CASE STORY: FIT

About FIT

The Flemish government created Flanders Investment & Trade (FIT) in 2005. This agency supports Flemish companies as they expand their activities abroad, and helps foreign companies find Flemish suppliers of quality goods and services. FIT has its headquarters in Brussels and 70 offices all over the world.

About SecWise

SecWise is a team of cloud security experts, dedicated to help our customers with cyber security and compliance in their digital transformation to a cloud and mobile work environment. Due to the increasing use of cloud infrastructure and mobile applications, the perimeter to protect is getting bigger. Our mission is to ensure that security does not stand in the way of increasing productivity and the accompanying digital transformation, on the contrary, that it can facilitate this transition in a secure way.

SecWise secures FIT's cyber-doors to prevent attacks

In 2015, Flanders Investment & Trade launched an IT strategy to systematically switch to the cloud. With headquarters in Brussels, five offices in Flanders, and 70 offices with over 250 employees abroad, this was quite a task. At the same time, in addition to traditional centralized perimeter security control, attention also had to be paid to decentralized cyber security. After conducting various security audits and evaluating several security applications, FIT opted for the Microsoft 365 Defender suite. ***"Not only does this solution lend itself very well to our cloud-only approach; Microsoft also scores very highly in security benchmarks"***, says IT Team Manager, Kurt Spitaels.

What are the key take-aways?

- FIT switches fully to the cloud
- The organization secures its cloud-only approach with the Microsoft 365 Defender suite
- FIT now has a much better overview of all its security and any possible breaches

Remarkable numbers

- FIT implemented all M365 Security components
- 400: employees now work securely in the cloud
- 5: months for all devices and cloud servers to be protected by the new security solution

Stimulated by the classic benefits – flexibility, operational cost, no more hardware, decentralized and accessible from anywhere, etc. – Flanders Investment & Trade's journey to the cloud is constantly gaining new destinations. The organization has been gradually replacing its on-premise IBM Domino environment with Microsoft Azure, Microsoft Dynamics and Office 365 including Exchange and SharePoint since 2015. It has also added Skype for Business with PSTN connectivity, and is now using Microsoft Teams with Direct Routing to PSTN. FIT has a pioneering role to play here.

FIT contacted SecWise, a cyber security specialist from Cronos Groep, to provide robust security for all its cloud applications. "After all, Microsoft secures its centralized data centre, but not so much its user set-ups. We therefore asked SecWise to analyse where there might be any holes in our security strategy. They carried out an assessment with penetration and cloud security testing over five days, before drawing up an implementation plan consisting of four phases over five months", says Spitaels.

Migration to the Microsoft security suite

While making this switch to Microsoft Teams and renewing its licence, FIT realised it was already very close to Microsoft's E5 licence, which includes the Microsoft 365 Defender suite. "This suite is perfectly aligned with our decentralized and cloud-only approach, and our Microsoft portfolio in particular. ***Its integration is naturally a much closer fit than for other providers, which helps keep us a few steps ahead of any attackers.*** A fragmented system without any flow of intelligence, on the other hand, can give you a false sense of security", says Spitaels. "I also need to limit the number of products for our small IT team. I can't just go and recruit 20 experts for each security application. And Microsoft is covering more and more aspects all the time."

> ***The robust integration of Microsoft 365 Defender with other Microsoft applications offers a number of significant security benefits. If your security is fragmented, without a good flow of intelligence, you have a much less integrated overview and a false sense of security.***
>
> *– Kurt Spitaels, IT Manager at FIT.*

In the first phase, FIT secured all its Microsoft Office 365 applications and activated Office 365 Advanced Threat Protection, which blocks any spam and malware emails, among other things. At the same time, FIT also applied Microsoft's Zero Trust model with Conditional Access to provide further protection for computers and users. "We don't trust anyone and there's an extra condition for gaining access: the user needs to use an authenticator app with multi-factor authentication to sign in. So if there's a login from Brussels, for example, and then another one from Mogadishu two hours later, we receive an 'impossible activity' alert. All these alerts are monitored and investigated systematically: checking false notifications, resetting passwords, blocking connections, and so on."

> ***If there's a login from Brussels, and then another one from Mogadishu two hours later, we need to see flashing lights and run our security checks.***

Strict control of FIT devices

In a second phase, FIT started using Microsoft Endpoint Manager (Intune) software for its device management. “We manage and configure all our employees’ computers and phones worldwide. All our computers come from Brussels, and phones are purchased locally. Defining the policies with Endpoint Manager means we can ensure that someone can only use Microsoft Outlook, for example, and not the native app on the device. And ***we can even clear all the data from a device remotely, if necessary, in the event it is lost or stolen***”, says Spitaels. For optimal cyber protection, in a third phase, FIT also installed Microsoft Defender ATP on its employees’ computers, and Azure Advanced Threat Protection to protect against lateral movement attacks.

In a final fourth phase, the organization activated a new Azure Security design to protect the public cloud environment. Koen Jacobs, Managing Partner at SecWise: “Companies often limit themselves to a lift-and-shift approach when moving their applications to Azure, but you also need to modify the security. We find doors that aren’t properly locked during almost every assessment we carry out. We also developed a security reference framework or ‘security governance’ for FIT.”

Make it as difficult as possible for hackers

FIT has taken huge strides forward with its cyber security over recent years, but it remains a constant point of attention. ***"Hacking attempts used to stay under the radar much more easily"***, admits Spitaels. "Increasing our security makes it more difficult for hackers. Don't forget that we live in cyber-sensitive countries, and sometimes circulate sensitive information. But we have a much better overview of all our components now, and we receive more alerts faster when any potential malware is detected."

This is one of the main reasons why FIT joined forces with Cronos and SecWise. "We found that they had the right profiles and experience. Top-notch security requires funding but we cannot do things half-heartedly. Security is too important. SecWise helps us maintain our security maturity at all times, and are constantly trying to cover any weaknesses. That's why we've also looked to them to do our initial screening of alerts and help develop our Shadow IT. Security is a journey, not a destination."