actor's application. Once permission is granted, the attacker will have persistent access to the 365 account(s). One defense is disabling user consent — this option is the safest, but may generate additional requests for admins to add new applications, as users will be unable to grant permissions.

Even with these best practises in place, administrators cannot hope to do this alone. User training is also an essential step, as human error is ultimately to blame in far too many compromises. (One report estimates that mistakes by humans caused 90 percent of all cyber data breaches seen in 2019!) Assess the human components of your security posture, and educate employees about these password-based attacks. Consider sending employees benign phishing emails, and holding a contest open to anyone who reports them.

These steps will certainly harden your assets in the cloud — but the truth is, nothing can make an organization invincible. A strategy brief from the Microsoft Cyber Defense Operations Center says that "Microsoft operates under an 'Assume Breach' posture. This means that despite all the protections in place, we assume systems will fail or people will make errors, and an adversary may penetrate our infrastructure and services." Cyber criminals have a powerful financial incentive to be persistent; a mature security approach must assume they will eventually be successful, and be prepared to react. Next, we will look at the need for rigorous detection and response capabilities.

5 The need for speed: endless data & machine learning

As Heinz said, the infinite permutations of configurations pose a significant challenge. The biggest issue facing IT professionals confronted with securing the cloud, however, is data. Having your entire data center facing the internet means a massively expanded attack surface to monitor for anomalies. The longer a breach goes unnoticed, the deeper a hacker can penetrate and the more damage they can do. But how can you tell if one user or account is behaving strangely? You can invest in cloud security programs, if you have the pricey specialists needed to monitor them, and even experts cannot possibly go through all the logs by hand — the data points grow exponentially with the complexity of network topographies.

If an organization makes a large investment into technology stacks that generate alerts, analysis leveraging data science is necessary to garner insight from them at scale— and to direct action. With the potential for billions of events a day, such tech generates logs at a blistering rate no human could possibly keep pace with. A Security Information and Event Management (SIEM) program can assist in aggregating and funneling these alerts — which can number into the thousands per day and come in 24 hours a day — but can still generate false positives and a bloated collection of irrelevant logs, unmanageable for any analyst to keep up with. The solution is incorporating machine learning into your cloud security framework, so that all this data becomes a blessing instead of a curse. Because of the scale of the cloud, you end up with far more data about what constitutes normal usage patterns.

Alexis Yelton, ActZero's Head of Data Science with a focus on building machine learning models for software products, explains why machine learning is critical to parsing this data in order to identify future attacks. She says incorporating anomaly-detection models that use past data to establish a baseline allows security professionals to determine what normal activity looks like. The models can be trained to detect very unusual activity, and bring it to the attention of security analysts. "With anomaly detection, you gain the ability to detect new attacks, and with supervised models you get a really strong signal as to what's an attack."

The status quo is sending a lot of alerts, but the goal here is high-fidelity detections — finding all the attacks without a lot of false positives. This helps with the issue of alert fatigue, says Yelton. "When you're going through that many alerts, you'll miss ones that are actual attacks. In fact, there have been some high-profile breaches in which big enterprises lost hundreds of millions of dollars from attacks that were actually detected, but the admins or analysts looking at it did nothing. We strive to reduce those false positives to prevent that from happening." (To learn more about this, listen to Yelton's appearance on The Data Standard podcast.)

6 Secure your Microsoft cloud with managed detection & response

The right configurations will reduce risk, but monitoring for suspicious activity in your 365 account is still necessary. It's also critical you have the ability to respond to threats yourself. Microsoft makes it clear companies using its cloud offerings have a responsibility to protect themselves: "Microsoft does not monitor for or respond to security incidents within the customer's realm of responsibility. A customer-only security compromise would not be processed as an Azure security incident and would require the customer tenant to manage the response effort." And most breaches are on the customer's end — Gartner cautions that "through 2025, 99 percent of cloud security failures will be the customer's fault."

ActZero is a cybersecurity startup that makes small- and mid-size enterprises more secure by empowering teams to cover more ground with fewer internal resources. Our intelligent managed detection and response service provides 24/7 monitoring, protection and response support that goes well beyond other third-party software solutions. Our R&D team of data scientists, security specialists, and cloud engineers leverage cutting-edge technologies like AI and ML to scale resources, identify vulnerabilities, and eliminate more threats in less time. We actively partner with our customers to drive security engineering, increase internal efficiencies and effectiveness and, ultimately, build a mature cybersecurity posture. Whether shoring up an existing security strategy or serving as the primary line of defense, ActZero enables business growth by empowering customers to focus their resources on their core competencies.

It was always a problem to track what's happening locally on your endpoints and network. It's an even bigger problem in the cloud, especially if you didn't design for security up-front. As Microsoft puts it, "hybrid attacks that span from cloud to endpoints require a wide range of sensors for comprehensive visibility." ActZero's cross-vector coverage protects your endpoints, network, and Microsoft cloud offerings, and our Client Portal provides real-time reporting on what's working. We'll help analyze those endless logs and provide you with high-value notifications of cloud compromise, not a bunch of noise. And for those concerned about handing over the "keys to the cloud," ActZero underwent a rigorous SOC2 audit that proves we handle your data responsibly; check out our CXO Insight that offers questions you can ask your provider to assess whether they do.

Our R&D team of data scientists, security specialists, and cloud engineers leverage cutting-edge technologies like AI and ML to scale resources, identify vulnerabilities, and eliminate more threats in less time.

For more on our cloud capabilities, please see our solution brief on M365 Detections.

To learn about the risk of account takeover check out our M365 ATO Threat Insight.

Or, to understand how to cover more ground across the endpoint, network and cloud, request a demo of our MDR service today.

ActZero

TORONTO
207 Queens Quay, Suite 820
Toronto, Ontario M5J 1A7

MENLO PARK
2882 Sand Hill Road, Suite 115
Menlo Park, California 94025

SEATTLE
925 4th Ave., 20th Floor
Seattle, Washington 98104

in ActZero   ActZeroAI   f ActZero.ai