

ATTIC

FOR MICROSOFT 365

**WORLD CLASS CYBERSECURITY
FOR OFFICE 365 AND AZURE
ACTIVE DIRECTORY**



FIX YOUR DIGITAL SECURITY

Attic is the first cybersecurity service, attainable for SMBs. With proactive remediation of unsecure SaaS configurations, Attic ensures that your online business remains resilient.

Attic for Microsoft 365 allows you to quickly improve security of Office 365 and Azure Active Directory.

As cyberattacks on SMBs continue to rise, it's crucial to realize that no business is immune to threats like whaling or ransomware. The increased use of cloud-based services has resulted in an expansion of attack surfaces for both SMBs and larger enterprises. Most organizations today rely on some form of online service to accelerate and streamline their business.

But with this increased reliance on technology comes the challenge of protecting your business against the ever-growing number of cyber threats. That's where Attic comes in – providing a simplified yet effective solution to the complex problem of cybersecurity. With Attic for Microsoft 365, you can rest assured that your business is safe and secure.



Attic for Microsoft 365 helps you to work safely online in Office 365

11
seconds

Once every 11 seconds a ransomware attack is carried out somewhere.

Source: Cybersecurity Ventures

78
percent

78% of all Microsoft 365 users does not use multi-factor authentication.

Source: CoreView

50+
checks

Attic performs over 50 checks, many of which include automatic fixes.

For various Microsoft 365 settings

1
critical alert

Admin has disabled MFA. Click approve to turn it on again.

Example of Attic security alert, including suggested actions.

SECURE YOUR BUSINESS WITH ATTIC

Attic for Microsoft 365 helps to protect businesses against cybercriminals by automating their security through an easy-to-use interface. The Attic app is linked to your Microsoft 365

environment over a dedicated, secure connection, and automatically verifies all settings to identify potential vulnerabilities.

After a one-time setup for your systems, the Attic app will work seamlessly in the background.

Attic not only detects problems, but in most cases also suggests a solution. The app will notify you of any identified vulnerabilities in Microsoft 365, including a one-click fix for many known problems. Our system will ensure that everything is set up correctly so you can safely focus on running your business.

Key to Attic is the automation of cybersecurity in order to make Zolder BV's service both scalable and affordable. This means that SMBs can get easy access to enterprise-grade cybersecurity and stay informed of their security status anywhere and anytime – in the office, at school or even on the football field.



HOW DOES IT WORK?

Once we've convinced you that Attic is the best way to quickly and easily secure your Microsoft 365 environment, we will get to work to prepare the system. In order to deliver our service, Zolder BV must be registered as a Cloud Solution Provider (CSP) in your Microsoft 365 subscription. We can then create a link to your company, through which Attic can access your settings and change them if necessary.

Attic will send a request for a CSP link to one of your Microsoft 365 admins.

CHECKS & FIXES

The key to Attic's functionality is Checks & Fixes, a continually expanding script library that checks your Microsoft 365 environment for vulnerabilities. These scripts are executed in the background with a set interval of, for example, 15 minutes. Each script uses an API to check a specific setting in the Microsoft cloud and generates an alert if the setting deviates from the preferred optimal situation.

For example: multi-factor authentication is set up for all company users, and one of them disables this security setting. This would enable attackers to get access to your systems more easily, so Attic generates an alert.

The alert is logged as a service ticket in the app and a push message is sent to inform you of the issue. Notifications can also be sent to one or more email addresses to ensure the problem is resolved as soon as possible.

In this example, in which MFA is disabled, you can restore the correct settings by applying the Fix in the Attic app with a single touch of a button.

Need help? You can contact our Service Desk for help with every service ticket. This way, Attic helps to keep your system secured at all times.



ATTIC = SPEED

Securing your online business means that vulnerabilities must be resolved without delay. Attic's fully automated processes run at fixed intervals. The amount of time it takes for potentially suspicious behavior to occur, to be detected, and to be remediated is determined by the following factors:

1. Check interval

All checks in Attic are configured with a minimum interval of 15 minutes. So, if, for example, a user disables MFA, Attic will generate an alert after a maximum of 15 minutes.

2. Customer authorization

The fixes Attic suggests must be approved by an administrator before implementation. To speed up this process, automatic authorization can be set for certain fixes in advance. Pre-authorized fixes are applied in a matter of minutes, keeping your systems optimally secured at all times.

3. Sentinel processing time (optional)

Attic M365 Monitoring creates a link with Microsoft Sentinel. Just like every Security Information and Event Management (SIEM) solution, Sentinel requires some internal processing time before a logged event triggers an alert. This usually takes no more than 30 minutes.

SENTINEL MONITORING



Microsoft Sentinel is part of your organization's Microsoft 365 subscription and a free SIEM solution available to all Microsoft subscribers.

It is possible to stream a number of log sources in the Microsoft cloud to Sentinel at no extra cost. Microsoft will charge you for other log sources in their cloud and external sources, such as firewalls.

To enable Microsoft365 Monitoring in Attic using Sentinel extra onboarding is required, as a link must be created to an Azure Subscription. This enables Microsoft to charge you for adding extra log sources. Activation of these log sources in Attic is only done after explicit customer approval to avoid unexpected costs.

After onboarding, all free log sources are added, and Sentinel correlation rules are activated. These rules trigger alerts when suspicious behavior is detected. Sentinel alerts are handled in the same way as our Checks & Fixes.

PERSONAL DATA

As a CSP and security monitoring service, Attic needs access to the personal data of your Microsoft 365 users to function properly. This access is subject to our Privacy Statement and Processing Agreement, which also describes our specific activities.

Attic does not use personal data to generate alerts. In case an alert is generated that relates to an employee, for example an admin, only their email address and name are collected in order to provide targeted remediation advice.

SECURITY

In addition to personal data protection as described in the Processing Agreement, several important security measures apply.

Changes

Attic makes no changes without explicit customer approval. We recommend setting up an internal change management process to ensure smooth processing of changes suggested by Attic. Our Service Desk is ready to assist you if any change leads to unexpected results and a rollback is required.

Secure Application Model

The CSP link between Attic and the Microsoft 365 environment is created from a management tenant that is entirely separated from Zolder BV. The link adheres to the Secure Application Model for CSPs required by Microsoft.



THE ATTIC TEAM

Attic is developed by the world class cyber experts of Zolder BV, who have more than 70 years of accumulated experience in the area of cybersecurity and ethical hacking.

Zolder's mission is to apply this expertise to provide affordable solutions and enable SMBs to secure their online business.



**Zolder
Founders**



DO YOU WANT TO FIX YOUR ONLINE SAFETY?

Visit our website and start your subscription today! Thanks to Attic's approach to automation your online business can be better secured within 24 hours.

www.atticsecurity.com

ATTIC
FOR MICROSOFT 365