at bay

The Cybersecurity Tools Hidden in Microsoft 365

Improve your cyber security by turning on features embedded in software you already use

GREG OTTO
Sr. Security Writer

at-bay.com

Table of Contents

Introduction 3

Microsoft Authenticator 4

Microsoft Secure Score 7

Microsoft 365 Malware and Phishing Protection 9

Cybersecurity Simplified with At-Bay Stance 11

Introduction

Security software can be extremely complex and expensive, especially for businesses that don’t have the budget or expertise to stand up an in-house security team. Luckily, there are ways for businesses to strengthen their cybersecurity posture by using tools inside software they already have access to.

Microsoft 365, used by a million companies worldwide, offers a robust suite of security tools within its core business productivity products. For business owners and IT specialists looking to bolster their defenses, learning how to use these built-in tools could be a cost-effective way to enhance their security posture and avoid a harmful cybersecurity incident.

In this guide, we share some of the top security tools your business can turn on in Microsoft 365 to help it defend itself against cybersecurity threats.

Microsoft Authenticator

Microsoft Authenticator is a mobile app designed to reinforce the security of your company's Microsoft 365 accounts. It adds an extra layer of protection over your users' traditional usernames and passwords by using technology known as multi-factor authentication (MFA).

At its core, MFA relies on two different inputs to confirm an account and allow access. The idea is similar to having two different locks on your door — knowing the key to just one won't grant you entry. In digital terms, one key is something you know (your password), and the other is something you have (your smartphone with the Authenticator app).

Here's a comprehensive look at how Microsoft Authenticator seamlessly integrates with Microsoft 365:

How to Implement Microsoft Authenticator

To begin using Microsoft Authenticator with Microsoft 365:

1. **Download and Install**: Download the Microsoft Authenticator app on your smartphone from the iOS App Store or Google Play Store.
2. **Pair Your Account**: Then, pair the Authenticator with your Microsoft 365 account by signing in through the app or scanning a QR code provided by Microsoft.
3. **Sign-in Process with MFA**: First, enter your username and password into Microsoft 365. Next, check your Microsoft Authenticator app, which will alert you to approve the sign-in, send you a six-digit code, or ask for biometric confirmation (like a fingerprint or face recognition).

Different Microsoft 365 Authentication Methods

There are several ways users can authenticate their logins to Microsoft 365:

→ **Push Notifications**: The app can send a notification to your device, which you can simply tap to approve to login into your account. Conversely, if someone is trying to break into your account, the push notification will serve as a warning that your password has been compromised. This method is fast and convenient, reducing the need to remember a code while still verifying your identity.

→ **One-Time Codes**: Microsoft Authenticator generates a one-time code that you must enter on the sign-in page. This code refreshes every 30 seconds for added security, ensuring that even if a code is compromised, it quickly becomes useless.

→ **Biometrics**: If your device has the capability, Authenticator can use your fingerprint or facial recognition features to verify your identity.

These different methods of account verification give companies options to safeguard their vital accounts. According to Microsoft, 99.2 percent of attacks can be deterred by MFA, so finding the method that best fits your company can go a long way to thwarting cybercriminals.

How Microsoft Authenticator Improves Businesses' Cybersecurity

Authenticator can deter attackers from logging into accounts using trial-and-error (known as brute forcing) or using stolen credentials they have obtained through other attacks. When attackers use company-related credentials to access corporate networks, they often steal data or implant malware. By having Microsoft Authenticator deployed, companies can prevent attackers from accessing their networks and while also determining what corporate accounts are compromised.

Here are some other ways Authenticator improves cybersecurity:

→ **Upgraded Security Posture**: Authenticator's integration with Microsoft 365 means that if a password is stolen or guessed, the would-be intruder still cannot access the account without the code generated for you from the app on your mobile device.

- **Seamless User Experience**: The additional security doesn't come at the cost of convenience. Easy-to-approve notifications and the flexibility of using biometrics, like a fingerprint or facial recognition, make for a smooth user experience.
- **Accessibility in Any Environment**: The app can generate codes without an internet connection, meaning you can still get into Microsoft 365 even when your device isn't online.
- **Versatility Across Other Services**: The Authenticator app is not confined to Microsoft 365 and can be used for securing access to a variety of services that support MFA.

For small business owners and IT experts, adding Microsoft Authenticator to your set of tools is a smart step toward making your defenses stronger. It strengthens a culture of security without compromising ease of access to your business-critical applications — crucial for dynamic business environments that move quickly and need to stay safe from online dangers.

Microsoft Secure Score

Microsoft Secure Score is a tool that helps you check and improve your company's security posture on Microsoft 365. Think of it as a way to get a better understanding of how secure your current setup is and to get advice on how to make it stronger. It can be accessed by logging into your company's Microsoft 365 Defender portal.

How Microsoft Secure Score Works

Microsoft Secure Score looks at your company's safety habits and settings in Microsoft 365 to check how secure your business is. It gives you a score that's based on how things are set up, how people in your organization act regarding security, and other important safety checks. Like a credit score for your cybersecurity, it helps you understand where you stand and what you can do to improve your defenses against threats.

Functionality

Secure Score measures your Microsoft 365 deployment and provides feedback in the following ways:

- **Assessment and Scoring**: Microsoft Secure Score examines various aspects of your Microsoft 365 deployment, including mailboxes, data, device management strategies, and user behaviors.It uses the data and activities from your Microsoft 365 services to assess whether you are aligned with the best security practices.

- **Evaluation Against Security Controls**: The tool measures your organization against a series of recommended security controls. These controls may include actions like enabling MFA, applying proper data governance, securing your identities, and managing device compliance. Each control has a point value. The more controls you implement, the higher your score.

- **Industry Comparison**: Microsoft Secure Score allows your organization to compare scores with historical data and industry averages, giving perspective on how your organization stacks up against other companies of similar size or within the same sector.

Guidance and Recommendations

Microsoft Secure Score provides a list of improvements that can enhance your organization’s security. Each recommended action includes guidance on how to implement it, the potential increase to your score, and how it will impact users. Suggestions are listed in order of importance to help your business concentrate on changes that will really make your security stronger, without making work less convenient.

Action Planning

The Secure Score dashboard allows you to plan and track improvements. You can set a target score and work toward it by following the recommendations spelled out by Microsoft Secure Score. You can also assign tasks to team members, set completion dates, and monitor progress.

By using Microsoft Secure Score, small businesses can really understand their safety habits, pay attention to the most important areas for better security, and see how much they improve over time. It’s a great added feature in Microsoft 365, giving businesses the knowledge they need to constantly enhance their security posture as threats change.

Microsoft 365 Malware and Phishing Protection

Microsoft is a leader in tracking malware due to its global reach, extensive data collection, and advanced analytics, which together enable the company to quickly identify and respond to emerging threats. Exchange Online Protection (EOP) and Microsoft Defender for Office 365 are key in protecting Microsoft 365 instances from dangers that come through email. We've seen first hand how email can be a cybersecurity pain point: In the second half of 2022, 41% of At-Bay's insurance claims originated from a malicious email.

Here's how each of these services work within Microsoft 365.

What is Exchange Online Protection (EOP)?

EOP is an email filtering service that's part of Microsoft 365, and it directly integrates with the cloud-hosted Exchange Online email service. Its main job is to block spam, phishing attempts, and malware from reaching your organization's inboxes. Think of it as your first line of defense, automatically included with Microsoft 365 subscriptions that feature Exchange Online.

EOP delivers:

- **Spam and Bulk Mail Protection**: EOP checks incoming emails using detailed rules and patterns to spot and block unwanted mass emails, which we usually call spam.
- **Malware Prevention**: With the help of a frequently updated database, EOP looks at attachments and links inside emails for any signs of harmful content, helping to protect against familiar threats.
- **Policy Filters**: You can tailor EOP to your business needs by setting up specific policies that can filter or redirect email based on certain criteria, enhancing security and compliance.
- **Reporting Tools**: Administrators can see what's going on with EOP, which provides tools for reports and tracking emails. This helps them check and follow the path of emails as they move through the filtering service.

What is Microsoft Defender for Office 365?

Adding to what EOP does, Microsoft Defender for Office 365 is a service packed with more advanced features to actively protect your emails and teamwork in Microsoft 365. Defender fights against trickier dangers like emerging threats, phishing schemes, and unknown malware, although it may come at an extra fee.

Microsoft Defender includes:

Safe Attachments	This tool scrutinizes email attachments in a safe, isolated “sandbox” before they ever reach the user, identifying and eliminating new and complex malware.
Safe Links	Whenever you click a link in an email or document, the system checks the web address in real time to make sure it’s safe. This helps prevent malicious links from compromising your systems.
Anti-Phishing Protection	By using machine learning and studying how people communicate, Defender for Office 365 can spot when someone is trying to trick you by pretending to be someone else, and then act to stop phishing threats.
Anti-Spoofing Measures	The service uses specific methods to determine if the sender is real, which lowers the risk of bad actors pretending to be other users or using fake domain names.
Simulation Training	IT staff can set up fake attacks in a controlled environment to find weak spots in security rules and how people act. Then, they can use what they learn to guide needed security training and strengthen defenses.
Advanced Threat Hunting and Reporting	Defender for Office 365 offers smart insights on threats, detailed tools for looking into threats, and thorough reports about attacks and patterns. This helps create strong, upfront defenses and better plans for responding to threats.

EOP and Microsoft Defender for Office 365 team up to give your business’s email a multi-layered security strategy. EOP steps in first, blocking the usual email threats before they can do any damage. After that, if necessary, Microsoft Defender tackles the trickier threats that EOP might miss. Together, this pair allows small businesses to stay ahead of attacks, helping them defend themselves before threats can interfere with their operations.

Cybersecurity Simplified with At-Bay Stance

Tools like Microsoft Authenticator, Microsoft Secure Score, Exchange Online Protection, and Microsoft Defender for Office 365 offer a great way to fortify your digital defenses. But cyberthreats change quickly, and staying ahead of cybercriminals can quickly become a full-time job if you don't have the support you need. That's where the At-Bay Stance™ Exposure Manager comes in — we watch for emerging vulnerabilities so you can focus on your business.

Stance Exposure Manager integrates with Microsoft 365 to constantly check for new security threats and alert you when something needs attention. With this tool, you'll know exactly when and how to deal with security problems, and you can get in touch with cybersecurity experts if you need more help.

Continually monitoring our customers' cybersecurity posture is a key tenet of InsurSec, which combines top-notch cybersecurity tools and insurance protection. Our integration with Microsoft 365 isn't just an extra piece of InsurSec — it's a key part of a full defense plan. By using this Stance Exposure Manager integration alongside Microsoft's built-in security tools discussed above, you can have a cybersecurity plan that won't slow down your business.

Already an At-Bay Stance Exposure Manager user? Learn more about how the Microsoft 365 integration with At-Bay Stance Exposure Manager can supercharge your cybersecurity strategy.

Not yet using Stance Exposure Manager? Now's the perfect time to start. Get unprecedented visibility into your cybersecurity posture, where your business is vulnerable, and what to do. To learn more, contact our Stance Advisory Services team or send us an email at security@at-bay.com.

This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form. At-Bay Insurance Services LLC is a licensed insurance agency and surplus lines broker in all fifty states and the District of Columbia.