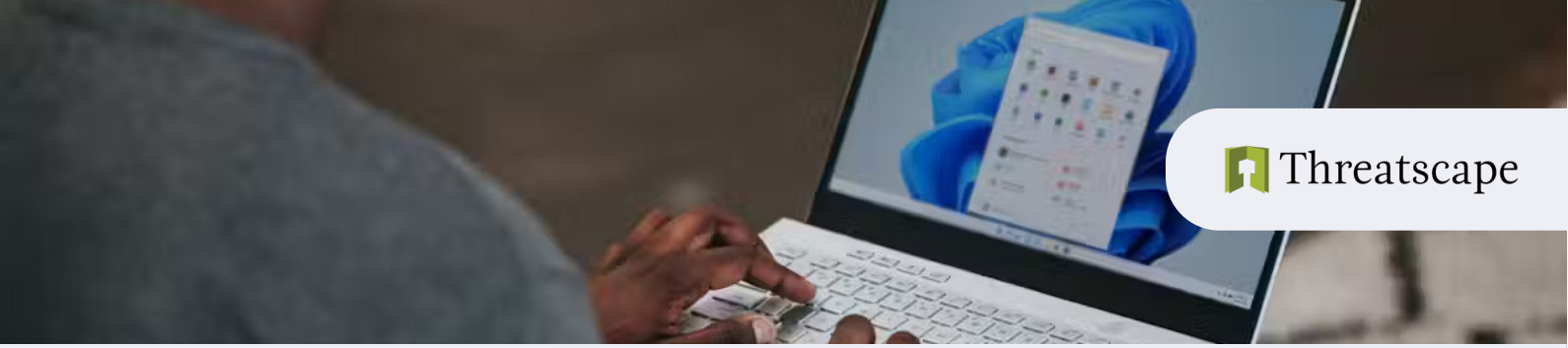

Penspen – Case Study

Organisations face mounting pressure to safeguard data, ensure compliance, and maintain operational agility, often with limited internal resources. Penspen, a prominent energy consultancy firm operating across 12 global offices, exemplifies this challenge.

With a lean IT team supporting over 1,200 employees around the world, Penspen needed to find a way to scale its cyber security capabilities, meet stringent compliance requirements (notably ISO 27001 and data residency laws), and respond quickly to evolving threats.

Penspen operates in highly regulated environments, where data sovereignty and secure access are non-negotiable. The firm's hybrid infrastructure, consisting of cloud-connected laptops and geographically diverse users adds to the complexity. For Penspen, it is essential to retain data securely, enable remote productivity, and stay responsive, all while complying with a range of legal and contractual obligations across jurisdictions.

This creates a dual challenge: maintaining and strengthening the business's security while remaining agile and operational, and modernising without compromising compliance or user experience.

Recognising the limitations of their existing setup and the fragmented nature of their security estate, Penspen turned to Threatscape to help drive a transformational shift in how they managed cyber security, from compliance through to their capabilities.

Leveraging Threatscape's Microsoft Security Expertise

Threatscape entered the picture via Microsoft-funded security workshops. These workshops provided assessments, remediation advice and POCs to demonstrate the value of capability and cost consolidation. Post licence upgrade, deployment services were funded by both Microsoft and Penspen directly.

By utilising Penspen's Fast Track vouchers, Threatscape was able to reduce Penspen's costs while still delivering an in-depth service, carried out by Threatscape's award-winning Microsoft security team. This service focused on:

Consolidation and Visibility Across Microsoft Security Tools

A key step in the engagement was helping Penspen to transition from a disparate security model (with a mixture of third-party point solutions) to a more integrated Microsoft security stack. At the time, Penspen was utilising a range of Microsoft licences, alongside various ad hoc tools. The decision to consolidate onto Microsoft 365 E5 was informed by a need for consistency, policy-based control, and the ability to confidently respond to risks in a holistic manner.

Deployment of Defender for Endpoint and Conditional Access Policies

Threatscape assisted in the secure deployment and policy configuration for Defender for Endpoint, giving Penspen control over endpoints across all locations. Conditional Access policies then added granular access control based on risk, location, and user behaviour, increasing security without hindering productivity.

Integration of Intune and Autopilot for Secure Device Management

With users dispersed globally, device provisioning was a significant administrative burden for Penspen prior to their engagement with Threatscape. The implementation of Intune and Autopilot enabled devices to be shipped directly to end users, securely configured remotely, and ready to use, freeing up time for more meaningful tasks.

Competitive Advantage

By demonstrating alignment with ISO 27001 and implementing advanced Microsoft security capabilities, Penspen enhanced its ability to meet tender requirements, particularly in regulated sectors, providing a competitive advantage when bidding for both government and private sector contracts.

Knowledge Transfer to Empower the Internal IT Team

Perhaps most critically, Threatscape ensured that Penspen's team understood what had been implemented within their environment, and why. Threatscape's approach combined technical implementation with operational empowerment. Rather than delivering a single solution, Threatscape's Microsoft team focused on transparency, clarity, and documentation, ensuring the Penspen team could manage and extend the environment independently.

> *As noted by Andrew Bond, Penspen's Director of IT: "It's absolutely essential to have that knowledge transfer… It's really lifted the capabilities of the team."*

Business Benefits and a Future-Proof Cyber Posture

Threatscape's engagement with Penspen delivered measurable improvements.

Enhanced Posture Visibility

Penspen now has consistent visibility across users, devices, and applications, a key development over their prior siloed view which will allow them to manage ongoing cyber security with confidence.

Operational Agility

The ability to configure and ship devices directly to users has reduced provisioning delays and increased productivity within the organisation.

Confidence in Compliance

With ISO 27001-aligned policies, Conditional Access enforcement, and documented processes, Penspen is now better positioned than ever to meet client and regulatory requirements and engage with potential customers.

Resource Efficiency

By automating tasks like patch management, user password resets, and spam filtering, valuable time has been freed up Penspen's internal IT team, allowing them to take a more strategic focus going forward.

A Collaborative Experience

Penspen found the experience of working with Threatscape's Microsoft security experts smooth and productive, and with no interruption to their regular responsibilities. The delivery model balanced rigour with flexibility, adapting to the pressures of a small team without compromising on outcomes.

> *"Working with Nathan from Threatscape was very easy. He was extremely knowledgeable and able to be responsive to our team, but also flexible. We [were able to] meet both the delivery of our normal day-to-day services and the delivery of the security project." -*
> *Andrew Bond*

Penspen's engagement with Threatscape reflects a broader truth in modern cyber security. Success is no longer about tools alone, but about integration, visibility, and adaptability. By consolidating platforms, automating secure workflows, and building on internal capabilities, Penspen has laid the groundwork for a resilient and scalable security strategy.

Threatscape not only delivered solutions but empowered Penspen's team to own and extend them. This partnership has turned compliance requirements into strategic advantages and transformed a lean IT operation into a confident, responsive security team.

For other organisations navigating compliance requirements, constrained resources, and hybrid IT environments, Penspen's journey with Threatscape demonstrates how a well-aligned and knowledgeable partner can delivery clarity, control, and long-term security confidence.

Why Threatscape

We are one of very few specialised security companies with a dedicated Microsoft Security Practice. Our Microsoft consultants and engineers work exclusively within the Microsoft suite, guaranteeing a reliable depth of knowledge and technical excellence in a constantly evolving feature set.

As now five-time winners of the Microsoft Security Partner of the Year Award, including the global award in 2020, Threatscape's expertise in this space is backed by Microsoft's own stringent frameworks for partner success.

Threatscape's experience and technical capability has been validated through five Microsoft Advanced Specialisations, demonstrating the breadth of our Microsoft skill. Advanced Specialisations are subject to an external audit of subject-related processes, methods, documentation, and reporting, considering both the knowledge and professionalism of in-house staff, along with the organisation's overall expertise in relevant areas. In order to be awarded an Advanced Specialisation, all facets of the audit must be met, without exception.

We are also positioned to deliver Microsoft funding through the Partner Programme, including both FastTrack and the Partner Cybersecurity Investment Program, or CSI.

Microsoft's FastTrack programme assists customers in planning, onboarding, managing, and driving value and satisfaction from their Microsoft deployment. FastTrack partners are trusted by Microsoft, on the back of their engineering expertise and proven track record of delivering guidance and service enablement.

Similarly, CSI is an invitation-only programme created by Microsoft to offer funding to eligible organisations to enable them to expand their deployment through preliminary engagements with new services.

Where appropriate, Threatscape may deliver a Microsoft Sentinel Engagement, a Cybersecurity Assessment, a Threat Protection or Data Security Engagement, or a tailored Overwatch Initial Assessment, utilising our leading Microsoft Security technologies to create a real-time baseline based on 330+ security controls to enable prioritised, evidence-based security optimisation.

Contact Us