Zero Trust Security In Microsoft 365

AgileIT

ADAPTIVE • RESPONSIVE • STRATEGIC

Zero Trust Security in Microsoft 365

Contents

Introduction 2

What are Zero Trust Networks? 3

Why is Zero Trust More Secure? 4

Why is Zero Trust So Important? 5

How to Plan your Zero Trust Implementation 6

1. Determine Your "One True Identity" Source with IAM (Identity and Access Management) 7

2. Determine Device Trust 8

3. Inventory Your Access Scenarios 8

4. Choose your Zero Trust Access Tools 9

5. Migrate (Rolling Deployment) 9

Zero Trust is a Mindset, Not an Exact Science 10

Implementing Zero Trust Security With Microsoft 365 11

Azure AD 11

Windows Defender Advanced Threat Protection 12

Cloud App Security 13

Azure Information Protection 15

Microsoft Intune 16

Azure Security Center 17

Enterprise Mobility + Security (EMS) 17

Zero Trust Security Means Thorough (and Effective) Conditional Access 18

INTRODUCTION

The days of castle-and-moat cybersecurity are over. At least, they *should* be over. The old model is no longer cutting it–not even close. Across the globe, cybercrime is costing companies trillions a year. In fact, according to the 2017 Annual Cybercrime Report, it is estimated to cost the world $6 trillion a year by 2021. That has increased from $3 trillion since 2015. The IBM-sponsored 2017 Data Breach Study from Ponemon Institute counted the global average cost of just one data breach to be $3.63 million. Their study also found the average size of a data breach is now around 24,000 files per incident.

At this point, the problem is simple from a bird's eye view: even as threats have evolved, companies have maintained a castle-and-moat mentality–meaning they view cybersecurity as an outdoors-we're-in-danger, indoors-we're-safe scenario. According to that thinking, as long as they put up a strong perimeter of security, the company's data will be safe behind the walls. But the reality no longer fits with this castle-and-moat mentality. As this report from McAfee notes: "Internal actors are responsible for 43 percent of data loss. Half of these incidents are intentional while the other half are accidental."

It's no longer a situation in which data centers serve a contained network. Today's environment has a complicated mix of challenges. On one hand, some things are contained on-site within a perimeter of firewalls. On the other hand, other applications exist in cloud networks that are exposed to

chaotic cobwebs of users from different access points and devices around the world.

It's an unmanageable situation when you're tackling it with the old mentality. There are too many applications that run openly with too many default connections, most of which are based on unmerited trust. The solution is simple: trust no one, trust nothing. In the language of daily life, that phrase might sound anti-social and cold. But in cybersecurity, it is pragmatic. It is fast becoming the only practical solution to this massive quagmire of security that we call the internet.

WHAT ARE ZERO TRUST NETWORKS?

The term Zero Trust Network, also known as Zero Trust Architecture, was conceptualized in 2010. John Kindervag, the principal analyst for Forrester Research Inc., created the Zero Trust model and coined the phrase.

Zero Trust Networks scrutinize and verify everything that attempts to connect to its system whether from an internal or external source. A Zero Trust Network forbids access to anything until the source is verified and authorized. That really does mean refusing access to all machines, IP addresses–the whole scope.

Each request to connect is vetted and approved on an individual basis. Credentials are short-term and temporary, tightly monitored and limited to that particular user's device trying to connect to a specific location of the network at the specific moment in time–similar to a temporary burner phone.

This high level of carefully controlled and monitored authorization on a case-by-case basis has become necessary as cyber attacks have grown in sophistication. It has also become a more realistic possibility as technologies have emerged that make the Zero Trust approach effective.

WHY IS ZERO TRUST MORE SECURE?

This Zero Trust philosophy is more secure because it tests connections *before* they are made. In the old model, the one still used by many companies today, networks allow actors to connect to applications before testing and evaluating the connection.

Here's a common analogy that Zero Trust advocates make when explaining the problem with the old way of doing things: imagine if airports removed their security measures that vetted people's identities and removed checkpoints to ensure they didn't have anything dangerous before connecting with their flight. Imagine if TSA allowed anyone to get on the plane, and *then tried* to vet each passenger ten minutes before departure while everyone's sitting on the plane, buckled up and ready to go. That's essentially what's happening in cyberspace. A packet can wander freely into a network segment and engage with an application before being required to show any credentials.

A Zero Trust Network introduces the test and validation process before any packet can engage, and it does this vetting with every attempt to connect, whether from an internal or external source. It reverses the old

way of doing TCP/IP protocol. This makes it harder for bad actors to get through the front door–or any door or window, for that matter. It manages any movement from a lateral threat within the network by using micro-segmentation, enforcing granular perimeters, and assessing the user, location and other data throughout the process.

It would be nice if we lived in a cyber world where a Zero Trust policy was not needed (just as it would be nice to never have to go through TSA security checks). However, such an open level of trust is no longer possible. Of course, every organization must retain a moderated measure of trust to continue functioning (so the term Zero is more aspirational than literal), but the days of security based on generous trust and minimal internal vetting are coming to an end.

WHY IS ZERO TRUST SO IMPORTANT?

It's still surreal to think the smartphone has only been around for about eleven years since when Apple introduced the first iPhone in 2007. It is especially so when you think about how quickly and thoroughly smartphones have changed the world. In the early 2000s, before the creation of smartphones and other mobile-centric, cloud-based technologies, there wasn't an urgent need for something like a Zero Trust Network. Now we have:

1) Cloud computing, which has no perimeter to defend and can't be contained.

2) A huge variety of mobile devices that introduce a chaotic web of access points.

3) The Internet of Things, which uses sensors on physical objects–sensors that are notoriously difficult to control, update, and secure.

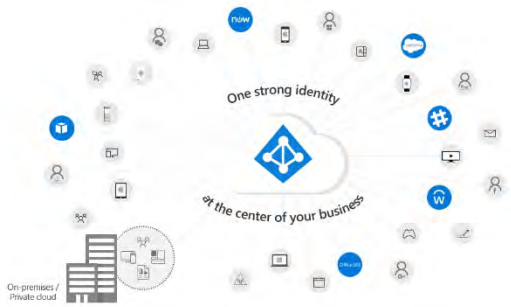
The public has loved these new technologies, but from the vantage point of cybersecurity, it has created a perfect storm. Additionally, when you throw in shadow IT vulnerabilities into the mix–i.e. the tendency of employees to introduce their own third-party software preferences or devices into a company's network without IT's knowledge or permission–your company's cybersecurity suddenly becomes the Wild West.

HOW TO PLAN YOUR ZERO TRUST IMPLEMENTATION

Although the need for a Zero Trust philosophy is urgent (even if having literally "zero" trust is more of an ideal than an actuality), making the big transition into Zero Trust should be done in planned, cautious stages. You should not rush into it without crafting a thoughtful strategy. The following five steps will guide you through the planning process of Zero Trust Network Implementation.

1. Determine Your "One True Identity" Source with IAM (Identity and Access Management)

It is crucial to first establish your one true source of identity. Identity and Access Management is the key to this process. This is where you evaluate the identity of each source and assign the appropriate level of authorization before the user or device gains access to sensitive resources. Some examples of this kind of technology that will help you with IAM include the following:

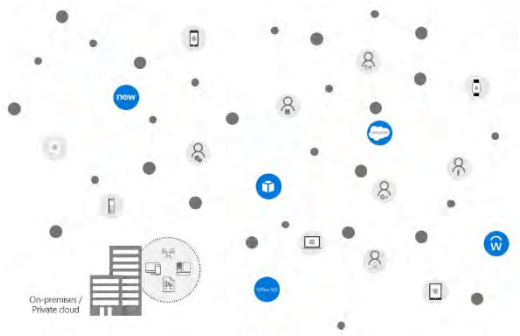


- **AzureAD**: The Azure Active Directory "centralizes identity and access management to enable deep security, productivity, and management across devices, data, apps, and infrastructure". It works for every scenario across the board: apps in the Cloud, on mobile devices, and on-premises. You can use features such as conditional access to layer security and manage access.
- **OpenLDAP**: This is an open source implementation of the Lightweight Directory Access Protocol (LDAP), a vendor-neutral application protocol for managing distributed directory information services over an IP network.
- **Okta**: Okta's IAM products help you to centrally manage every user, app, device, and API in your organization.
- **Amazon IAM**: The tools in Amazon IAM allow you to control access to Amazon Web Services. You can create and manage groups and users. You can also create permissions to allow and deny access as needed.

2. Determine Device Trust

A Zero Trust approach means adopting a Manage vs. Unmanaged Device strategy to device security. This is especially true as more companies allow and even encourage BYOD (Bring Your Own Device). This approach means you assess each device that tries to connect with the network to classify it as either managed (a company-sanctioned, vetted device) or unmanaged (a personal device of the employee). If unmanaged, the system automatically assigns a stringent level of application access and data protection to it.

The system evaluates the device for compliance to determine if it has the appropriate software and updates installed. A remote health attestation review of a device will also use a variety of techniques to determine if the device is in "poor health" (i.e. vulnerable to attacks or infected with malware). This stops high-risk devices from gaining access to your network before they can do any damage. Depending on how the device performs in its compliance test, a corresponding access level is given to it.



3. Inventory Your Access Scenarios

It's important to map out all access scenarios so you can prioritize where Zero Trust will bring the most benefit the fastest. As you create your inventory of access scenarios, you're listing every possible source (user or device) and/or

destination (resource) that needs to be addressed in your Zero Trust Network. Creating a comprehensive inventory will ensure nothing is overlooked or falls through the cracks. This will also help you identify at least one access scenario that is the most urgent need and would benefit the most from an immediate switch to a Zero Trust approach.

4. Choose your Zero Trust Access Tools

The next step is to choose a Zero Trust Access platform. This is when you'll begin the shopping process and seeing which Zero Trust products on the market might be the best fit. You'll want to consider fundamental questions such as whether you want the platform on-premises or in the cloud.

And as you evaluate which Zero Trust access tools to use, it's important to check if those tools will properly integrate with every SaaS vendor used in your company. As you look at Identity, Security, Device Management, and SAML solutions, you will need to take the time to double-check any integration issues. And this is one big reason why Zero Trust Network implementation should not be a rushed process.

5. Migrate (Rolling Deployment)

The fifth step to implementation ensures no damage is done while transitioning to a Zero Trust approach. The goal is to keep the migration moving forward with caution and without disrupting productivity. This means:

- Incremental deployment
- Deploying from the top down, from the most valuable targets (i.e. EnterpriseAdmins) to the least valuable in terms of content and data

- First deploy management and compliance tools, *then* layer on any conditional access and multi-factor authentication (MFA) for the rest of the company

ZERO TRUST IS A MINDSET, NOT AN EXACT SCIENCE

As you can see from the steps above, there are multiple options in the process. There are many tools and vendors to choose from to help your company create your own version of a Zero Trust Network. There is leeway and room for improvisation within each company when, for example, you conduct a rolling deployment. In other words, it's not an exact science, but the process should generally include the steps above.

Even the idealistic name "Zero Trust" is meant to describe the fundamental mindset behind your cybersecurity strategy, not the literal end-result. Every organization must run on certain levels of trust in its network, but the real question is how to shape the process of granting that trust. Companies need to stop haphazardly throwing their trust to devices and users like candy in a parade. They need to become much more protective of who and what they trust. And that's what the Zero Trust philosophy is all about.

IMPLEMENTING ZERO TRUST SECURITY WITH MICROSOFT 365

While zero trust architecture can be complex, it has been top-of-mind for the engineers at Microsoft, who have built a robust and mutually supportive framework of tools to secure your endpoints, data and infrastructure with a zero-trust methodology.

Azure AD

Azure Active Directory (AD) is the cornerstone of implementing Zero Trust security in Microsoft 365. It operates using a conditional access approach. For example, Azure AD's Identity Protection makes access control decisions that are dynamic. They're done on a case-by-case basis that evaluates each user, device, location, and session risk. This assessment is done for every resource request.

The process does the following, as explained by Microsoft:

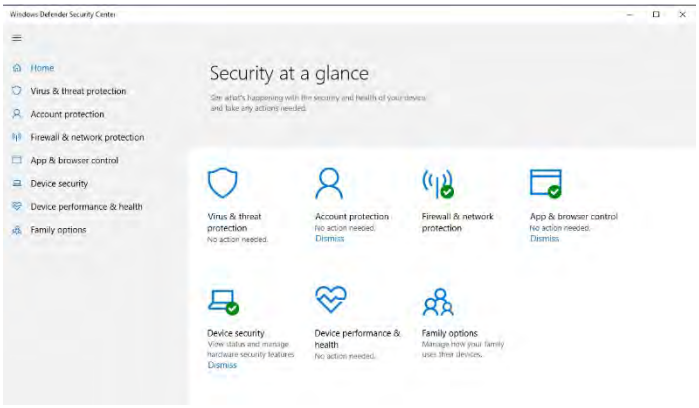
- It combines attested runtime signals about the security state of a Windows device
- It evaluates the trustworthiness of the user session and identity so that it can respond with as strong a security configuration as possible

Essentially, conditional access establishes a set of rules that can be designed to monitor and regulate every scenario in which a user attempts to access your company's resources. That level of control is at the heart of a Zero Trust security philosophy.

Azure AD's role is essential, but it is just one part of a many-pieced whole in Microsoft 365's arsenal. It uses many other tools to establish a Zero Trust Network.

Windows Defender Advanced Threat Protection

Microsoft 365 has an endpoint protection platform (EPP) and an endpoint detection response (EDR) rolled into one powerful piece of technology called Windows Defender Advanced Threat Protection (ATP).



Its capabilities are described by Microsoft this way:

> *[ATP] provides intelligence-driven protection, post-breach detection, investigation, and automatic response capabilities. It combines built-in behavioral sensors, machine learning, and security analytics to continuously monitor the state of devices and take remedial actions if necessary. One of the unique ways Windows Defender ATP mitigates breaches is by automatically isolating compromised machines and users from further cloud resource access.*

Microsoft gives this scenario as an example: attackers are able to extract hashed user credentials from a device by using the Pass-the-Hash (PtH) and "Pass the Ticket for Kerberos" techniques. The attackers then use the credentials to move laterally and leapfrog into other systems.

Other Microsoft tools, such as Windows Defender Credential Guard and System Guard, will prevent these attacks (and even protect the system as it boots up and continues running), but you still need to know when such an attack has happened.

Essentially, Windows Defender ATP brings these attacks to light using its endpoint protection and detection response. It also creates a risk level for the compromised devices that were involved. In the bigger scope of the conditional access approach mentioned above, after ATP assigns a risk level to a machine, this assessment can later be used when deciding to give a token to that advice to access other resources.

Cloud App Security

A tool like Cloud App Security is a necessity in today's unpredictable work environment. Employees come to work with a variety of past experiences and preferences for software and online tools. When an employee brings into the company something they've liked using elsewhere without notifying IT or asking their permission, that employee has unknowingly created what's called "Shadow IT"–when employees bring in third-party programs without having them vetted or approved.

Besides exposing your network to potential bad actors, unchecked Shadow IT can place Personally Identifiable Information (PII), such as Social Security Numbers, or other sensitive company data at risk.

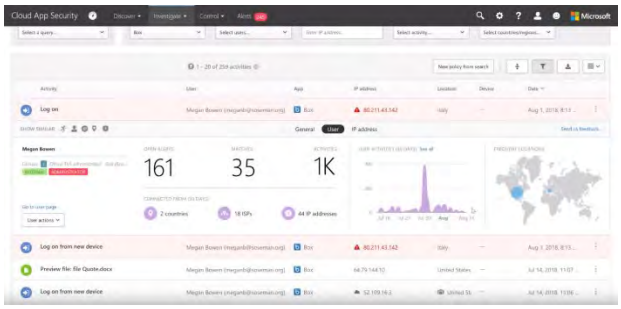
This is why Microsoft 365 has Cloud App Security (CAS), an important tool in its Cloud Security stack. Besides our breakdown of this tool in this article, you can watch our Tech Talk video overview that explains how it assists you in wrangling in the unpredictable elements of Shadow IT.

As Microsoft describes it:

[Cloud App Security] is a comprehensive solution that can help your organization as you move to take full advantage of the promise of cloud applications, but keep you in control, through improved visibility into activity. It also helps increase the protection of critical

data across cloud applications. With tools that help uncover shadow IT, assess risk, enforce policies, investigate activities, and stop threats, your organization can more safely move to the cloud while maintaining control of critical data.

CAS does a wide range of tasks to help you maintain control when Shadow IT sneaks in. The Cloud App Security tool will:



- Import system logs from more than 20 different kinds of Firewalls (i.e. Sonicwall, Watch Guard, Sysco, Palo Alto Networks, etc.)
- Use a custom log format tool so you can use CAS for any logs you have
- Parse a day's worth of logs (for a medium to large-sized business) in only a few hours
- Check and analyze a catalog of more than 16,000 cloud applications and instantly show you on the dashboard how many applications, IP addresses, users, and how much bandwidth use (download and upload) are present
- Provide a concise overview of the most used apps ranked by bandwidth and grouped by type
- Display a list of your top bandwidth consumers with the amount of bandwidth that's been used
- Allow you to click on each data point to see more details and dig deeper
- Provide a locations map that displays every location in the world where the information is being sent

When you click on a country on the map, you will see (for example) old installs of apps that have been left behind. With a click, you are presented with the risk level, security features, compliance certifications, and a display that identifies which users are active in those apps.

You can also access a list of apps in use and filter the list by security score. You can click and see who has interacted with each app. This gives you the insight to detect malware and find the end-users involved as you investigate security incidents.

In other words, it gives you the eyes to see the security weaknesses no matter they are located, the bad actors involved, and the path to resolving the weaknesses.

CAS can also be configured to alert you when certain incidents happen, depending on your security needs. In our video at the top of this section, you can learn more details about this crucial process of using CAS.

Azure Information Protection

Microsoft's Azure Information Protection (AIP) shares similarities with Cloud App Security. Except it is far more powerful. Cloud App Security is designed to protect data in Office 365. AIP goes beyond the cloud and expands to protect on-premise infrastructure.

It is one tool in a unified package that makes up Microsoft Information Protection (MIP). MIP takes the features of Cloud App Security, Windows Information Protection, and Azure Information Protection and unifies

them in a single location where you can manage every aspect of your security.

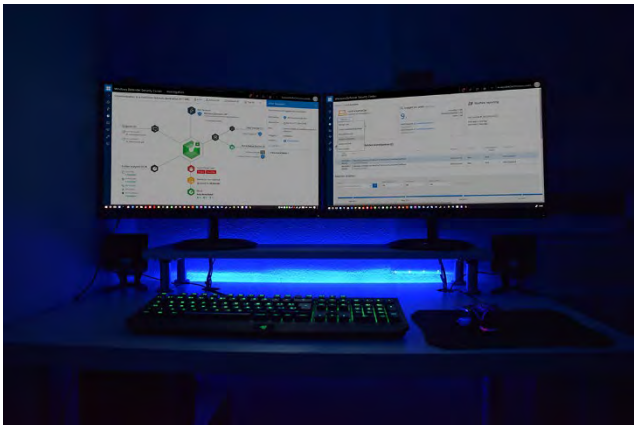
The AIP tool assists you in classifying and protecting documents and emails using labels. Each label type can be customized and applied automatically using rules and conditions you specify or you can apply them manually (or a combination of both using notifications). The labels can apply to identify watermarks, regulate access, control access offline, and set expiration dates on materials that are time sensitive.

AIP is a powerful tool for establishing rules and conditions for your Zero Trust Network. To learn more about the details of how it works and how to set it up to your exact specifications, watch our Tech Talk video on AIP.

Microsoft Intune

Intune is Microsoft's primary tool for managing mobile devices, computers, and applications in an organization. This includes the enrollment, registration, and overall management of all client devises. Along with Azure, Intune has control and visibility of any assets and data that are valuable to the organization. It has the ability to automatically establish trust requirements based on tools such as AIP and CAS mentioned earlier in the article.

Azure Security Center



The Azure Security Center is a collection of security best practices carefully integrated and combined into one software package. Microsoft has taken the hard-earned lessons it has learned from keeping its own data centers secure and placing them all in a user-friendly interface that is mobile-friendly. This means you can instantly access to a world-class enterprise security interface and summary of your company's security status on your mobile device.

To learn more about Azure Security Center, watch our Tech Talk video and see the amazing (and incredibly convenient) features of this tool.

Enterprise Mobility + Security (EMS)

Enterprise Mobility + Security in Microsoft 365 delivers what its name promises: an effective combination of mobility and security on an enterprise level. As you've seen above, Microsoft leverages plenty of brilliant tools to make it happen, and they come together nicely and in a way that's user-friendly and manageable in its EMS package.

As Microsoft explains:

> *...EMS protects across users, devices, apps and data and is specifically designed to work together with Office 365 and Windows 10 to enable security that does not compromise user experience. EMS also secures and manages across thousands of SaaS*

applications, on-premises apps, as well as safeguarding data across iOS and Android devices. Most recently we integrated the management experience for IT into a single easy to use console. All this adds up to an intelligent security solution to support your organization's digital transformation.

To learn more about Enterprise Mobility + Security watch our Tech Talk video and see first-hand how Microsoft makes it so powerful and effective.

Zero Trust Security Means Thorough (and Effective) Conditional Access

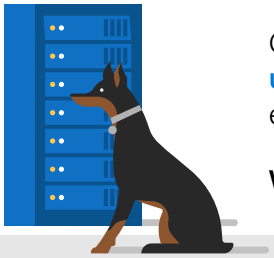
All of the powerful tools above come together to accomplish the objective of Zero Trust security: require all requests for network access to flow through an access control proxy and make all assessments based on device and user trust.

The bottom-line: Zero Trust security means conditional access that is comprehensive but intelligent enough to allow flexibility and productivity. This fits the description for Microsoft 365's security tools nicely.

NEXT STEPS

Agile IT has managed secure cloud migrations for over 1,000,000 users and over 1,500 organizations. Our solutions include Identiyy, Single Sign On, Multi Factor Authentication, Secure Score, Mobile Device Management and Cloud App Security onboarding and management. If you want a head start on securing your devices, data and identities, or want fully managed security as a service, we provide a variety of customized solutions with a fixed price guarantee. To get started on your security journey, **schedule a call today**.

Are you prepared when it comes to security? Many organizations are not.



Cyberattacks can happen any time, any day. They are **scary, costly to remediate, and unfortunately all too common**. This is why proactive protection and security of your IT environment is so important.

WE CAN HELP!

Security Assessments Offered

Pick one, two, or all three of the security assessments below where we will perform detailed analysis of your environments and provide actionable security insights. The ultimate goal: assessing your risks and providing the best solutions to keep your company safe and secure.

OFFICE 365 SECURITY ASSESSMENT

- Identifies security objectives
- Uses security analytics tool to render a security configuration score
- Recommendations to balance security and productivity needs
- Provides guidance on successful implementation of Office 365 security features

Duration: 3 days

Free Consultation

SHADOW IT ASSESSMENT

- Provides insights on cloud usage, security objectives, and requirements
- Helps mitigate security threats with Microsoft Cloud App Security
- Creates a Cloud Visibility and Control roadmap

Duration: 3 days

Free Consultation

RAPID CYBERATTACK ASSESSMENT WORKSHOP

- Identifies security gaps related to ransomware attacks
- Implements Microsoft 365 readiness specific to ransomware defense
- Creates a remediation plan and a Microsoft 365 roadmap specific to ransomware defense

Duration: 3 days

Free Consultation

WHY AGILE IT ?

Agile IT is widely recognized as one of the leading cloud migration and solution providers. We hold more than 15 Microsoft Partner Competencies, including Data Center, Cloud Platform, Identity and Access; recognizing our high levels of technical expertise and customer satisfaction.

C.W. Driver's IT team realized they needed a cloud expert to help them address data security vulnerabilities and eliminate expensive hardware and infrastructure costs.

"Agile IT is well-founded in cloud computing and cloud engineering, so I was confident to move forward with the project."

Blaine Crawford, IT Director

Agile IT
3517 Camino del Rio South #215
San Diego, CA 92108

Schedule Your Call Now!

www.AgileIt.com