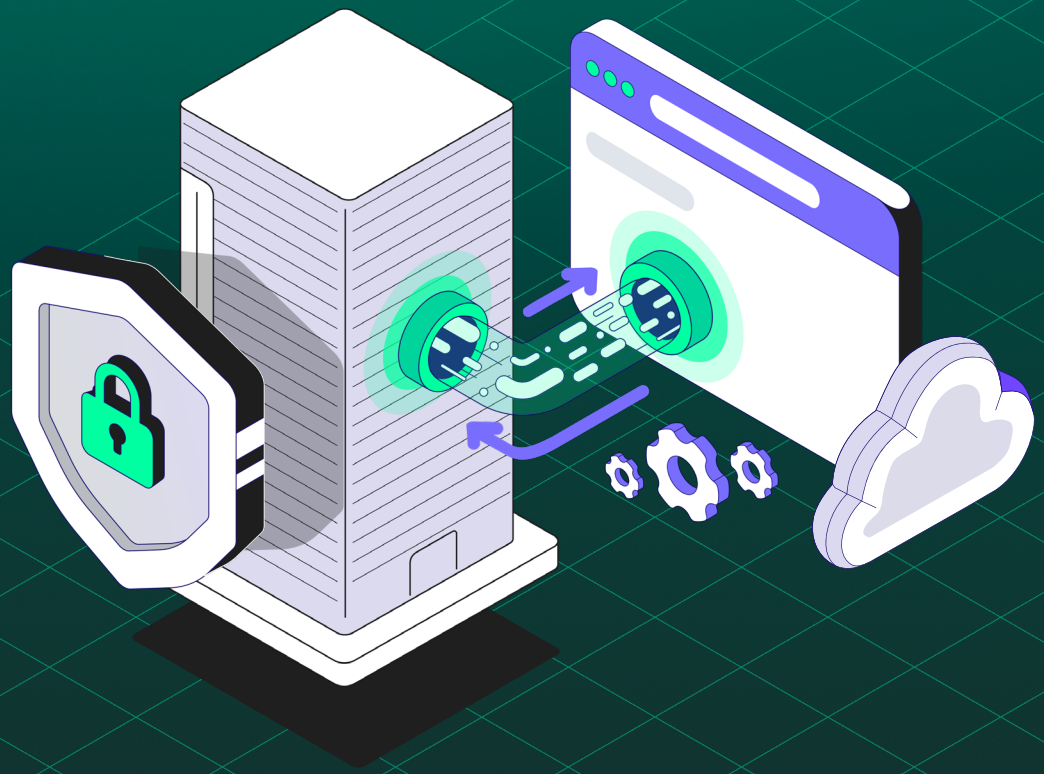
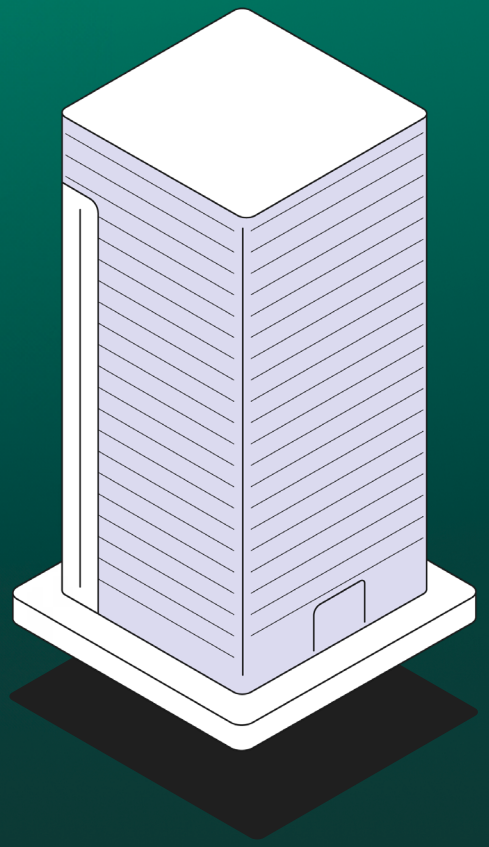
CASE STUDY

Building Secure by Design into Mission-Critical Communications



Company Background

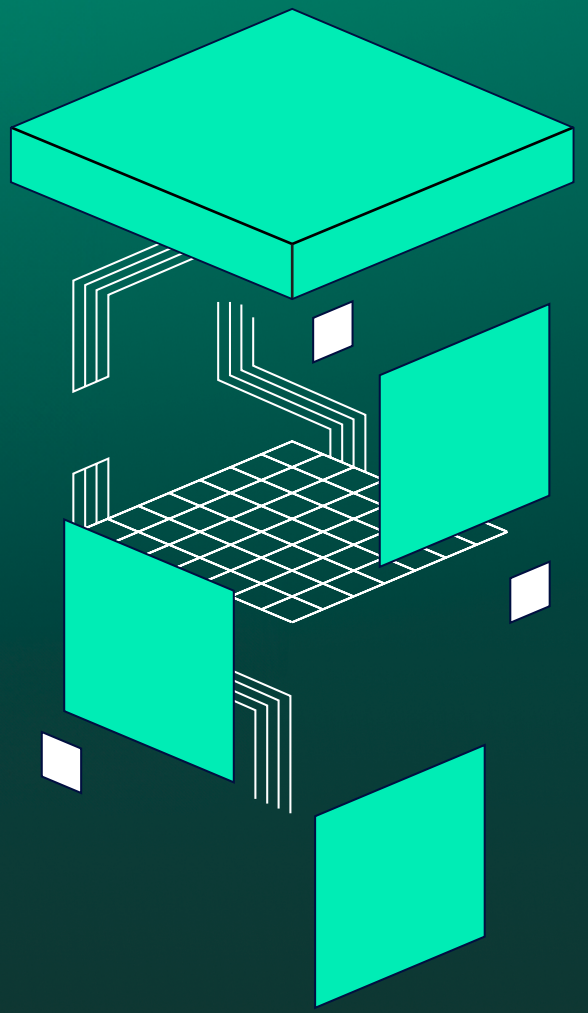
A Global Telecommunications Company provides mission-critical communications for the public sector. The organization plays a critical role in enabling their clients to operate effectively in high-pressure environments. With more than 200 upgrade projects underway, the Company needed to ensure that every design and solution met stringent security, compliance, and resilience standards. Recognizing the risks of escalating costs and long project timelines, the team wanted to embed Secure by Design (SbD) principles into their engineering lifecycle, with a focus on threat modeling as a scalable way to identify and mitigate risks early.



THE CHALLENGE

They faced several key challenges:

- No automated threat modeling process in place.
- Complex solution architectures with many components requiring robust risk visibility.
- High compliance requirements, including alignment with NIST standards to meet client regulatory needs.
- The need for automation to make threat identification scalable across multiple projects.



THE SOLUTION

Embedded security into design processes

The Global Telecommunications Company selected IriusRisk as its automated threat modeling tool to embed security into its design process. With a familiar and intuitive user interface (built on draw.io principles), engineers quickly adopted the platform. The solution enabled teams to:

- Identify and mitigate threats at scale across complex systems.
- Align directly with compliance frameworks such as NIST CSF and 800-53, making it easier to demonstrate security assurance to regulators.
- Reduce reliance on manual security processes and penetration testing by embedding security earlier in the lifecycle.

> ***I'm a big advocate for IriusRisk. We've ramped up usage across the business in the last 18 months. The ability to align threat models with compliance standards and demonstrate metrics to leadership has been a game-changer. It closes the knowledge gaps between architects and makes threat identification much more efficient.***
>
> Threat and Vulnerability Lead

THE RESULTS

A tool that's to easy to adopt and use

- Threat visibility at scale: Complex architectures mapped and assessed consistently.
- Compliance efficiency: NIST-aligned outputs quoted directly to leadership and regulators.
- Reduced penetration testing requirements, saving time and money.
- Increased collaboration: Bridging gaps between architecture and security teams.
- Positive team adoption, with engineers and architects finding the tool easy to use.

Key Reasons for Using IriusRisk

Automated threat identification across complex systems

Compliance alignment with NIST and other customer regulatory requirements

Ease of adoption thanks to a familiar UI and structured onboarding

Data sovereignty with the ability to host models in the UK

Demonstrable metrics to showcase impact to leadership and compliance teams

“

Using IriusRisk significantly accelerated our secure design program by automating key aspects of threat modeling. This automation not only saved a considerable amount of time but also ensured a consistent and thorough analysis across all projects. The tool’s integration with our existing development workflows allowed security requirements to be verified before product deployment, enabling us to more effectively prioritise and address security gaps.

Threat and Vulnerability Lead