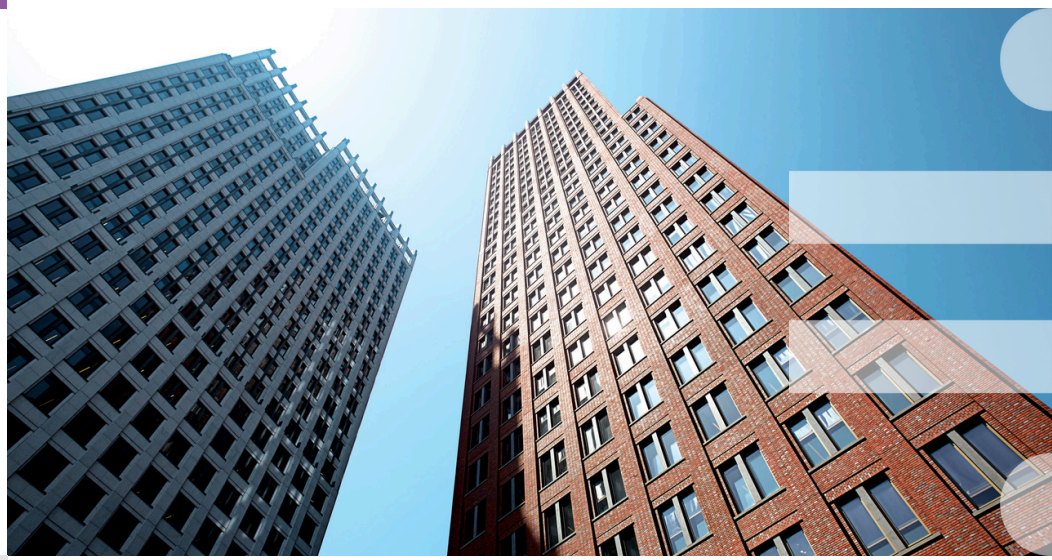
CASESTUDY

Ministerie van Justitie en Veiligheid

The Ministry of Justice and Security relies on the **Trusted Cloud for secure digital innovation**



GOALS

- Secure and controlled use of the cloud in accordance with GDPR and BIO
- Enable digital innovation for all departments of the Ministry of Justice and Security
- Ensure continuity and compliance in a complex IT landscape
- Maintain trust and control when making technological choices

SOLUTIONS

- Development of the Trusted Cloud: A shielded cloud environment with its own policies
- Access exclusively via the internal JenV network (Express Route via JuBIT)
- Four-eyes principle and review for change management and security
- Structural collaboration in the Cloud Center of Excellence, innovation sprints, and policy development
- Preventive software code scanning and continuous policy enforcement by Solvinity

Trusted Cloud as a secure compass

The Ministry of Justice and Security (JenV) is responsible for our legal order, a system in which people must be able to live together, regardless of their beliefs or lifestyles. The ministry also works towards a safer and more just society. This is done in cooperation with partners such as municipalities, educational institutions, businesses, inspectorates, and the Tax Administration.

Innovating while maintaining control

Within the ministry, everything revolves around security, transparency, and preventing data leaks. At the same time, the need for digital innovation is significant. The move to the cloud was a logical choice due to its flexibility, scalability, and technological possibilities. On the other hand, there are also risks. “Our main concern was: are we sufficiently in control if we move to the cloud?” says Remco Boersma, enterprise architect at JenV. “A single mistake by a user could be enough to unintentionally expose systems. That was a risk we could not take.”

JenV wanted a stable and flexible environment that enables innovation while fully complying with all requirements regarding legislation and regulations such as GDPR and BIO, as well as its own security policy. Together with Solvinity, provider of secure managed clouds, JenV developed the Trusted Cloud: a virtual data center in the public cloud, shielded from the internet and accessible only via the ministry’s internal network.

> *“The Trusted Cloud gives us the space to innovate without compromising on security and control.”*
>
> **Remco Boersma,** Enterprise Architect, Ministerie JenV

“The Trusted Cloud is essentially a public cloud, but with a trusted layer around it,” says Boersma. “We have implemented both technical and organisational measures. For example, approval from multiple parties is always required for changes. This six-eyes principle helps maintain the balance between control and progress.”

RESULTS

- Compliance with GDPR and BIO, with shared responsibility between JenV and Solvinity
- Enhanced digital resilience through real-time monitoring and direct logging to the SOC
- Scalable capacity and secure, flexible deployment of technologies such as GenAI and machine learning
- Proactively prepared for exit strategies and European cloud options to enable greater digital autonomy

ABOUT MINISTRY OF JENV

The Ministry of Justice and Security (JenV) is responsible for the rule of law in the Netherlands and works towards a safe and just society. They provide legal protection and intervene when necessary. The ministry is involved in legislation in the areas of civil law, criminal and sanctions law, and administrative law, and oversees the quality of the legislation.

ABOUT SOLVINITY

Solvinity provides Secure Managed Cloud services to government institutions, municipalities, and the financial and business sectors. With these services, the company supports organisations with high security requirements in their digital transformation. In addition, the company offers CI/CD, container technology, and 'Stretched' DevSecOps solutions. The organisation distinguishes itself through very high standards for cybersecurity and certifications according to (inter)national norms, including SOC 1 and SOC 2 on both the Solvinity cloud and Azure.

Solvinity
Secure Managed Cloud

Controlled innovation
The combination of technical security, policy enforcement, and joint governance within the Trusted Cloud ensures full compliance with GDPR and BIO. Checks and balances determine whether new applications are suitable for the Trusted Cloud, guaranteeing both manageability and trust. Software development for the ministry also follows strict rules. New code is thoroughly scanned together with Solvinity before being granted access to the Trusted Cloud. This way, JenV prevents vulnerable or non-compliant software from unintentionally entering the environment.

Based on this clear approach, the Trusted Cloud creates space for controlled innovation. The ministry can safely deploy new technologies such as GenAI, machine learning, or text-to-speech applications. Temporary peaks in capacity can also be absorbed flexibly. In this way, the Trusted Cloud supports digital renewal without compromising on security or compliance.

> *"Our long-term partnership with Solvinity provides trust, transparency, and innovative solutions that fit our unique challenges."*
>
> **Remco Boersma,** Enterprise Architect, Ministerie JenV

Trust and Shared Responsibility
JenV and Solvinity have been working together for more than ten years. Over that time, the relationship has grown into a partnership where openness, knowledge sharing, and flexibility are central. For example, Solvinity is part of the Cloud Center of Excellence, where both parties share and combine knowledge and experiences. "Our collaboration goes beyond a classic client-supplier relationship. It's not a case of 'you ask, we deliver'," says Boersma. "Together, we set up JuBIT (Justitie Beveiligde Internet Toegang). They know our organisation and translate technical possibilities into practical and secure solutions. Solvinity is always looking for the question behind the question. There is definitely room to explore together what is and isn't possible within our policy and environment."

To safeguard security, both organisations handle monitoring, logging, and compliance together. Solvinity provides the technological foundation and is responsible for the infrastructure, policy enforcement, and logging. The log data goes directly to the ministry's Security Operations Center (SOC), allowing the ministry to act quickly and effectively in case of deviations, incidents, or policy violations. The Trusted Cloud thus offers not only control but also complete transparency.

Digital Autonomy and Alternatives
JenV and Solvinity look ahead together, from exit strategies to European cloud alternatives. All strategic issues are on the table. For governments, these are highly relevant topics. This also requires not just technological, but administrative decisions. For example, reducing dependence on foreign tech companies, safeguarding digital sovereignty, and future-proofing the IT infrastructure.

That's why the ministry is preparing for alternatives not only technically, but also in terms of policy. "What if we want to move away from the public cloud? Can we move back, or switch to another environment?" Boersma concludes. "We need to develop, test, and demonstrate these scenarios. Solvinity helps us proactively address these challenges."