STORMSHIELD

CUSTOMER CASE

Court of appeal in Katowice: a new centralised infrastructure

JUSTICE

The war in Ukraine and in cyberspace, the ongoing need for public institutions to adapt to an evolving cybersecurity landscape, and the necessity to ensure continuity and security of operations – these are the three main reasons why the Court of Appeal in Katowice introduced French manufacturer Stormshield's solutions across all 37 subordinate units.

Long-standing cooperation

In 2020, the world was gripped by the coronavirus pandemic, and most organisations were forced to accelerate digital transformation.

At that time, the Court of Appeal in Katowice decided to centralise its infrastructure. This meant, among other things, that all UTM devices in each of the court's regional units should come from a single manufacturer. Stormshield was chosen without hesitation.

"Stormshield is not new to our organisation. Before 2020, around 50% of the courts in the Katowice appellate district were already using Stormshield. Since it had been our main UTM solution and had proven itself under our conditions, we were pleased to learn – after defining the requirements and completing the procurement procedure – that Stormshield devices would be deployed across all units. It made sense both from a budgetary and technical standpoint, as it was crucial for us to be able to design the devices as clusters."

Piotr Pałys
IT System Administrator
at the Court of Appeal in Katowice

The implementation took only three months across all units. Common global policies for all courts have been developed and UTM firewalls have all been attached to the central Stormshield Management Center console, while also creating specific local rules and migrating from previous solutions.

Stormshield's hidden strengths

The fundamental role of UTM firewalls in any organisation is to block unwanted external traffic. In addition, for some institutions, other features are also important, as they enhance digital resilience and improve task efficiency. For example, sandboxing and the user-friendly Stormshield Management Center console, which allows all 74 firewalls to be managed from one place – a huge aid to daily operations. It is also vital that the court's administrators can rely on support from both the manufacturer and the technical department at DAGMA IT Security when expanding the infrastructure.

What does the Stormshield infrastructure at the Court of Appeal in Katowice look like?

Over 70 devices were deployed across 37 units, and as representatives of the organisation stress, this was done at lightning speed. The first step was preparing the implementation project with its individual stages.

SOLUTIONS USED

- → SN210
- → SN710 / SN720
- → SN910 / SN920
- → SN3100

"We've known Stormshield solutions for years, but even so, during implementation, support met with us twice to introduce functionalities we hadn't previously used, like 2FA. It wasn't just about implementation, though. With a deployment of over 70 devices, we occasionally encounter unusual technical challenges. Of course, we're able to resolve most of them ourselves, but when we can't, the engineers at DAGMA IT Security and Stormshield offer the technical expertise we truly need."

Piotr Pałys
IT System Administrator
at the Court of Appeal in Katowice

When war broke out in Ukraine in 2022, most public institutions had to further strengthen their cybersecurity to better monitor and respond to potential incidents and threats. The Court of Appeal in Katowice proactively introduced additional safeguards such as geolocation-based IP address blocking.

Thanks to blocking traffic from Russia and Belarus, all the devices are protected against cyberattack attempts from those regions. There was no serious attack, partly because Stormshield firewalls effectively block any such attempts.

Implementing MFA and Yubico keys

A very important security aspect for the Court of Appeal in Katowice was enabling 2FA, particularly for users connecting via VPN. Engineers from DAGMA IT Security demonstrated a solution enabling Stormshield devices to use RADIUS-based authentication with Yubico hardware keys. The presented system integrates with the existing UTM setup, expanding its functionality. Management is simple and intuitive – a key advantage in such an extensive environment.

Plans for the future

Representatives of the Katowice court emphasise that cybersecurity is an ongoing process. Therefore, further changes to both infrastructure and security policies are planned across all units.

"Our environment is continuously monitored, functionalities are being expanded, and required licences are being renewed. In 2025, we plan to replace the older series of devices with the latest ones featuring TPM modules, performance upgrades via licensing, redundant power supply, and full compatibility with the newest firmware. Our goal is continuous development and implementation of the latest defence mechanisms."

Piotr Pałys
IT System Administrator
at the Court of Appeal in Katowice

Selecting the right IT security solutions is not just a matter of technology, but also of risk and cost management strategy. Key aspects include protection against threats, licensing transparency, and compliance with legal data requirements.

Compared to competitor devices, Stormshield has significantly fewer vulnerabilities and is subject to fewer attacks, which is extremely important from our perspective. It's also important that data is stored in data centres within the European Union. And most importantly, Stormshield's licensing is structured in a practical way, allowing clusters to be used at a lower cost than with global solutions.

Version 1.0 - Copyright Stormshield 2025