VECTRA
SECURITY THAT THINKS

INDUSTRY RESEARCH REPORT

The 2020 Spotlight Report on Office 365

INTELLIGENT
THREAT DETECTION
AND RESPONSE

CLOUD-NATIVE

ENTERPRISE

TABLE OF CONTENTS

Vectra® protects business by detecting and stopping cyberattacks

As a leader in network detection and response (NDR), Vectra protects your data, systems and infrastructure. Vectra enables your SOC team to quickly discover and respond to would-be attackers —before they act.

We rapidly identify suspicious behaviors and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra is Security that thinks®. We use artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

$6.5-7 BILLION

The cost of account takeovers was estimated at $6.5 to $7 billion in annual losses across multiple industries.

Forrester Wave: *Risk-Based Authentication* report, Q3 2017

HIGHLIGHTS

4M **Microsoft Office 365 accounts were sampled for this study**

96% of customers sampled exhibited **lateral movement behaviors**

71% of customers sampled exhibited **suspicious Office 365 Power Automate behaviors**

56% of customers sampled exhibited **suspicious Office 365 eDiscovery behaviors**

Attackers live off the land while creating chaos in the clouds

The largest security risk in a SaaS environment today is identity. Specifically, it is a misuse of identity and the privilege access granted to it. Before implementing any SaaS platform, first consider how much access is really being granted to a user.

Attackers are now focusing on account takeover rather than email compromise to gain initial access.

More importantly, how is that privilege access being used? The principle of least privilege is even more important in SaaS environments, where only identity is controlled and data and resources are highly consolidated.

In the SaaS world, Office 365 has dominated the productivity space, with more than [more than 250 million active users each month](). For many of those users, Office 365 is the core of enterprise data sharing, storage, and communication, making it an incredibly rich data target.

It was no surprise that Office 365 has become the focus of attackers. Despite the increased adoption of MFA and other security controls, financial and reputational damage from Office 365 data breaches have continued to mount.

Of those breaches, account takeover attacks are the fastest growing and most prevalent. Attackers are now focusing on account takeover rather than email compromise to gain initial access.

Today, Office 365 accounts are used to move laterally to other users and privileged resources. Based on Vectra customer data observed in 4 million accounts from June-August 2020 lateral movement is the most common type of suspicious behavior inside Office 365 environments, closely followed by command-and-control communication.

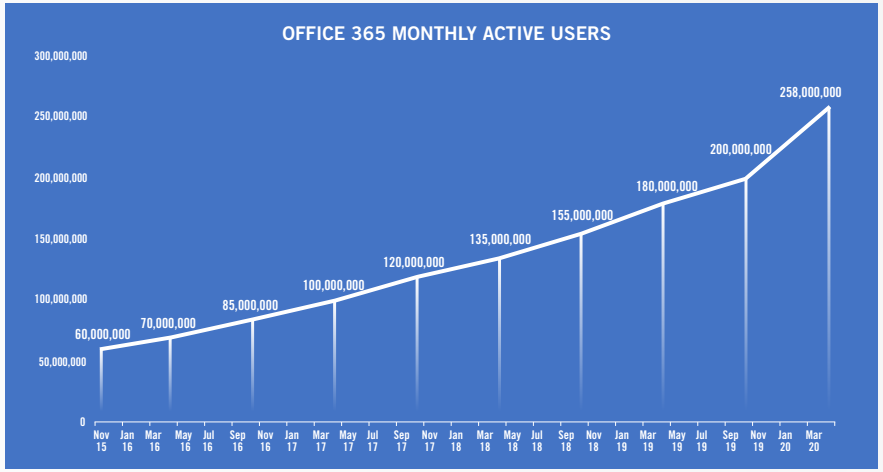


Figure 1: [Office 365 monthly active users]()

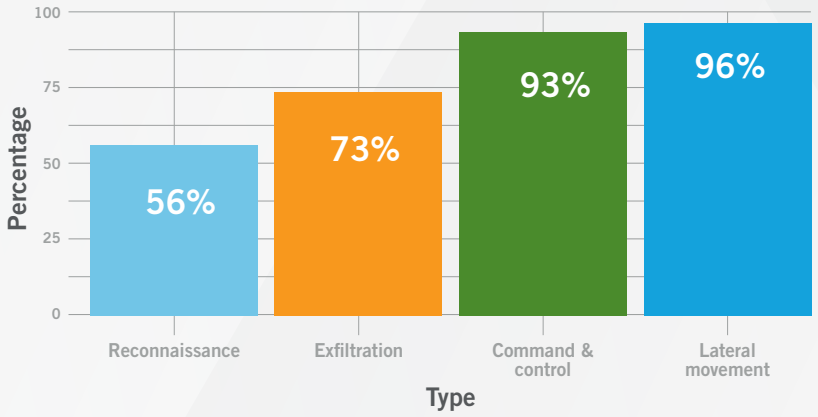


Figure 2: Frequency of suspicious behavior categories observed in Vectra NDR Office 365 deployments

The cloud is an entry point and the end goal of attackers who spread laterally in search of assets to steal. In Office 365, threats traverse the attack lifecycle with no endpoint or network activity taking place and evade traditional network and endpoint detection.

The problem has become quite severe. According to the Forrester Wave: Risk-Based Authentication report from 2017, the cost of account takeovers was estimated at $6.5 to $7 billion in annual losses across multiple industries.

Common techniques used by Office 365 attackers

- Searching through emails, chat histories, and files looking for passwords or interesting data.
- Setting up forwarding rules to get access to a steady stream of email without needing to sign-in again.
- Leveraging the trusted communication channel – the email isn't spoofing an email from the CEO; it is an email from the CEO – to socially engineer employees, customers or partners.
- Planting malware or malicious links in documents that many people trust and use, again leveraging trust to get around prevention controls that may trigger warnings.
- Stealing or holding files and data for ransom.

These are straightforward attack techniques. However, smart cybercriminals can launch attacks that are far more sophisticated.

LEGITIMATE TOOLS AND SERVICES USED BY OFFICE 365 ATTACKERS

Power Automate

Microsoft Power Automate lets users create custom integrations and automated workflows between Office 365 applications. It is enabled by default and includes connectors to hundreds of third-party applications and services. Power Automate's wide availability and ease of use also makes it a partially useful tool for attackers to orchestrate malicious command-and-control and lateral movement behaviors.

eDiscovery

Microsoft eDiscovery is an electronic discovery tool that searches across Office 365 applications and data and exports the results. Attackers use eDiscovery as a powerful internal reconnaissance and data exfiltration tool.

OAuth

OAuth is an open standard for access authentication. It is utilized by third-party applications to authenticate users by employing Office 365 login services and the user's associated credentials. Attackers are leveraging OAuth enabled malicious Azure applications to maintain persistent access to users Office 365 accounts.

Attackers can use Office 365 as the entry point to pivot onto the user system for ongoing access. One way to do this is to setup mail rules triggered by an email with a specific subject, or even just syncing the Outlook client. These can turn a compromised Office 365 account into a persistent reverse shell on the user's system.

Two Office 365 tools are of particularly high value to attackers: Power Automate and eDiscovery Compliance Search.

Pivoting from the cloud to physical systems is a technique that the APT33 group – believed to be an Iran state-sponsored operator – used as a method of attack. APT33 gained access to Office 365 via password spray attacks. Mail rules were then used to establish a reverse shell on the systems of the compromised users.

Once inside the physical network, APT33 proceeded to execute a standard attack path on physical systems to gain domain administrator privileges. This attack showed that cloud-based systems were entry points and physical systems were the target.

Attackers are also adept at bypassing MFA for Office 365. Social engineering techniques are a common tactic to get users to install malicious Azure apps. Like mobile apps, users accept permission requests that give the app and the attacker unfettered access to resources. Access can persist for 90 days with no interim authentication challenges, even if the password is changed.

Most critically, attackers live off the land using legitimate Office 365 tools and features to remain hidden and bypass security controls.

This attack method, widely attributed to China, was used against Australian companies. The social engineering trick involved spoofing an app from MailGuard 365, a security app already used by the targeted organizations. Once installed, attackers were given persistent access, could read user profiles, and manipulate emails.

Most critically, attackers live off the land using legitimate Office 365 tools and features to remain hidden and bypass security controls. Two Office 365 tools are of particularly high value to attackers: Power Automate and eDiscovery Compliance Search.

Microsoft Power Automate, formerly Microsoft Flow, automates day-to-day user tasks like managing email attachments or approval flows. It is enabled by default in all Office 365 tenants and it can be configured to do amazing things that reduce time and effort for users as well as attackers. Below are a few examples:

- Connect via HTTP to a command-and-control point to send data.
- Automatically sync OneDrive files to an attacker-owned Google Drive on every file modification update.
- Tweet all emails that include specific keywords.

With over 350 application connectors available – and more being added every week – the options for cyberattackers who use Power Automate are vast.

Office 365 eDiscovery Compliance Search enables a single search of information across all Office 365 apps. Imagine searching for "password" or "pwd" across Microsoft Outlook, Teams, all files in SharePoint and OneDrive, and OneNote notebooks using one simple command.

All these techniques are actively used now, and they are frequently used together across the attack lifecycle. Power Automate and eDiscovery were among the most common suspicious behaviors in the Office 365 environments of Vectra customers.

Highlighting the risks presented with native tools in Office 365, Microsoft published the timeline of an attack using live-off-the-land techniques to maintain complete Office 365 access for 240 days. The attackers used eDiscovery to find data and Power Automate to exfiltrate it.

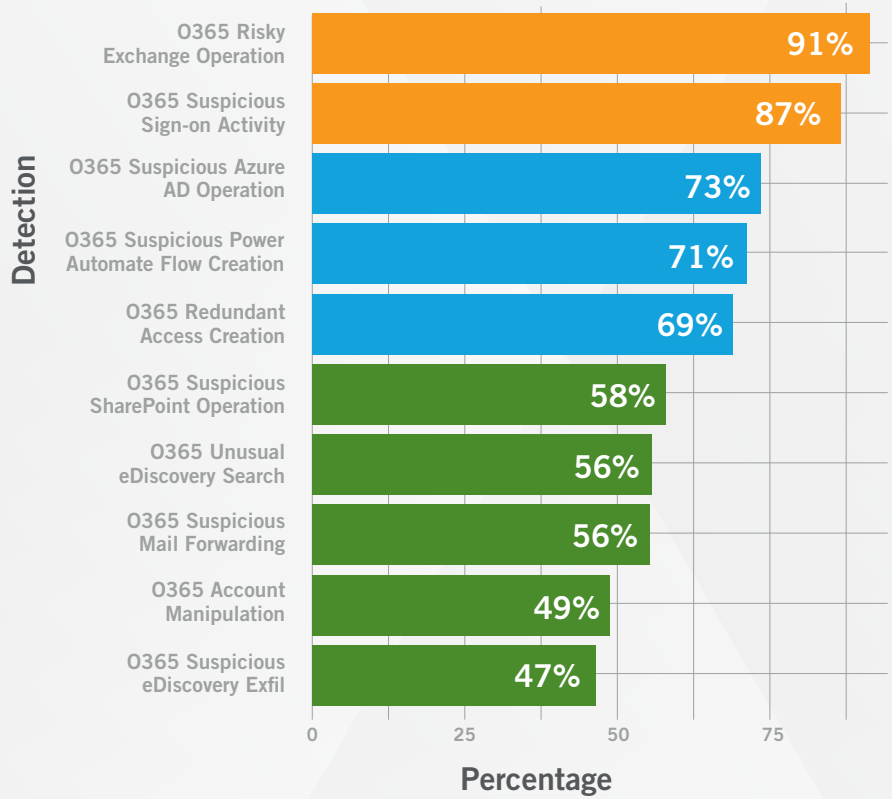


Figure 3: Frequency of the Top 10 suspicious behaviors observed in Vectra NDR Office 365 deployments

An analysis of 4 million Office 365 accounts monitored by Vectra identified the Top 10 most prevalent behaviors associated with attacks against Office 365. These were primary behaviors linked to threat actors who employed command-and-control and lateral movement attack techniques.

MITRE ATT&CK Mapping: Top 10 suspicious behaviors observed in Vectra NDR Office 365 deployments

MITRE ATT&CK

Vectra detection in Office 365	MITRE ATT&CK framework	Associated attacker behavior
Risky exchange operation	• T1484 Group Policy Modification • T1098 Account Manipulation	**Lateral movement** An attacker is manipulating Microsoft Exchange to access a specific set of data or to enable continued attack progression.
Suspicious sign-on activity	• T1078 Valid Accounts	**Command and control** An adversary has stolen a valid account and is using it as part of an attack.
Suspicious Azure AD operation	• T1078 Valid Accounts	**Lateral movement** Attackers might be escalating privileges and performing administrator-level operations after a regular account takeover.
Suspicious Power Automate flow creation	• T1041 Exfiltration Over C2 Channel • T1008 Fallback Channels T1105 Ingress Tool Transfer • T1059 Command and Scripting Interpreter • T1020 Automated Exfiltration	**Command and control** An adversary has leveraged Power Automate as a persistence mechanism inside the environment.
Redundant access creation	• T1098 Account Manipulation	**Command and control** An adversary has provisioned access into a sensitive role to create redundant access into the network.
Suspicious SharePoint operation	• T1078 Valid Accounts • T1213 Data from Information Repositories	**Lateral movement** An attacker has located a SharePoint administrative account and is using it in pursuit of attack progression.
Unusual eDiscovery search	• T1119 Automated Collection • T1213 Data from Information Repositories • T1083 File and Directory Discovery	**Internal reconnaissance** An adversary has gained access to eDiscovery capabilities and is using it to perform internal reconnaissance across the environment.
Suspicious mail forwarding	• T1114 Email Collection	**Data exfiltration** An external attacker has established persistent access to the contents of a specific mailbox without having to maintain persistence by installing software.
Account manipulation	• T1098 Account Manipulation	**Lateral movement** An attacker has escalated the account's Microsoft Exchange access rights to enable business email compromise or the collection of additional information to aid in the next step of the attack.
eDiscovery exfiltration	• T1048 Exfiltration Over Alternative Protocol	**Data exfiltration** An adversary has gained access to eDiscovery capabilities and is using that access to collect or exfiltrate data.

Case study: Midsized manufacturer

Manufacturer suffers a business-email compromise fraud attack

The attacker zeroed in on the finance department, likely using LinkedIn to identify them. A low-and-slow brute-sweep attack was run against legacy protocols – again finding the place where MFA could not be enabled – to gain access to Office 365.

Once inside, the attacker setup rules to forward all emails related to either DocuSign or invoices, making the financial fraud motive clear. Cleverly, the attacker also setup rules to erase threat evidence and avoid discovery by automatically deleting all emails related to passwords and security.

In real time Vectra detected multiple stages of the attack and enabled the security team to delete the forwarding rules and change passwords before any emails were sent outside the organization.

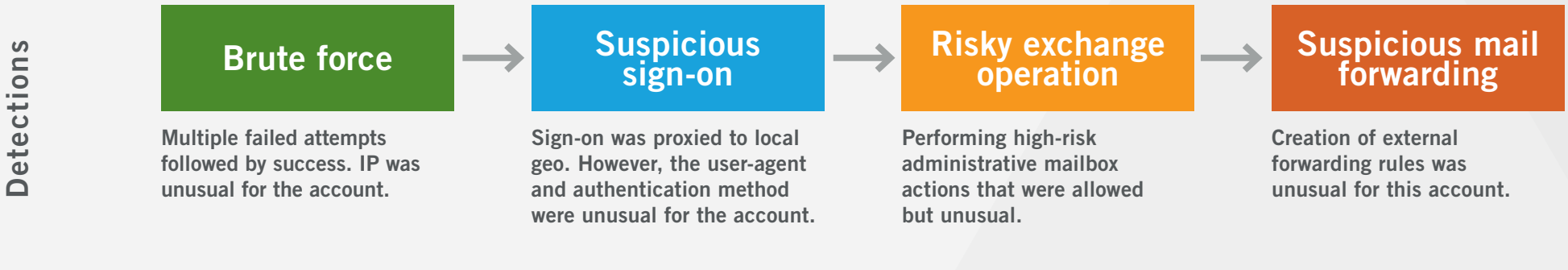


Figure 5: Vectra detections of business email fraud attempts

Case study: Research university

A medical research unit at a university was targeted with a phishing lure that promoted a free calendar optimization and time-management app.

One person took the bait and installed the malicious OAuth app, bypassing MFA and unknowingly providing complete access to Office 365.

Using that access, the attackers then sent internal phishing emails, taking advantage of trusted identities and communications to spread further inside the university.

Vectra detected the suspicious app installation, and as part of the investigation, noted that the internal spear-phishing detection had also fired. The security team was able to evict the attacker by removing the malicious app.

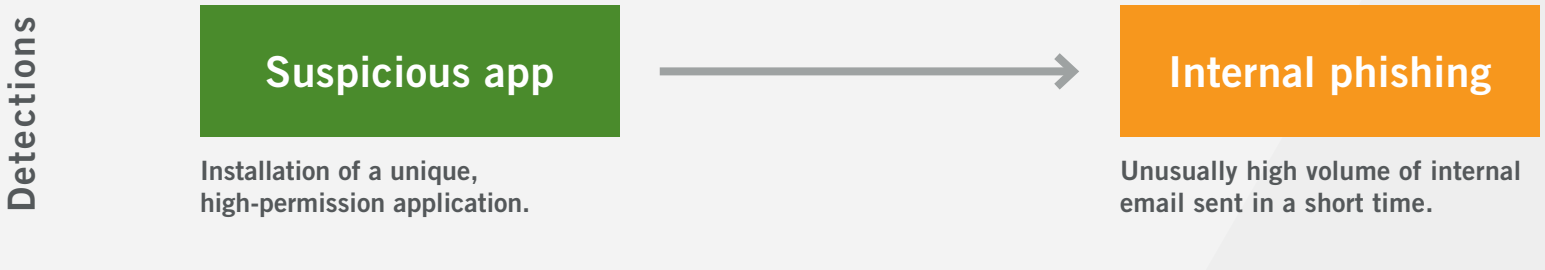
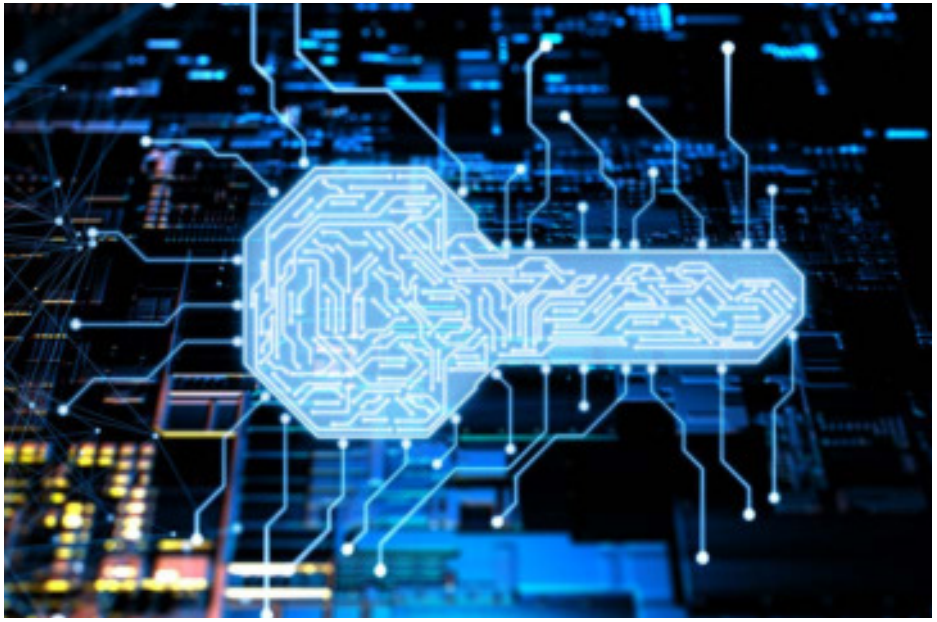


Figure 6: Vectra detections of MFA bypass attacks

Keeping your Office 365 deployment safe

Identifying user access misuse has been treated as a static problem using approaches that are prevention-based, policy control-centric or rely on manual entitlements that surface threats as they occur, leaving little time to properly respond. These legacy approaches continue to fail.

This type of access monitoring only shows that an approved account is being used to access resources. It does not provide insight into how or why those resources are being used.



It is insufficient to rely solely on the granted privilege of an entity or being agnostic to privilege. Security teams must have detailed context that explains how entities utilize their privileges – known as observed privilege – within SaaS applications like Office 365. Just as attackers observe or infer interactions between entities, defenders should think similarly about their adversaries.

This translates into understanding how users access Office 365 resources and from where, but without looking at the full data payload to protect privacy. It is about the usage patterns and behaviors, not the static access.

The importance of keeping a watchful eye on the misuse of user access cannot be overstated given its prevalence in real-world attacks. SaaS platforms like Office 365 are a safe haven for attacker lateral movement, making it paramount to focus on user access to accounts and services.

Ideally, when security teams have solid information and expectations about SaaS platforms, malicious behaviors and privilege abuse will be much easier to quickly identify and mitigate.

Security teams must have detailed context that explains how entities utilize their privileges – known as observed privilege – within SaaS applications like Office 365.

Email info@vectra.ai vectra.ai