
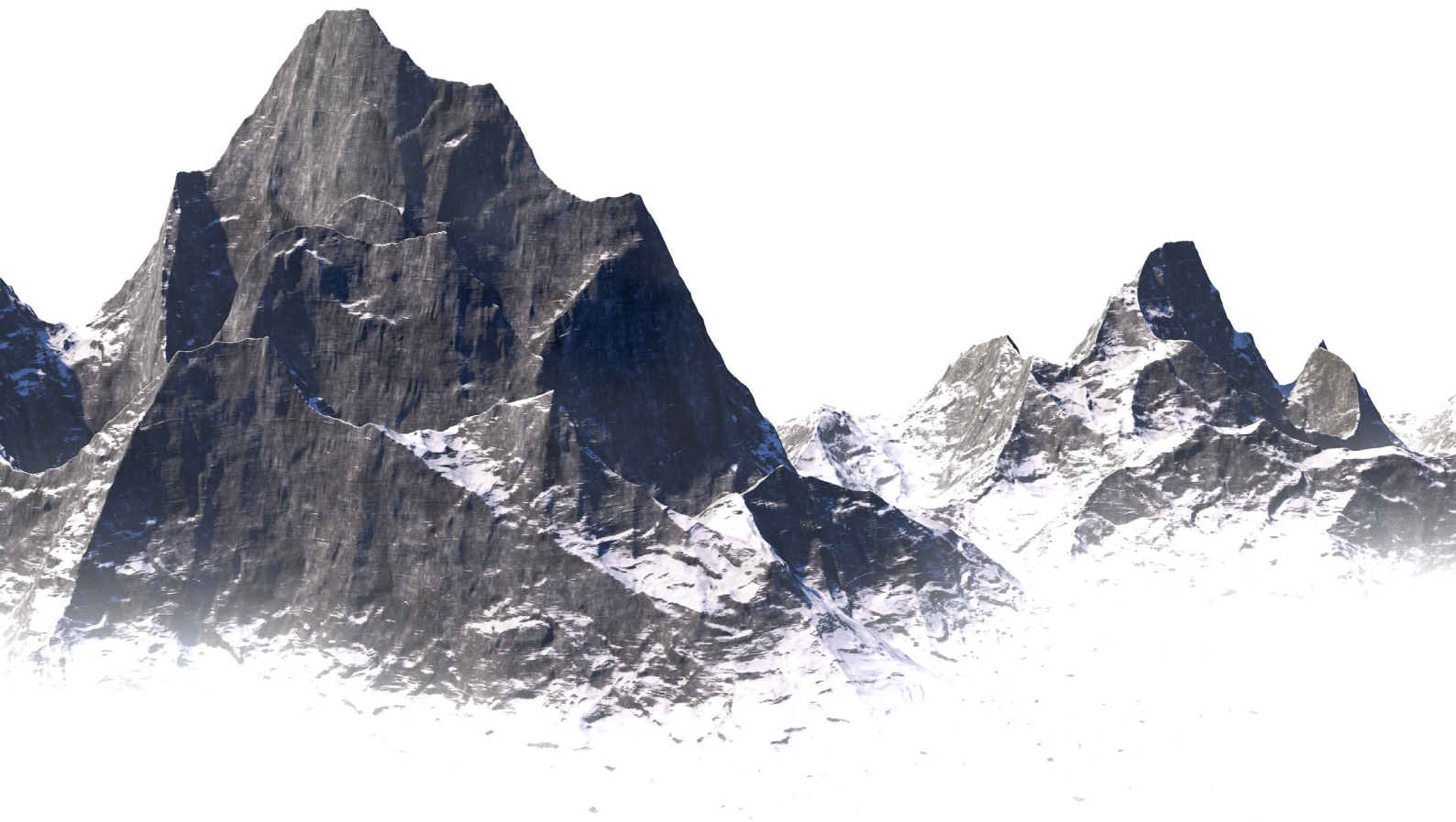


Climbing Towards Cyber Resiliency

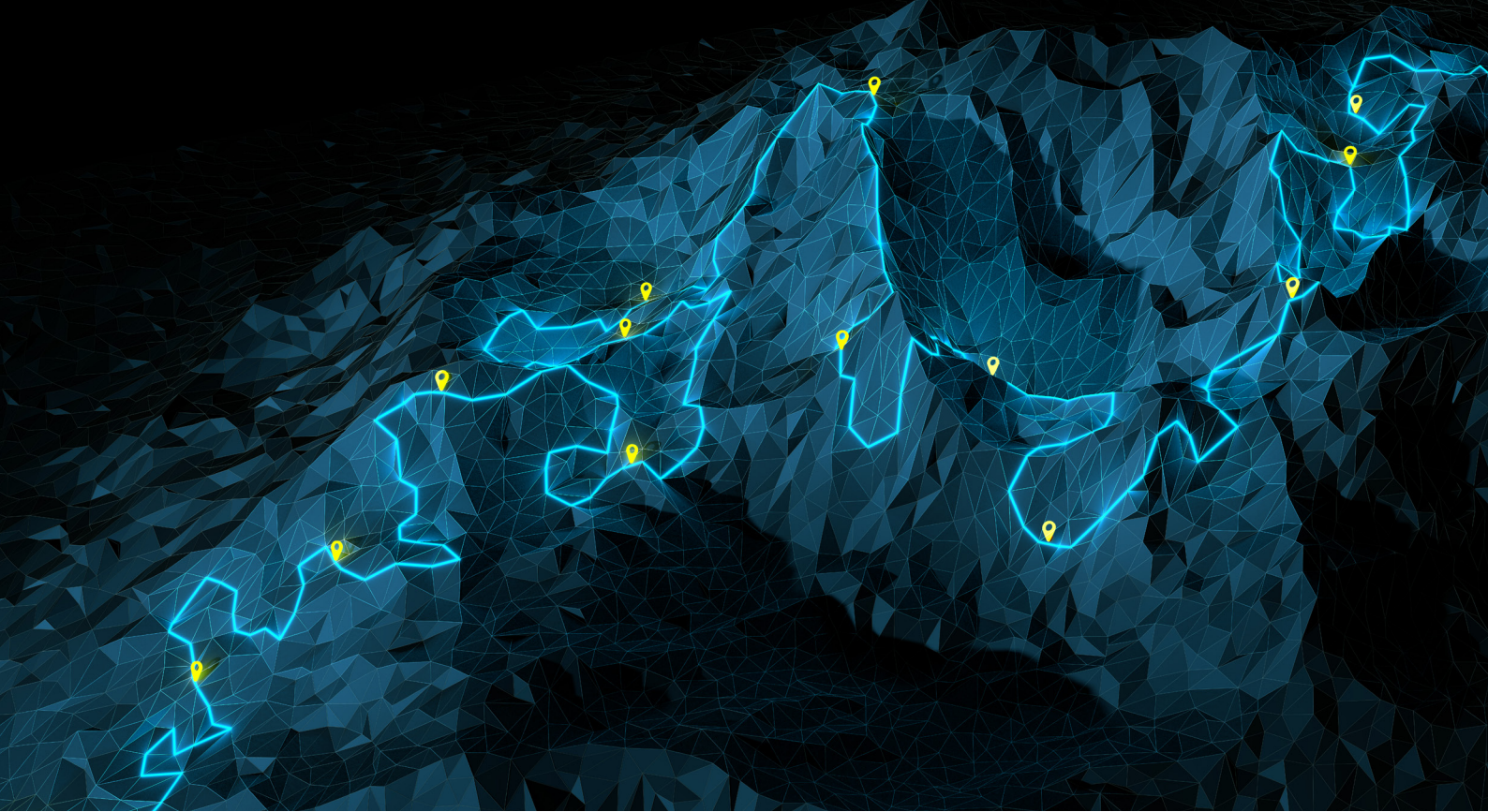


When defining and executing your cyber security strategy, it can feel like you have a mountain to climb. One on which a perfect storm of threat actors gaining ground, and insurers reframing the risks they're willing to cover, awaits you.

This is exactly the type of complex challenge that we, at WhiteSpider, thrive on. Founded by two mountaineering technologists; Phil Lees and Dave Chadwick, they named the organisation after an ice field on the north face of the Eiger mountain – one of the world's most technically challenging climbs. It's a name that we believe encapsulates our appetite and skill for creating successful outcomes where others fear to tread.



In this guide, we'll describe what you can expect to encounter on your path towards cyber resiliency, with WhiteSpider and VMware as your trusted partners.



Real-life examples from the cyber security landscape

As the largest cloud market in Europe¹, the NCSC is urging UK organisations across all sectors to prepare for an extended period of heightened cyber threat². With risks ranging from surgery delays due to patient records being held to ransom³, and retailers closing stores after breaches halt deliveries⁴, the ability to handle network compromises has become a strategic business priority.

Planning your approach

As risk factors and their impact are better understood, organisations need to adapt their investment priorities to consider:

- **Defence:** Prioritising security in IT investments
- **Identification:** Identifying and monitoring cyber threats
- **Business protection:** Investing in cyber insurance

We've already seen the insurance issue in action a number of times. As an example, one well-known fashion retailer approached us after being told they would be ineligible for cyber insurance unless they could demonstrate how they provide end-to-end network segmentation. We helped them solve this challenge.

¹ <https://www.trade.gov/market-intelligence/united-kingdom-cloud-services-market>

² <https://www.ncsc.gov.uk/news/ncsc-urges-organisations-to-prepare-for-the-long-haul-on-russia-ukraine>

³ <https://www.irishtimes.com/news/ireland/irish-news/hse-hack-will-cut-lives-short-due-to-delays-in-diagnosis-doctors-say-1.4597312>

⁴ <https://portswigger.net/daily-swig/uk-retailer-the-works-blames-store-closures-on-pos-problems-following-cyber-attack>

Equipping yourself for any conditions

We've chosen to invest in VMware NSX-T as it is uniquely positioned to provide best-in-class cyber security across any platform and for multiple use cases that include, but are not limited to:

- **Virtual segmentation:**

In the case of the fashion retailer, NSX-T provides a consistent end-to-end experience from the datacentre perimeter all the way to where applications reside.

- **Protecting unpatchable applications:**

A major retail bank uses NSX-T to protect an out-of-support operating system that cannot be retired; significantly reducing the attack surface.

- **Increasing developer productivity:**

One finance firm used NSX-T to create a self-serve IaaS environment where developers can use VRA and Terraform without creating challenges for the networking and security teams.

Preventing a fall

Any experienced climber will tell you that one of the most important safety factors is anticipating hazards and planning how best to respond.

In the context of cyber security, some threat actors are so sophisticated they can operate for months undetected – NSX-T helps organisations supplement efforts to prevent breaches with the ability to detect and contain malicious or unusual activity.





Improving your security posture

In a traditional network environment, anyone can connect to anything. This offers the potential for malware to proliferate undetected from east to west, creating footholds within your organisation that guide the threat actor to their intended goal.

Modern networking solutions such as NSX-T segment users and data across the estate which is combined with built in intrusion prevention (IPS) alongside intrusion detection (IDS). This means that not only is the network being continually scanned for anomalies in behaviour and identifying when action needs to be taken, but the damage of bad action is vastly limited.

A team effort

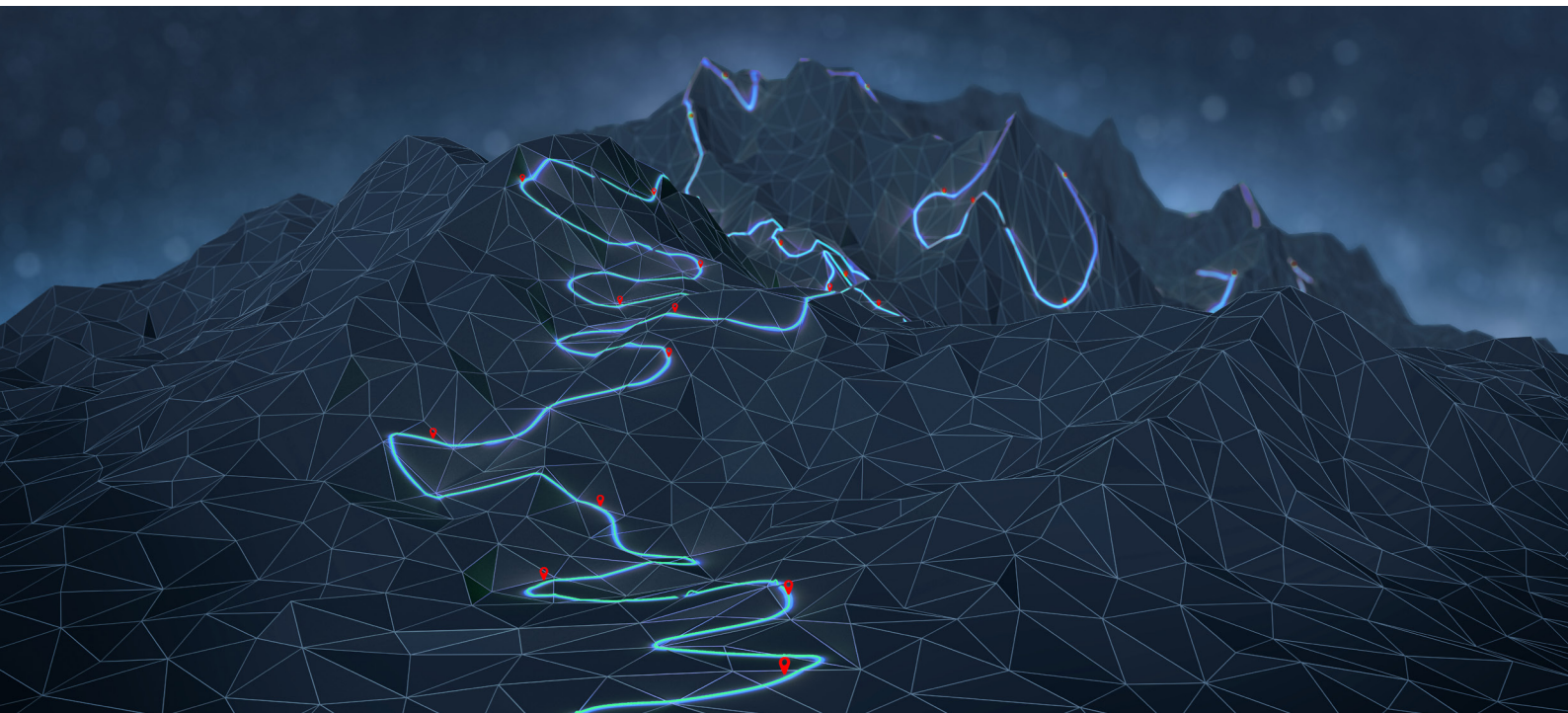
Having the right approach, attitude and trusted team around you means you can avoid expending unnecessary energy, or being exposed to unacceptable risk.

Our team helps customers with high network complexity to rapidly address technically challenging scenarios by creating software-defined environments where you write the code once, then deploy across the whole estate. And, thanks to our close partnership with VMware, we can assemble an expert team that can help you navigate any terrain.

Scaling new heights

Our customers are ambitious. And we're proud to help them achieve their strategic goals. Here's just a sample of the projects we've been engaged to deliver:

- When your organisation has to meet a strict SLA for hundreds of thousands of individuals, you need a networking security partner that can deliver. By applying our skill in AI/ML and DevOps to find and remediate issues, we are able to commit to – and meet – a 60-minute SLA which allows our utility-aggregator customer to avoid penalties by meeting time-sensitive commitments.
- With multiple mergers and acquisitions creating infrastructure complexity, Berry Global engaged us to help them achieve greater network resiliency and scalability. We helped Berry achieve an ambition to enhance services to staff and allow the IT team to focus on transformation rather than operation.
- When a hurricane threatened to flood their datacentres, we helped one client relocate their entire estate without downtime. This highly complex project not only meant the client achieved business resilience and maintained continuity – they saved significant real estate costs post-relocation.



Your route to the summit

From identifying your current cyber resiliency posture, right through to designing, implementing and maintaining a robust solution that supports your business priorities, we have a range of engagements designed to make sure you set off on the right foot.

Using our fully equipped facility and expert team, we're on hand to help with strategy workshops and health checks, plus Proof of Concept and Proof of Value sessions that showcase a wide range of hyper converged infrastructure, cloud interconnects and application centric infrastructure solutions.



About WhiteSpider

WhiteSpider is an advanced technology services company, specialising in the provision of consultancy, strategic advice, and practical support in enterprise service architectures. We help organisations across the world to standardise their IT and communications infrastructures as they transition to digital, software-defined architectures. With a strong history in data centre, cloud and networking technologies, WhiteSpider's team of experts possess unrivalled experience in designing, delivering and managing software-defined architectures that simplify and automate your IT estate, and truly deliver on your business objectives.

About VMware NSX-T

VMware NSX-T® is the network virtualization and security platform that enables VMware's cloud networking solution with a software-defined approach to networking that extends across data centres, clouds and application frameworks. With NSX, networking and security are brought closer to the application wherever it's running, from virtual machines (VMs) to containers to physical servers.

Ready to get started?

Choose the route towards cyber resiliency
that's right for you – contact us at

info@whitespider.com
or on **+44 020 3773 2380**