VIDDER

Securing Office 365 & Other SaaS

PrecisionAccess

Executive Summary

Securing Office 365 means securing Email, SharePoint, OneDrive, and a number of other applications offered as part of the Office 365 brand. In addition, it often means securing other SaaS applications such as Salesforce, Box, Workday, ServiceNow, etc. that use the same single sign on (SSO) identity provider as Office 365.

To understand how to secure these applications, one must understand how adversaries attempt to attack them. Below is a list of the four ways the data of these applications gets breached – prioritized by the probability of the threat.

Probability[1]	**Threat**	**Mitigation**
85%	Compromised password	MFA
10%	Compromised PC	Trust Assessment
4%	Man-in-the-middle	Mutual TLS, unalterable suite, pinned certs
1%	Malicious authorized user	IRM, PAM, Encrypting at rest (HYOK), DLP, …

Importantly, one security control, PrecisionAccess, defeats 99% of the attacks – creating the single largest improvement to the security posture of Office 365 possible. And it provides the same increased security for the other SaaS applications.

[1] Based on a number of data breach reports with the additional analysis of 1) separating out the data that was relevant to Office 365 vs. other data breaches and 2) creating a probability that adds to 100% as opposed to allowing for overlapping attacks.

Table of Contents

Scope of Applications

The present list of applications covered by the Office 365 brand includes: Exchange Online (email and calendar), Office 365 Sites (SharePoint), OneDrive for Business, Skype for Business Online, Yammer, Project Online, PowerBI, Office 365 Groups, Stream (Office 365 Video), Planner, and access to the Office Applications. With PrecisionAccess one can secure all of them, in one fell swoop.

Credential Theft

The good thing about Office 365 is that it's available to *authorized users* from everywhere over the Internet. The bad thing about Office 365 is that it's available to *adversaries* from everywhere over the Internet. When a username and password are all that's required to authenticate to Office 365, credential theft makes it easy to compromise it from anywhere in the world.

Even worse, most enterprises use Single Sign-On (SSO) to authenticate to Office 365 AND TO MANY OTHER SaaS applications. Therefore, credential theft can truly jeopardize a business. And that makes it the number one threat to the security of the enterprise. This is one threat that needs to be nailed.

It's Easy to Compromise Passwords

There are multiple ways that passwords get compromised. One common way is through password reuse. People often use the same password on multiple websites. If the password of any of those websites gets compromised, and if was also used for Office 365, then the adversary has access to that user's Office 365 account.

Alternatively, weak passwords enable adversaries to guess the passwords. Some adversaries have botnets set up just for this purpose. The bot herder distributes a list of usernames to the botnet zombies, and they attempt to log into websites with easily guessed passwords. If they succeed anywhere, there's a good chance they can succeed at important places like Office 365 using the same password.

And what is the incentive for employees and third parties to use complex passwords? It just makes their life harder. It's much easier to use P@ss1Q18 as their corporate password. It will meet most password complexity requirements, and employees can easily meet the requirement to change the password every 90 days by simply changing the last four characters to the present quarter. Of course, adversaries know this trick, too.

You Can Try this at Home

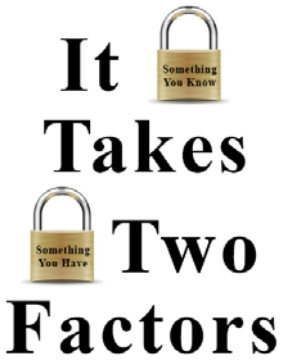
Here's a trick you can try at home to compromise the Office 365 accounts of some of your co-workers.

1. Download TheHarvester and run it to discover and download a number of the email addresses of your co-workers.
2. Download THC Hydra and an associated password list.
3. Download Tor, which includes a SOCKS proxy. Use this to remain anonymous for the final step.
4. Run Hydra to spray Office 365 with the email addresses you obtained from TheHarvester using the common list of passwords through the Tor SOCKS proxy.

The likely result is that you will discover the passwords of at least a few of your co-workers. If a complete amateur can do this in a couple hours, consider what a professional adversary can do with all the time in the world.

MFA is the Answer

Since passwords aren't enough, MultiFactor Authentication (MFA) is needed. One of the best forms of MFA is a cryptographic One-Time Password (OTP) with replay prevention because it is not feasible to guess the one-time password in a reasonable amount of time. An even better form of MFA is mutual TLS, which cryptographically enforces MFA and defeats all man-in-the-middle attacks at the same time.



PrecisionAccess Implements the Ideal MFA

Vidder's PrecisionAccess implements OTP and mutual TLS. Furthermore, it meets all the criteria of the ideal MFA. That is, it defeats weak and compromised passwords, it is transparent to the user, and it is easy to apply to all applications. For more about the ideal MFA of PrecisionAccess, see "The Ideal MFA" whitepaper.

Compromised PC

It may be more difficult to compromise a PC than it is to perform the credential theft listed above, but once the PC is compromised, MFA is useless (again, see "The Ideal MFA" whitepaper). Therefore, the second greatest threat to securing Office 365 is preventing a compromised PC of an authorized user from accessing Office 365 and other business critical applications.

It's Still Pretty Easy to Compromise a PC

It's been happening for a long time and it's not letting up. Combine the numerous vulnerabilities in operating systems and applications with phishing attacks, social engineering, and drive-by downloads, and PC's become compromised. While the traditional antivirus (AV) application may now be employing new techniques, the adversaries are also employing a new round of fileless exploits that completely bypass AV programs altogether.

Trust Assessment is the Answer

Trust Assessment is the combination of posture assessment, vulnerability assessment, and threat assessment. Posture assessment can enforce that the device is a managed device and that the device is running AV with the latest signatures, and, while that is useful, it's not sufficient. Vulnerability assessment can enforce that the device does not have any known vulnerabilities or configuration errors in its OS and all of its applications, which makes the device much more difficult to exploit. Finally, threat assessment can enforce that the device has not experienced any known bad behavior such as fireless exploits or connecting to an adversary's command and control servers.

PrecisionAccess Implements the Ideal Trust Assessment

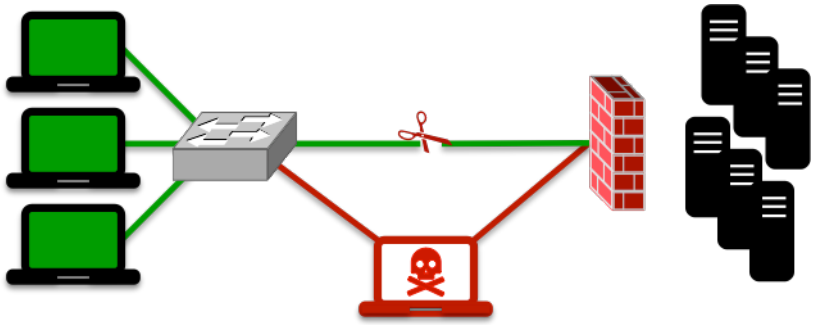
Vidder's PrecisionAccess provides visibility, reporting, alerting, and enforcement of all three components of Trust Assessment. Beyond that, PrecisionAccess is based on an application-layer tunnel – not a network layer tunnel. This inherently defeats malware from accessing protected applications. And, from the standpoint of Endpoint Detection and Response (EDR), the behavior of attempting to compromise the inherent security of an application layer tunnel is a clear Indication of Compromise (IoC) that can be used to detect that the PC is no longer safe to access Office 365 and other business-critical applications.

Man-in-the-Middle Attack

The man-in-the-middle attack doesn't get the respect it is due. Under the proper circumstances, this attack can defeat the security of multiple devices, simultaneously. Therefore, the third greatest threat to securing Office 365 is the man-in-the-middle attack.

It's Pretty Easy to Create a Man-in-the-Middle Attack

There are many ways to create a man-in-the-middle attack. Arguably the simplest is with a rogue Wi-Fi access point and the Mana Toolkit. Combined, the adversary will get clear text access to the conversations of multiple victims. Moving all the way up to the resources available to a nation state adversary, obtaining a forged PKI certificate will allow the adversary to have a more directed attack. And then there are a number of attacks that lie in the middle including a number of attacks that downgrade the cypher suite being used to encrypt and verify the communication.



Mutual TLS with Pinned Certificates and an Unalterable Suite is the Answer

Whereas regular Transport Layer Security (TLS) only verifies the authenticity of the server to the client, mutual TLS also verifies the authenticity of the client to the server, as well. And, whereas regular TLS accepts PKI certificates generated by hundreds of certificate authorities around the world, TLS with pinned certificates only trusts one (private) PKI certificate authority. Finally, whereas regular TLS lets both the client and the server determine the cryptography used to communicate between the client and the server, TLS with an unalterable suite defeats downgrade attacks.

PrecisionAccess Defeats All Man-in-the-Middle Attacks

Vidder's PrecisionAccess implements mutual TLS with pinned certificates and an unalterable cryptography suite of the highest cryptographic strength commercially available. The great thing about this combination of technologies is that it defeats all man-in-the-middle attacks. For more information please see the "Defeating All Man-in-the-Middle Attacks" white paper.

Malicious Authorized User

The malicious authorized user can do a lot of damage. If the user is a regular employee, that person can send intellectual property to competitors. If the user is an IT admin, that person can wreak havoc on the IT infrastructure. If that person is a Microsoft Azure admin, that person can access unencrypted data. Luckily…

The Malicious Authorized User is Uncommon

The Malicious Authorized User is Uncommon. Getting caught is a career ending crisis, and may also involve prison time. The best deterrent is to make that outcome clear to all users.

All the Tools and Still No Answer

There are lots of tools that can attempt to prevent, and/or help discover, malicious users, but none are guaranteed to work. For authorized users, Microsoft provides Office 365 Information Rights Management (IRM) to encrypt files and prevent printing of them no matter where they go. This can be a good deterrent for accidental misuse, but malicious authorized users can still photograph the content on

their screens. For admins, Privileged Access Management products can record all actions the admins take, which is a good deterrent against overt actions, but there are still many ways an admin can be malicious. To prevent Microsoft Azure admin accessing unencrypted data, there is Hold Your Own Key (HYOK) data at rest encryption, which can be costly and time consuming to implement. Finally, to help discover accidental misuse, Microsoft provides a Data Loss Prevention (DLP) capability, which can be applied to Exchange, SharePoint, and OneDrive. Unfortunately, all of these controls are very costly to implement and manage.

PrecisionAccess Can Help

Vidder's PrecisionAccess will not prevent or detect the most covert of malicious authorized users like some of the tools above may, but PrecisionAccess may be able detect the most overt actions of malicious authorized users. It can report and/or alert on some forms of anomalous behavior such as individuals downloading large amounts of data and admins working at odd hours, and can do this at a fraction of the cost of the tools mentioned above. However, the most paranoid of security architects will still want to implement those other controls.

Summary

In summary, PrecisionAccess is a mandatory security control for Office 365 and other business-critical SaaS applications. It defeats 99% of the probability of a threat by defeating credential theft, compromised PC's, and man-in-the-middle attacks. In addition, it helps with the last 1%, but many additional controls will be needed to address that 1%. The important thing is to prioritize the 99% of threats over the 1%.