ACEN

Federal Planning Bureau
Analyses and forecasts

REFERENCE CASE - Federal Planning Bureau

A permanently secure and compliant digital workspace

About Federal Planning Bureau

Federal Planning Bureau is an independent federal public institution that produces forecasts and analyses on economic, social, and environmental issues for the Belgian federal government. In doing so, they support political decision-making through objective figures and facts.

With a team of around 100 employees, including 75 researchers, the organization relies entirely on a stable and secure Microsoft 365 environment to support its operations and complex econometric models. As a result, the Federal Planning Bureau operates within a 100% Microsoft-based ecosystem.

The IT team responsible for keeping this Microsoft 365 environment secure and running consists of 8 people. Four experts are develop tools that support the complex research models full-time, while the other four focus on managing, maintaining uptime, and securing the overall infrastructure.

Federal Planning Bureau
Analyses and forecasts

The challenge

Following ever-evolving and stricter cybersecurity measures (e.g., NIS2) and increasing pressure from other government institutions, Federal Planning Bureau was forced to review its security and upgrade to a managed security solution.

Prior to the migration to this managed security solution, Federal Planning Bureau's IT team identified several critical challenges:

NIS2 legislation:

As an independent government agency, Federal Planning Bureau must comply with strict standards. The need to demonstrate that they are "in control" was a direct trigger to look for a professional solution. Additionally, proactively complying with NIS2 guidelines adds major value to their compliance, proving in black and white that Federal Planning Bureau is a secure and reliable partner to all stakeholders.

This was not purely about legal compliance, Federal Planning Bureau places immense value on being able to prove this compliance towards stakeholders. With NIS2 they reinforce their role as reliable partner for all federal services that entrust them with sensitive data

Unattainable specialization:

Managing and securing an M365 tenant has become a full-time job. "A policy you configure today might already be outdated within two weeks," says Johan Duyck, IT Coordinator at Federal Planning Bureau. Staying up to date within this specialization is therefore a must.

Operational pressure:

With a team of only eight people, setting up 24/7 monitoring in-house was simply impossible without losing focus on core activities.

"We realized more and more that managing an M365 environment is a job on its own. You have to be highly specialized to keep up with Microsoft's fast-changing roadmap."

Johan Duyck, IT-coördinator at Federal Planning Bureau

Security as a Service: It's not just tools, it's a whole team!

During the search for an suitable solution, complex and expensive solutions specially designed for thousands of users were recommended by other government institutions. These 'bazooka solutions' are not really suited to organizations like the Federal Planning Bureau, with its need for flexibility and smaller user base.

Instead, Federal Planning Bureau chose a flexible and high-quality partnership with ACEN. The partnership is built on three pillars:

1 ACEN managed Microsoft 365

Using intelligent tooling, ACEN scans the M365 tenant daily for misconfigurations, unusual exceptions (such as conditional access) and new security features. In addition, regular meetings take place between the dedicated ACEN expert and Federal Planning Bureau to report results, analyze data and take proactive action.

2 24/7 managed SOC

A specialized team from ACEN monitors the environment day and night, ensuring potential incidents are immediately detected and followed up. Alerts are smartly filtered and prioritized. This avoids alert fatigue and ensures fast & targeted action. Furthermore, a concrete incident response plan has been drawn up in the event of a potential incident.

3 Action Pack Units (APUs)

A flexible package of service credits used for proactive improvements on the established roadmap, extra consultancy or other specific ad-hoc security projects.

This pre-approved budgetary model ensures maximum flexibility and speed (eliminating the need to repeatedly draw up new quotes and/or request approval from various decision-makers). This way of working allows ACEN's experts to get straight to work without losing time, which is crucial in the cybersecurity sector.

"Securing a Microsoft environment has become a specialization in itself due to constant updates. With this model, an organization doesn't just buy standalone tools, but the guarantee that their security posture remains up to date 24/7."

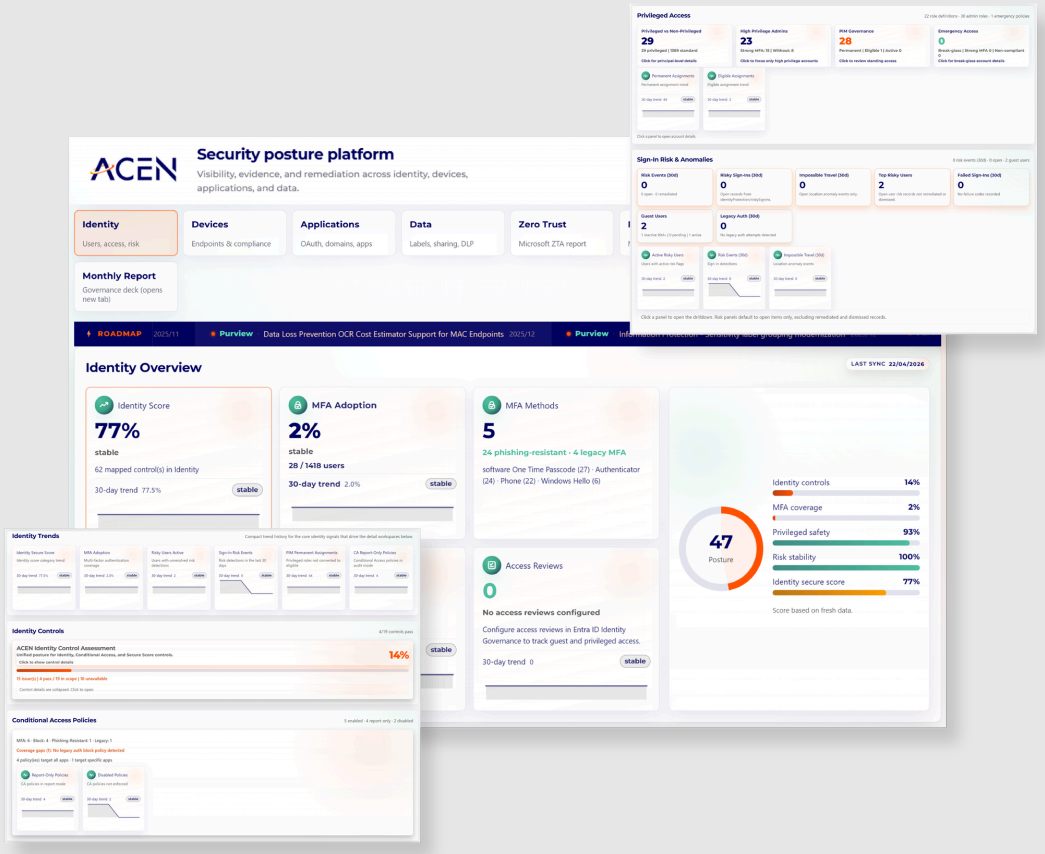
Jahirt Ruiz, Cybersecurity Expert at ACEN

The Result? Direct and measurable!

The switch to the managed model has brought several benefits:

Fast Implementation: The implementation process took place in several phases and was fully completed within two months. Thanks to excellent cooperation (and short lines of communication) between the experts on both teams, the end user experienced absolutely no disruption to their daily tasks during the implementation.

Time Savings and relief: The internal team is no longer burdened with the daily stress of security updates. They now have "a whole team of experts" at their disposal instead of an internal employee who may not even specialize in cybersecurity.

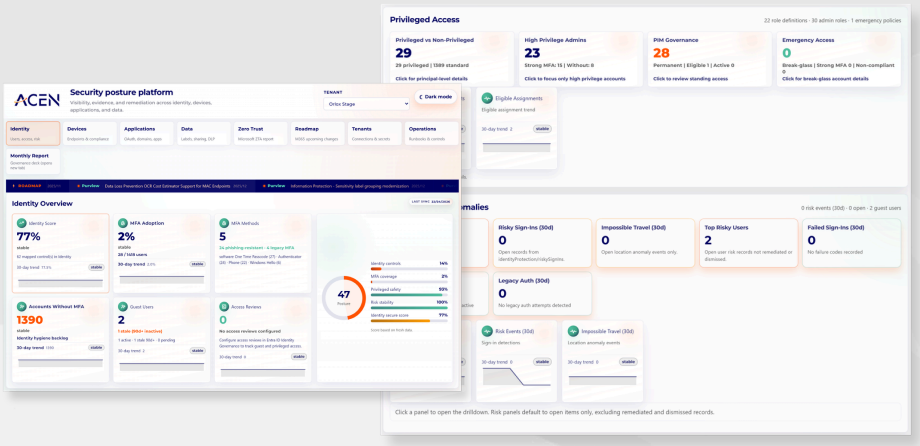


3. Peace of mind:

Thanks to the incident response plan and proactive monitoring, there is a clear sense of security within the organization. ACEN experts are on hand around the clock to intervene should an incident occur.

4. Compliance certainty:

Federal Planning Bureau now has a clear mapping of existing permissions and policies, resulting in greater control. From now on, they can prove that they meet all necessary security needs; to data providers, other federal government services and external parties. Furthermore, the NIS2 guidelines are firmly embedded into the cybersecurity roadmap.



ACEN – A Remote colleague

The collaboration between ACEN and Federal Planning Bureau is built on mutual trust. ACEN holds administrator rights and can therefore intervene immediately in the event of a threat or incident.

ACEN can also independently adjust certain configurations after consultation with Federal Planning Bureau. **Communication between both parties runs smoothly via short lines** (such as a shared Teams group) which drastically increases response speed compared to traditional ticketing systems..

"I was able to convince our management that with ACEN, we are bringing in a team of professionals who are ready 24/7. That takes an enormous amount of pressure off my own team."

Johan Duyck, IT-coördinator at Federal Planning Bureau