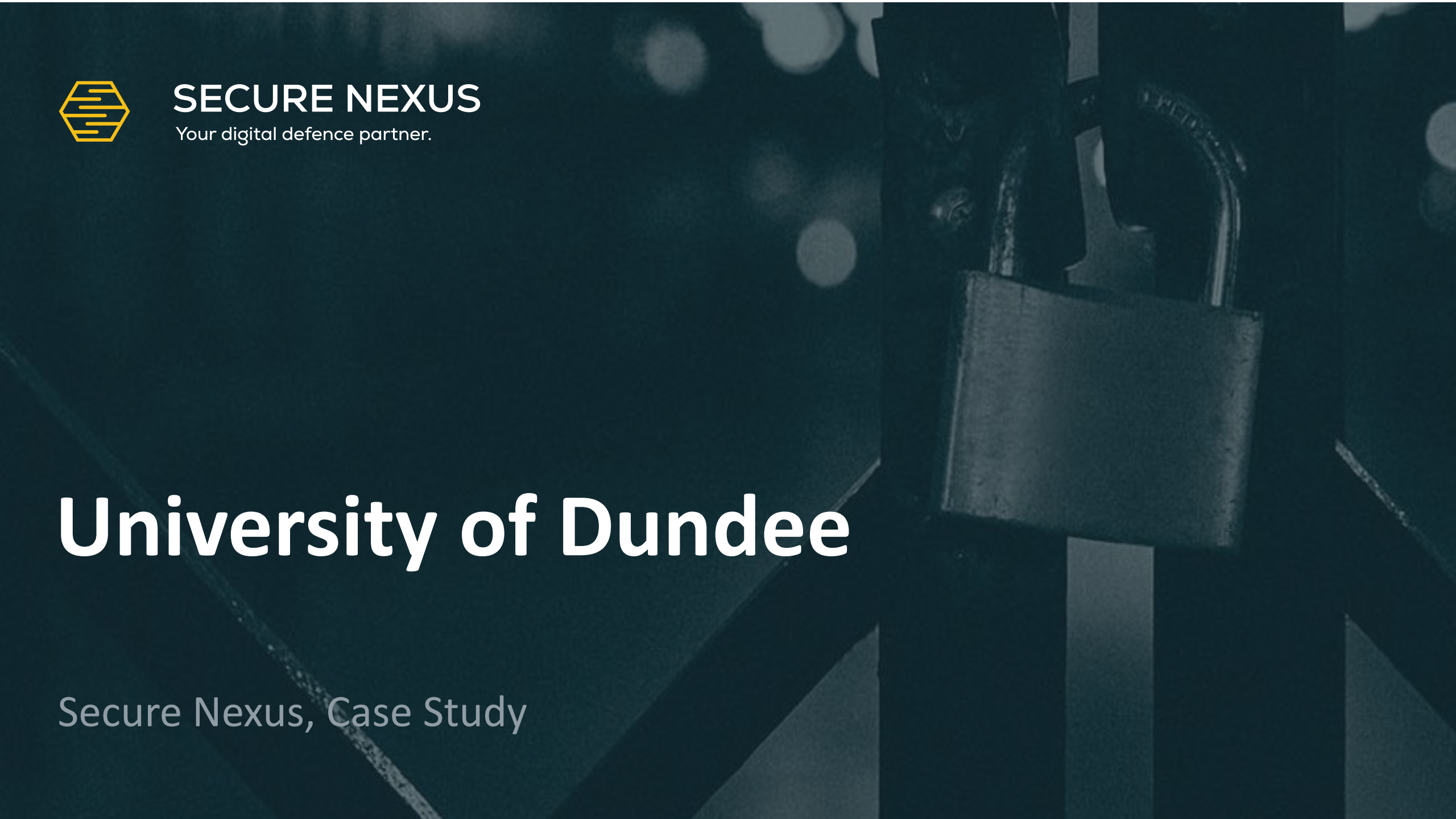


SECURE NEXUS
Your digital defence partner.

University of Dundee

Secure Nexus, Case Study

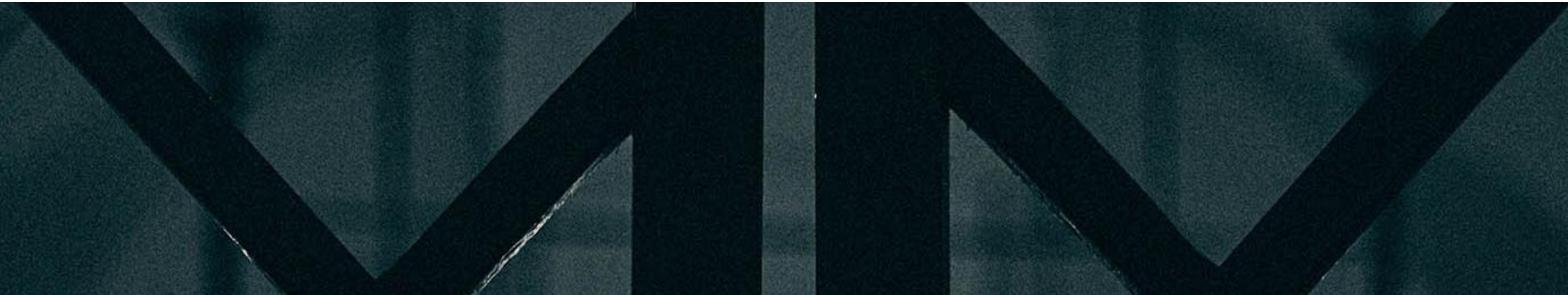
Client Overview

University of Dundee is a well-established UK public-sector university with a strong reputation for teaching, research, and innovation. Operating within a highly regulated higher-education environment, the university must balance open academic collaboration with robust security, resilience, and compliance requirements.

As a large and complex organisation, the University of Dundee supports a diverse range of users and services, including academic staff, professional services, researchers, and students. Its IT estate spans multiple campuses and encompasses a broad mix of systems such as teaching platforms, research infrastructure, administrative services, and externally facing applications.

From a technical perspective, the environment is inherently complex. It consists of a large, segmented network architecture with numerous VLANs, thousands of IP-addressed assets, and a mixture of legacy and modern systems. These assets underpin critical services, including research workloads, student systems, and operational platforms that must remain highly available and secure.

This scale and diversity create a challenging security landscape, where maintaining visibility, understanding risk, and validating controls are essential. The engagement with Secure Nexus was positioned to provide assurance across this environment, while respecting the operational sensitivity and mission-critical nature of a live university network



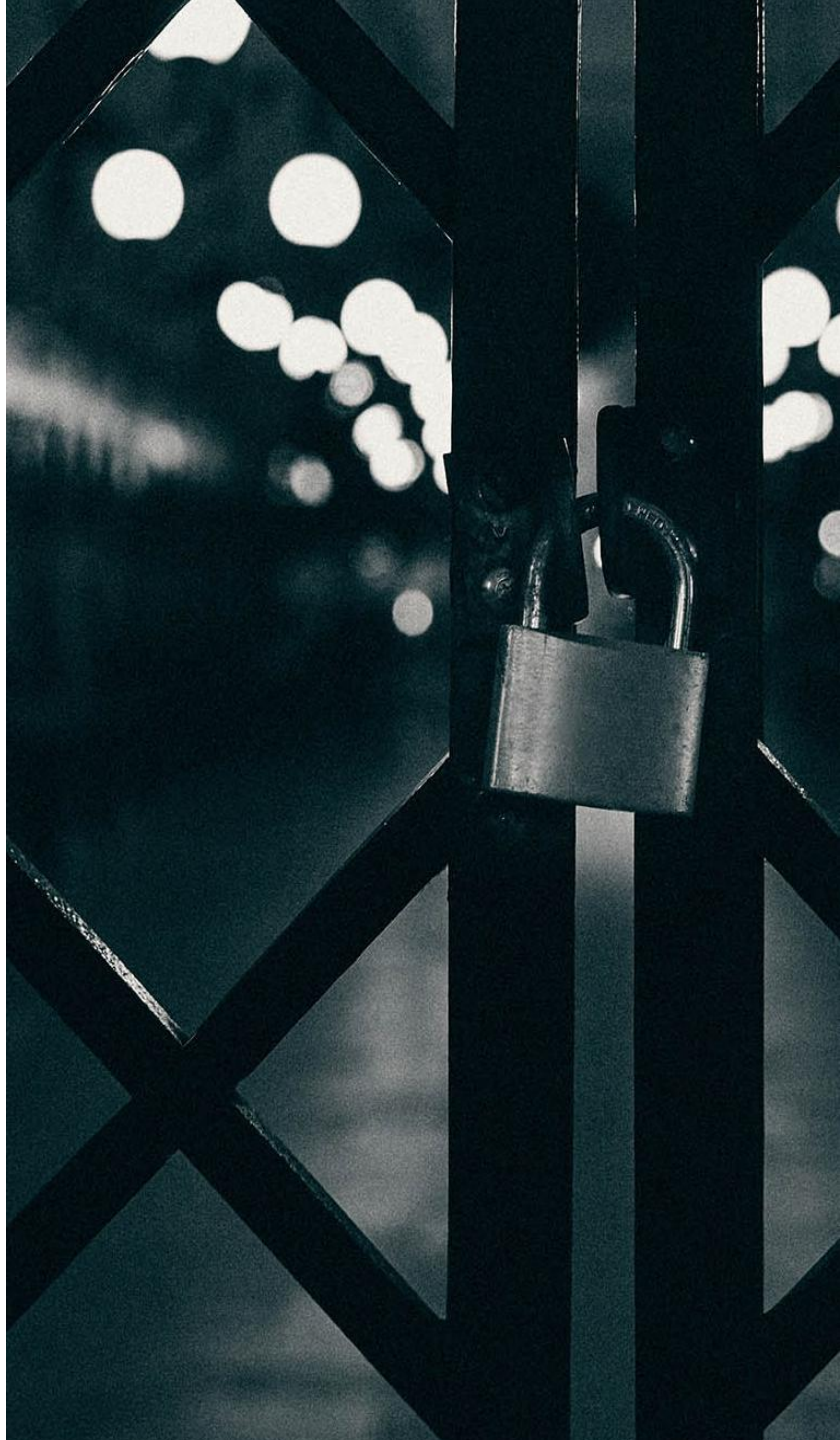
The Challenge

University of Dundee operates a large and highly diverse IT environment supporting teaching, research, and administrative services. This estate spans numerous network segments and VLANs, with thousands of IP-addressed assets and a mix of modern platforms and legacy systems, each carrying different levels of risk and sensitivity.

A key challenge was maintaining continuous visibility of vulnerabilities across this evolving environment. Point-in-time assessments did not provide sufficient insight for an organisation where systems and services change frequently, particularly within research and academic contexts.

In parallel, the university needed to validate its security posture against real-world attack techniques, rather than relying solely on theoretical risk or compliance-based checks. There was also ongoing pressure to demonstrate assurance and prioritise risk effectively, supporting governance, audit requirements, and informed remediation decisions.

All of this had to be achieved without disrupting live operations. Any security activity needed to respect the realities of a production university network, ensuring that teaching, research, and student services remained unaffected while still delivering meaningful assurance.



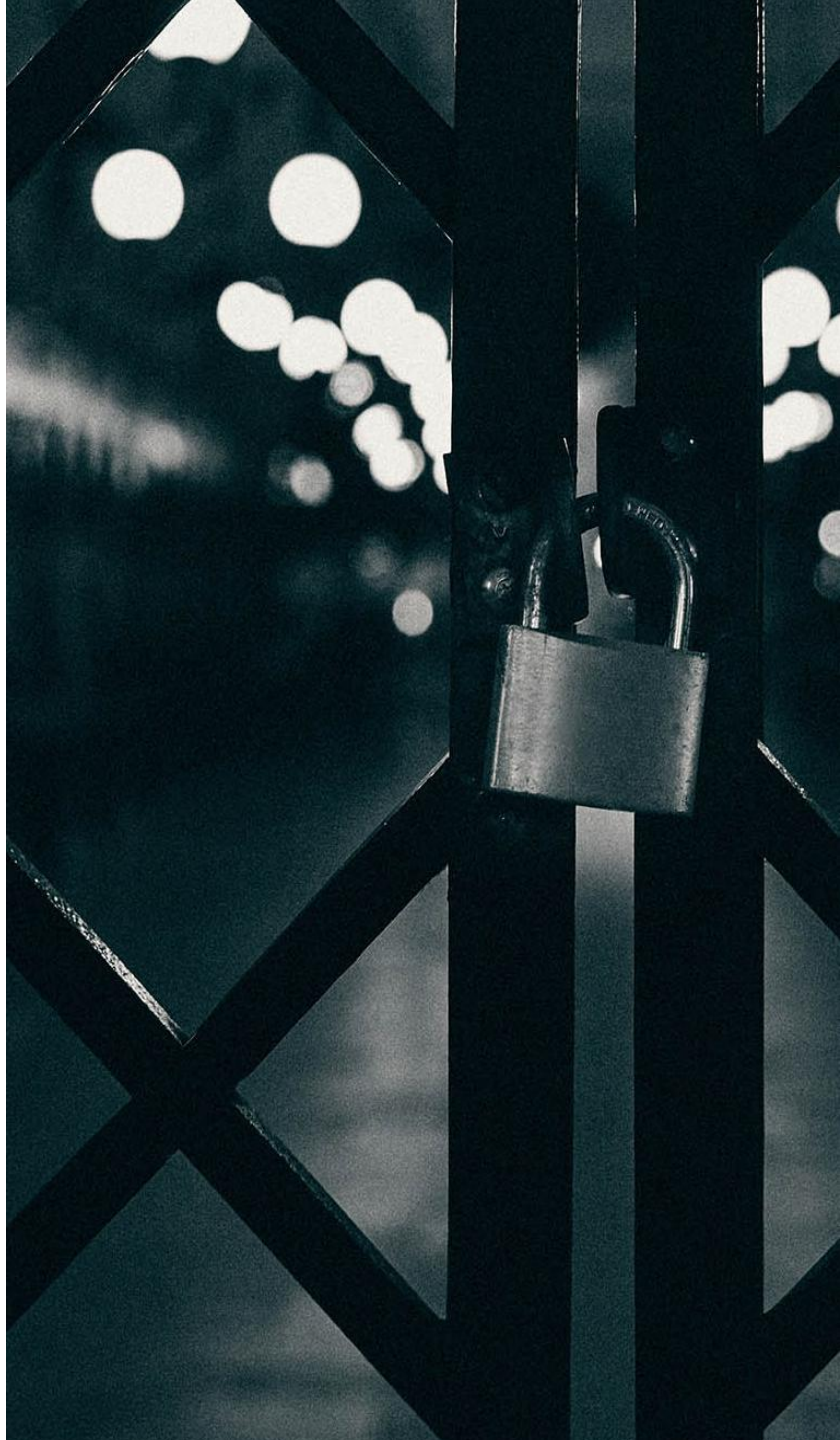
Objectives

For University of Dundee, success was defined by the ability to achieve clear, defensible security assurance across a complex and evolving environment, without introducing operational risk.

The primary objectives were to establish continuous vulnerability management across the university network, providing up-to-date visibility of weaknesses rather than relying on periodic, point-in-time assessments. Alongside this, the university required accurate asset discovery and configuration insight, ensuring that security decisions were based on a clear understanding of what systems existed and how they were connected.

A further objective was to validate real-world exploitability through controlled penetration testing, moving beyond theoretical risk to understand how vulnerabilities could be abused in practice. This allowed the university to prioritise remediation based on genuine risk and impact, rather than treating all findings equally or relying solely on CVSS scores.

The engagement needed to deliver clear, actionable reporting that could be consumed by both technical teams and senior stakeholders, supporting operational remediation, governance oversight, and wider assurance requirements.



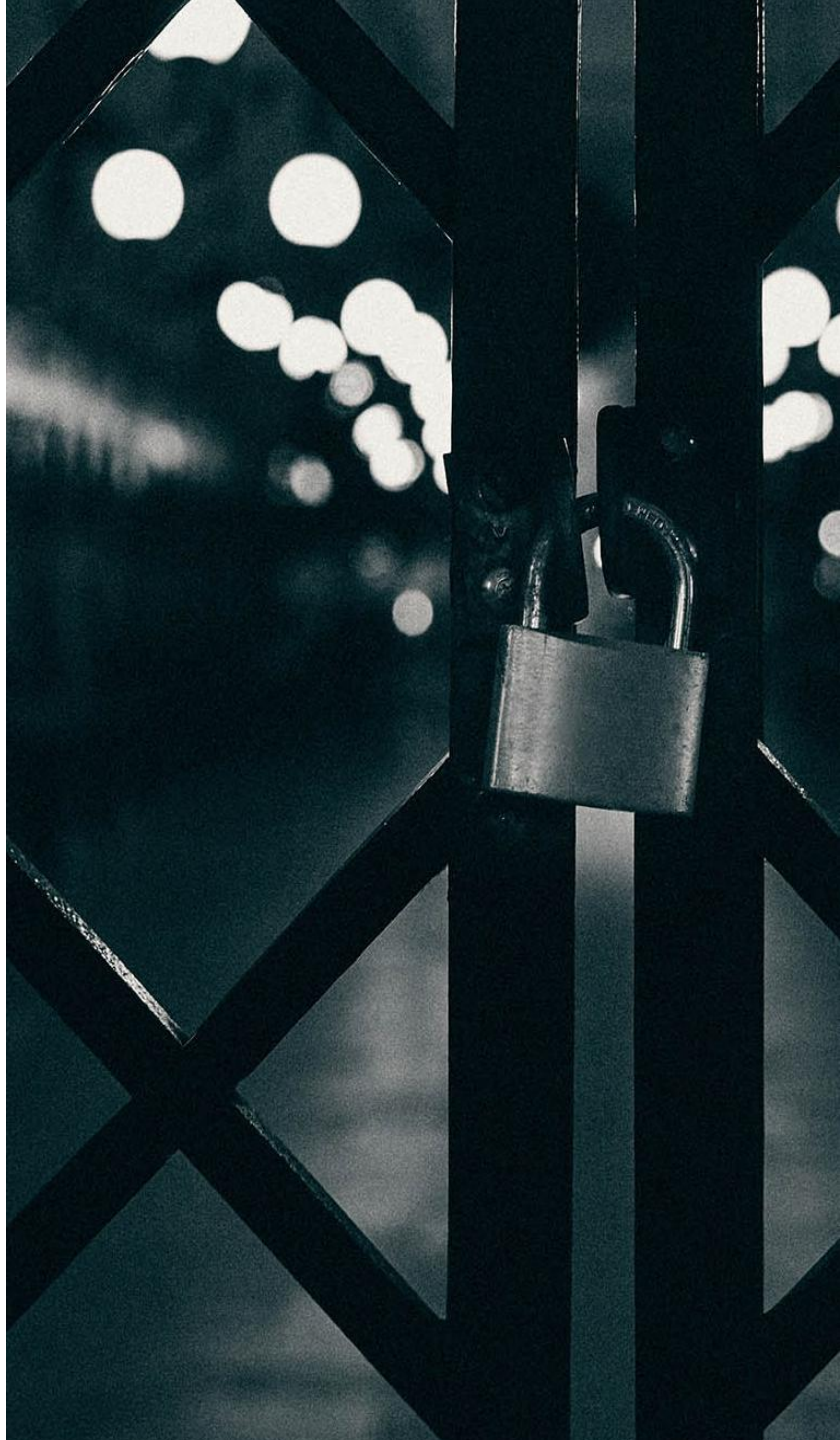
Secure Nexus Approach

Secure Nexus adopted a delivery-led, assurance-focused approach, working in close collaboration with the University of Dundee Cyber Security team throughout the engagement. Early engagement ensured a clear understanding of the university's operational constraints, risk appetite, and governance requirements, allowing the solution to be shaped around the realities of a live higher-education environment.

The approach was structured around a phased design and deployment model, enabling capability to be introduced incrementally and safely. This reduced operational risk, allowed validation at each stage, and ensured that security activities remained aligned with teaching, research, and administrative priorities.

All components were implemented in line with Secure Nexus build standards, applying least-privilege access, strong authentication, and controlled administrative boundaries. This ensured that security tooling itself did not introduce unnecessary exposure and remained auditable and well-governed.

Throughout the engagement, the emphasis remained on assurance rather than disruption. Security assessment activities were designed to operate predictably and safely within the production environment, delivering meaningful insight into risk while preserving the stability and availability of critical university services.



Solution Delivered

To address the university's assurance requirements, Secure Nexus delivered a layered security assessment capability designed to provide continuous insight, validation, and prioritisation across the environment. Rather than relying on a single assessment method, the solution combined complementary capabilities to reflect how real risk manifests in complex, live networks.

Continuous Vulnerability Scanning
Ongoing vulnerability scanning was implemented to provide continuous identification and prioritisation of weaknesses across the university network. This ensured that newly introduced vulnerabilities, configuration drift, and changes within the environment were identified promptly, allowing risks to be tracked and managed over time rather than discovered retrospectively.

Network Discovery & Assessment
Comprehensive network discovery and assessment provided accurate visibility of assets, network structure, and configuration state. This enabled a clear understanding of what systems existed, how they were connected, and where security gaps or misconfigurations could amplify risk. This context was critical in ensuring vulnerability findings were interpreted correctly within the wider environment.

Automated Penetration Testing
Automated penetration testing was used to simulate real-world attack techniques in a controlled manner. This validated whether identified vulnerabilities could be practically exploited and how they could be chained together, moving the assessment beyond theoretical exposure to demonstrable risk.

The combination of these capabilities was key. Vulnerability data alone can lack context, asset discovery without exploitation does not show impact, and penetration testing without continuous insight risks becoming outdated. Together, they provided the University of Dundee with a defensible, risk-led view of its security posture supporting informed remediation decisions, ongoing assurance, and confidence that controls were effective against realistic threat scenarios.

Architecture & Deployment Highlights

The solution was implemented using a secure and carefully controlled architecture, designed to operate safely within the University of Dundee's live production environment. Scanning and testing components were deployed within isolated segments, ensuring that assessment activity was clearly bounded and did not introduce unnecessary exposure to other parts of the network.

Integration was carried out in alignment with existing university network controls, working within established security, firewall, and routing policies rather than attempting to bypass or weaken them. This ensured consistency with internal governance and avoided the introduction of parallel or unmanaged access paths.

All scanning and testing activity was limited to predefined IP ranges and VLANs, agreed in advance with the University of Dundee Cyber Security teams. This allowed precise control over scope, clear accountability, and confidence that only approved areas of the environment were assessed.

Where appropriate, a combination of agent-based and agentless techniques was used. Agentless methods provided broad visibility and low-impact assessment across large network segments, while agents were selectively deployed to enable deeper insight where required, without unnecessary footprint.

Throughout deployment, the overriding principle was minimal operational impact. Activities were introduced in a predictable, phased manner, with validation at each stage to ensure stability. This approach allowed Secure Nexus to deliver meaningful security assurance while preserving the availability and performance of critical teaching, research, and student services.

Outcomes & Benefits

+ Improved visibility of assets and vulnerabilities across the university network, providing a clearer and more current understanding of security exposure.
+ Risk-based prioritisation of remediation activities, enabling technical teams to focus on issues with the greatest potential impact.
+ Validation of existing security controls through real-world testing, increasing confidence in their effectiveness and highlighting areas for improvement.
+ Clear, defensible evidence to support audits, assurance activities, and internal governance requirements.
+ Strengthened overall security posture without disrupting teaching, research, or student services.

“Secure Nexus have proved to be a valued and trusted partner in establishing and developing the University of Dundee's approach to IT asset visibility and vulnerability management across our organisation. Throughout the project, Secure Nexus offered a mix of both Higher Education experience and industry best-practice whilst designing and implementing various tools to deliver to our outcomes.

Forever mindful of our diverse and complex IT environment, Secure Nexus showed flexibility throughout and adapted to challenges as they emerged, working collaboratively to identify and implement solutions efficiently.

Following successful delivery of our project, Secure Nexus continue to work closely with my team, regularly discussing and reviewing our procedures, and highlighting opportunities for change utilising a continual service improvement approach.”

Bob McGregor, Head of Cyber Security, Digital & Technology Services

Secure Nexus, your digital defence partner

Secure Nexus works as a trusted security partner rather than a tool provider. By combining deep technical expertise with a strong understanding of higher-education and public-sector operating environments, Secure Nexus delivers practical, risk-led security assurance that stands up to scrutiny.

The focus remains on improving security outcomes, supporting governance, and enabling organisations to operate with confidence without compromising the availability or integrity of critical services.

Higher-Education Experience

Proven experience delivering security services within higher-education and public-sector environments, where scale, governance, and operational sensitivity are critical.

Risk-Led Design

A security-first design philosophy, ensuring that solutions are built around risk reduction, control, and assurance rather than tool deployment alone.

Operational Pragmatism

A strong balance between technical depth and operational pragmatism, enabling meaningful security outcomes without disrupting live services.

Defensible Assurance

A clear focus on delivering assurance, not just tools, providing defensible insight that supports risk management, governance, and informed decision-making.

SECURE NEXUS

Your digital defence partner.

enquires@securenexus.co.uk
01786 236 632

Trusted. Certified. Recognised.