Microsoft 365 Security Assessment

On the way to a secure digital workplace

Cloud applications and mobile devices make companies choose a digital workplace. And for good reason. Digital working increases your efficiency, makes your employees happier and ensures that you can give your clients a better service. The Microsoft 365 Security Assessment helps you make a secure transformation to the digital workplace.

The security challenges of your digital workplace

In the digital workplace, a growing number of cloud applications are accessible from every mobile device. And also from your employees' often unsecured devices and networks. This is a sure way to expose your organization to new cyber threats, which traditional security methods cannot adequately protect against.

You run the risk of:
> Losing control over your cloud applications and company data.
> Leaking sensitive company and client data by means of malware, phishing, hacking, theft of log-in data or an employee error.
> Breaching GDPR legislation.

In this fast-changing world, you can keep pace by implementing the right security strategy and measures.

proximus enterprise

Achieving a secure digital workplace

The Microsoft 365 Security Assessment gives you a **realistic and extensive overview** of:
> The cyber**security risks** that you are faced with **right now**.
> The **threats** that you will be facing **in the future**.

Together with you, we make a **detailed plan** to tackle the risks and threats as efficiently as possible, to enable your employees to work securely when on the go, and to protect your company data. We start with a **workshop** and you will receive a **user-friendly roadmap to optimize your security strategy**.

During the assessment your employees can continue to work uninterrupted, and we keep the workload on your IT department to a minimum.

Your Microsoft 365 Security Assessment in 5 steps

A **standard Microsoft 365 Security Assessment** takes about **1 month**. You can supplement the assessment with extra **workshops or managed services that we tailor to your company's needs**.

The assessment consists in:

1. A pre-engagement meeting	**2.** Kick-off workshop and technical set-up	**3.** Collection of all data (4 weeks)	**4.** Workshop Microsoft 365 – collection of issues and preparation of the report	**5.** Presentation of the report

During the entire evaluation **we minimize the workload** on your IT teams as far as possible, and the evaluation has absolutely no impact on your end-users.

In your own Microsoft environment
We only use Microsoft tools to analyze your security logs and warnings. Moreover, **we process all information in your own Microsoft tenant**. This means that your data remain secure in your own environment.

Including evaluation of real security breaches
In your evaluation report, we not only evaluate your cybersecurity policy and measures but we also include a number of security issues that occurred at your company during the period in which we collect your data.

After the assessment
We are also there to help after the assessment, if required, for the configuration and management of your cybersecurity.

Why Proximus?

> More than **15 years experience in cyber security**.
> Experience **in all sectors**: services, industry, finance, government, …
> Our **Microsoft Gold Partner for Security** award means that you are guaranteed the best service and the best advice at all times.

Find out more?

Contact our expert via proximus.be/security contact

proximus enterprise