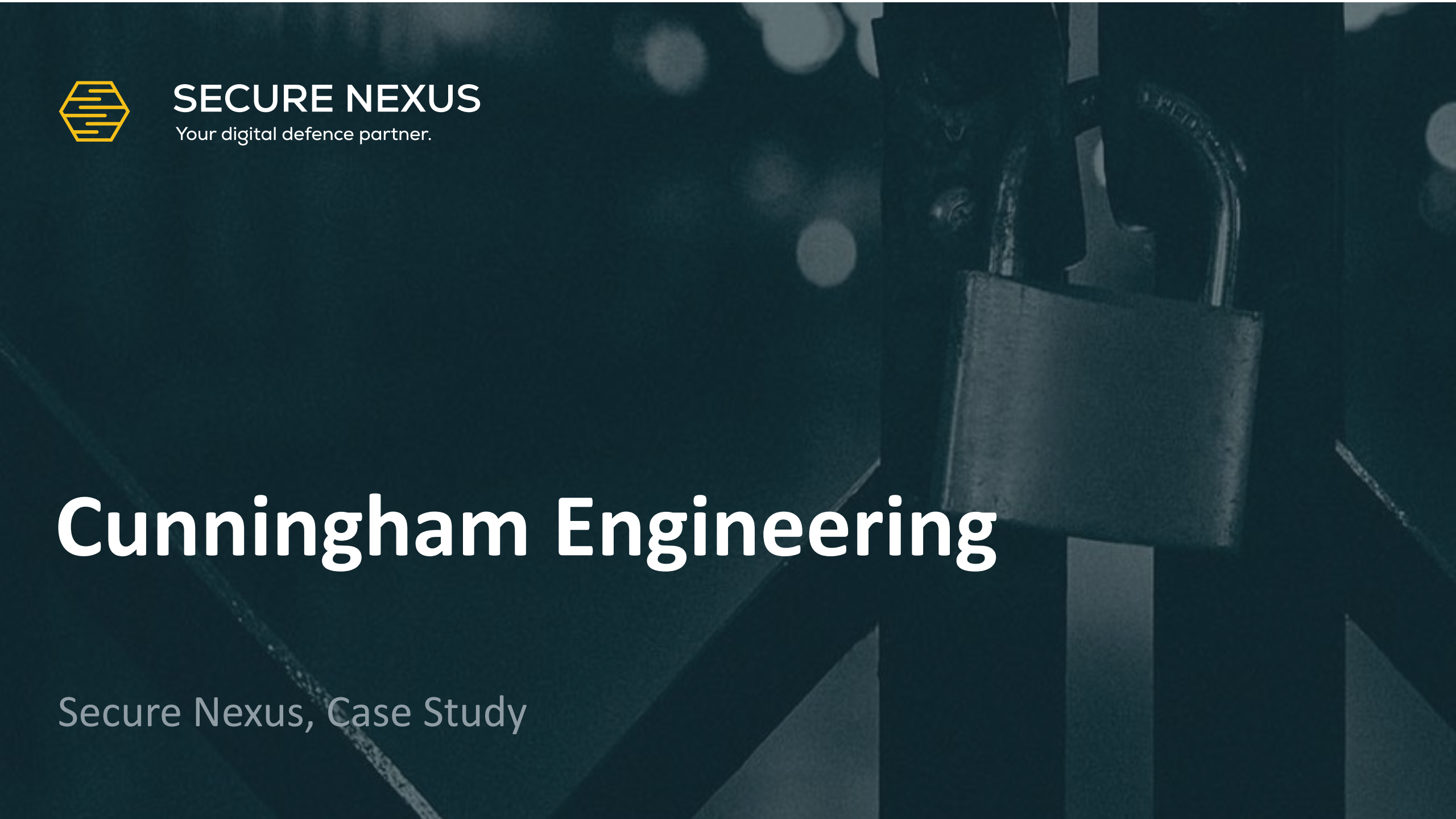


SECURE NEXUS
Your digital defence partner.

Cunningham Engineering

Secure Nexus, Case Study

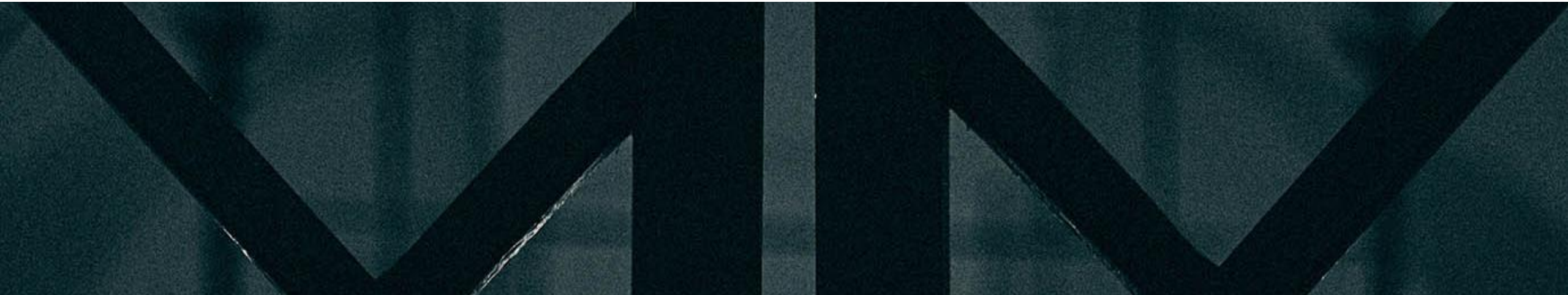
Client Overview

Cunningham Engineering is a UK-based SME operating within the engineering and construction sector, delivering specialist services in a fast-paced, compliance-driven environment.

The business operates with a small internal team and a high reliance on digital collaboration tools, including email, shared files, and cloud-based productivity services to support day-to-day operations, project coordination, and external communication with partners and suppliers.

As with many organisations of its size, Cunningham Engineering did not have a dedicated in-house IT or security governance function. Technology and security controls had evolved organically over time, creating increasing operational dependency without a corresponding level of visibility, assurance, or resilience.

At the same time, the organisation was facing growing exposure to cyber risk, driven by phishing threats, email impersonation, and data protection obligations, alongside rising expectations around GDPR compliance, auditability, and business continuity. This created a clear need for a more structured, security-first approach that could strengthen protection without adding internal complexity or management overhead.



The Challenge

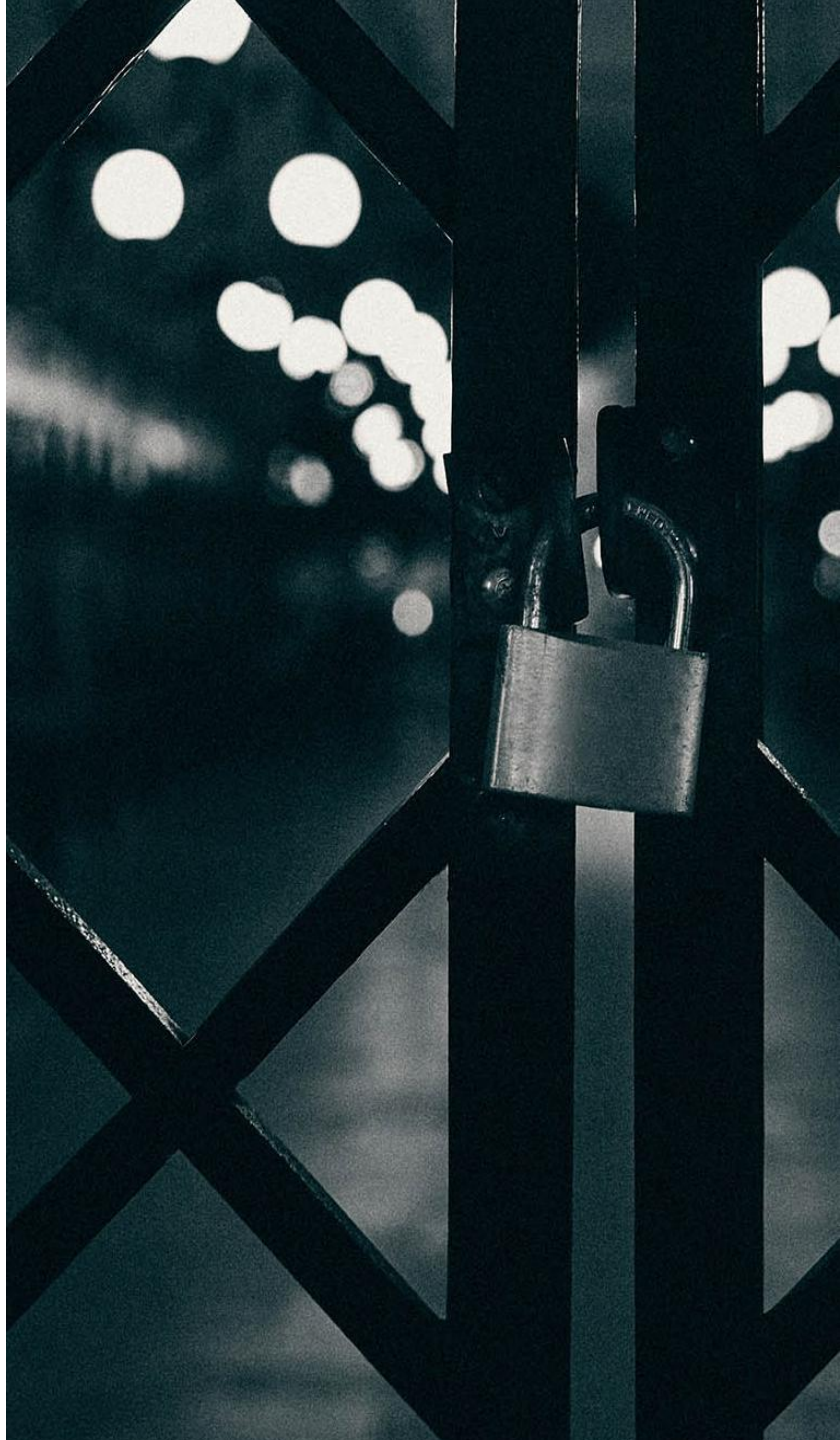
As Cunningham Engineering continued to grow, its IT environment had developed in a largely organic manner. Email, file storage, and user access were spread across a fragmented setup that lacked central governance, making it difficult to apply consistent security controls or enforce best-practice configuration.

The organisation had limited visibility into its overall security posture. There was no consolidated view of user activity, access risk, or endpoint health, meaning potential threats such as compromised accounts, unauthorised access, or unsafe user behaviour could go undetected until they caused operational impact.

Business-critical data was not protected by a formally defined backup or recovery strategy. There was no assured retention policy or tested recovery process in place, creating exposure to accidental deletion, ransomware, or data loss scenarios that could disrupt operations and delay project delivery.

Access control was inconsistent across services, with reliance on legacy authentication methods and limited use of role-based access. This increased the risk of account compromise, over-privileged access, and poor auditability, particularly as users collaborated with external parties.

These risks were validated during an initial cybersecurity assessment conducted by Secure Nexus, which identified multiple areas of exposure across identity, email security, and data protection. The findings confirmed the need for a structured, security-first redesign that could reduce risk, improve visibility, and provide ongoing assurance without adding complexity to the business.



Objectives

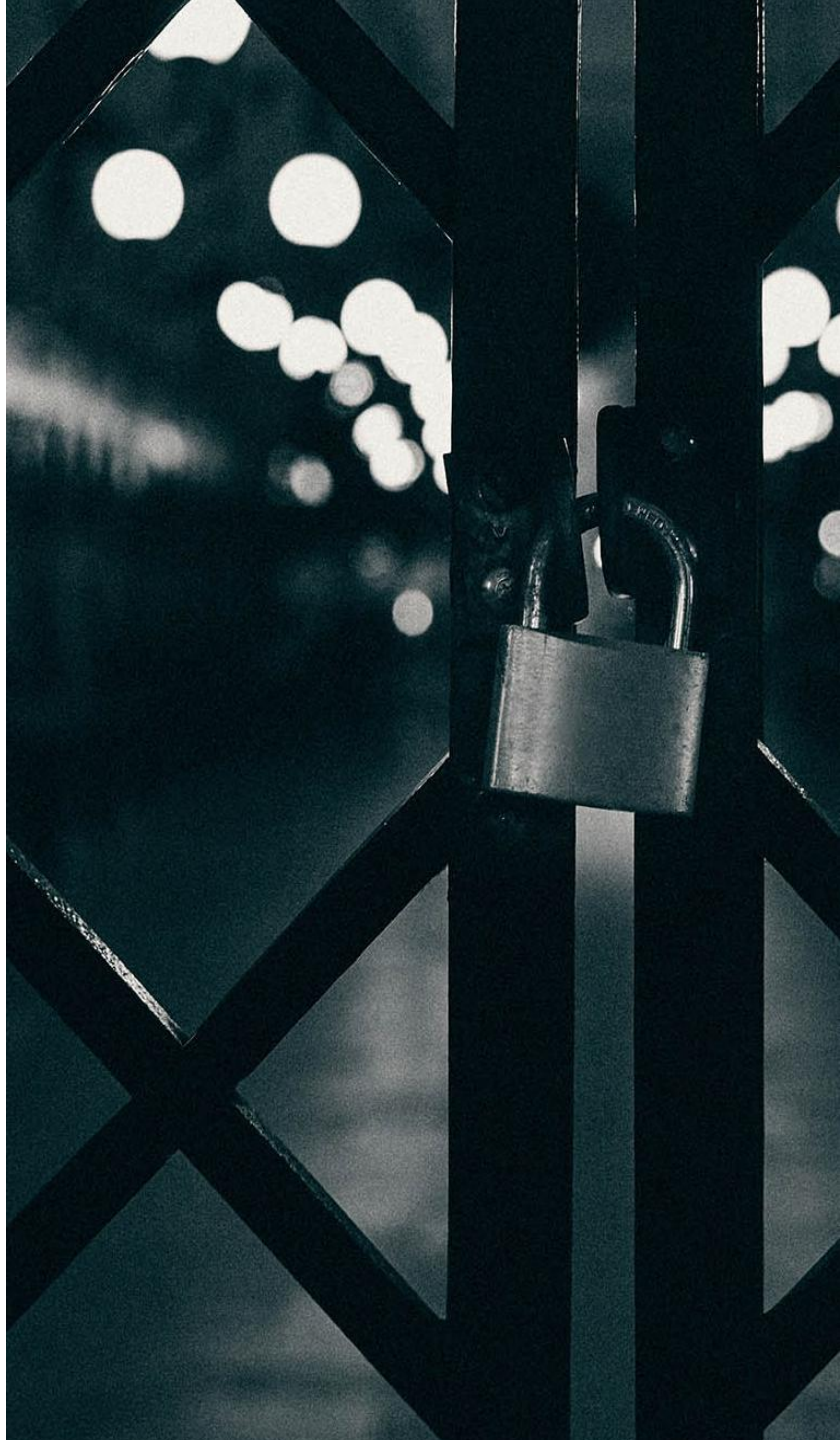
For Cunningham Engineering, success was defined not by the deployment of individual tools, but by achieving a measurable improvement in security, resilience, and operational confidence. The primary objective was to establish a secure, modern Microsoft 365 environment that could act as a reliable foundation for collaboration, email, and document management, while being configured in line with security best practice from day one.

Improving identity and access control was critical. The organisation needed stronger authentication, clearer role-based access, and full auditability of user activity to reduce the risk of account compromise and support future compliance or assurance requirements.

Protecting business-critical data was equally important. This required an assured backup and recovery capability, with defined retention policies and the ability to recover data quickly in the event of accidental deletion, ransomware, or service disruption.

Reducing exposure to phishing and email-borne threats was a key priority, particularly given the organisation’s reliance on email for external communication and commercial activity. The solution needed to harden email security while improving user resilience.

Cunningham Engineering required ongoing security oversight, monitoring, and assurance without the need to build internal security capability or add day-to-day management burden to the business.



Secure Nexus Approach

Secure Nexus adopted a security-first, outcomes-led approach, designed to reduce real-world risk while fitting naturally into the way Cunningham Engineering operates.

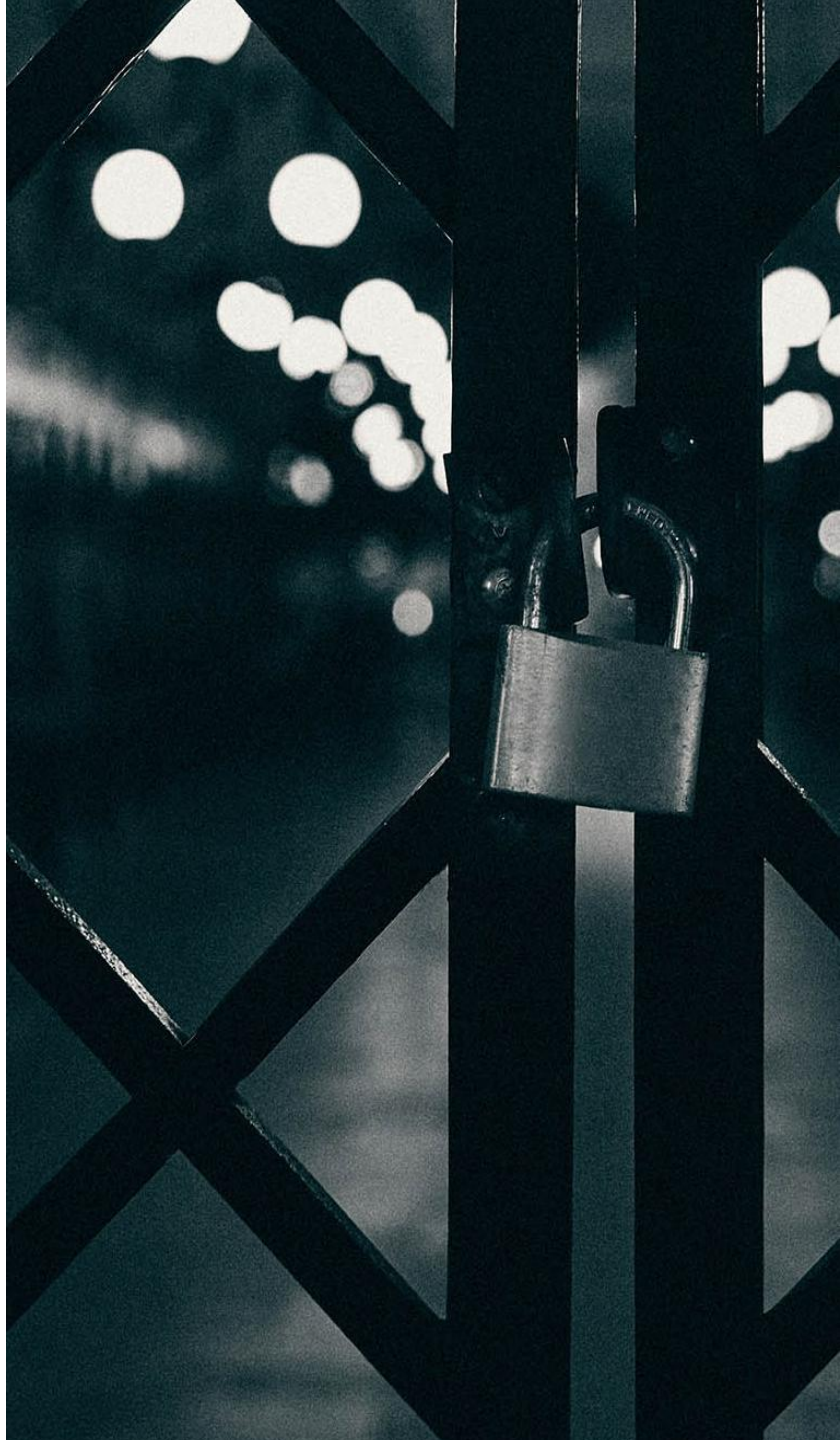
Rather than treating the engagement as a simple technology deployment, Secure Nexus began by establishing a clear understanding of the organisation's operating model, risk exposure, and dependency on Microsoft 365 for day-to-day business activity. This ensured that every control introduced directly supported a defined risk-reduction objective.

The approach centred on building security into the foundation of the environment. Microsoft 365 was positioned as the core collaboration and identity platform, with Secure Nexus applying hardened baseline configurations aligned to recognised best practice. Identity, access control, and auditability were prioritised early to ensure visibility and accountability were in place before additional services were layered on.

To address data protection and resilience, Secure Nexus implemented a dedicated cloud backup and recovery capability, isolated from the production environment. This provided assured recoverability, defined retention, and demonstrable resilience against data loss and ransomware scenarios.

Email security and phishing risk were reduced through a combination of technical controls and policy enforcement, strengthening protection against spoofing, impersonation, and malicious content without disrupting normal business communication.

Crucially, the solution was delivered as a managed service, not a one-off project. Secure Nexus retained responsibility for ongoing monitoring, security oversight, and continuous improvement, allowing Cunningham Engineering to benefit from enterprise-grade security assurance without increasing internal workload or requiring in-house security expertise.



Solution Delivered

To address Cunningham Engineering's security and resilience requirements, Secure Nexus delivered a secure, modern Microsoft 365 platform designed to reduce cyber risk while supporting day-to-day collaboration and business operations.

Secure Microsoft 365 Foundation
A new Microsoft 365 tenancy was deployed with a security-first configuration, providing a robust collaboration backbone for email, file sharing, and teamwork. Baseline security controls were applied from day one, ensuring the environment was hardened and auditable as it entered live operation.

Identity & Access Control
Centralised identity management was implemented with enforced multi-factor authentication and role-based access control. This ensured users only had access appropriate to their role, while providing full auditability of authentication and administrative activity, significantly reducing the risk of account compromise.

Email Security Hardening
Email security was strengthened through the correct implementation of SPF, DKIM, and DMARC. These controls reduced exposure to spoofing, impersonation, and phishing attacks, improving trust in outbound email and protecting users from malicious or deceptive messages.

Backup, Recovery & Resilience
To protect business-critical data, cloud backup for Microsoft 365 workloads was implemented using Druva. This delivered assured backup, defined retention, and the ability to recover data quickly in the event of accidental deletion, ransomware, or service disruption.

User Awareness & Phishing Resilience
Recognising that people are a critical part of the security model, the solution included security awareness and phishing resilience capabilities. This helped users better recognise threats and reinforced technical controls with informed user behaviour.

Outcomes & Benefits

+ Secure, reliable collaboration across email, files, and cloud services, enabling staff to work efficiently on a trusted Microsoft 365 platform.
+ Reduced operational and cyber risk through embedded security controls, without introducing additional complexity or management overhead.
+ Improved confidence in data protection and recovery, with assured backup, defined retention, and tested recovery processes in place.
+ Significant reduction in phishing and spoofing risk, driven by hardened email authentication and improved protection against impersonation attacks.
+ Auditable access and security controls, supporting compliance, investigation, and future assurance requirements.
+ Demonstrable backup and recovery assurance, ensuring business-critical data can be restored in the event of disruption, data loss, or ransomware.

Secure Nexus provided exactly what we needed - a clear, security first approach without adding complexity to our day-to-day operations, allowing the whole office to be linked and able to share required documents, also providing access to back-up systems ensuring we can remain compliant with all our document storage. They strengthened our M365 environment, improved our visibility and resilience and gave us real confidence in our data protection and recovery along with helping us achieve accreditation status on some of the leading construction platforms such as Construction Line Gold.

We also have access to valuable training modules developing our knowledge and awareness of the risks associated with online activity.

The team are pragmatic, knowledgeable and operate as a trusted partner rather than just a supplier.

Always contactable and ready to help with any issues we may have.

We would highly recommend Raymond and his team for any digital support.

Clair Johnstone
Operations Manager

Secure Nexus, your digital defence partner

Secure Nexus works as a trusted security partner, not simply a technology provider. By combining deep technical expertise with a strong understanding of how small and growing organisations operate, Secure Nexus delivers practical, risk-led security that strengthens resilience without adding unnecessary complexity.

The focus remains on reducing real-world risk, improving assurance, and enabling organisations to operate with confidence supported by security controls that are proportionate, effective, and continuously managed.

SME-Focused Experience

Proven experience delivering security services for small and medium-sized organisations without dedicated in-house IT or security teams, where simplicity, clarity, and accountability are essential.

Risk-Led Design

A security-first design philosophy that builds solutions around risk reduction, control, and assurance, rather than deploying tools in isolation.

Operational Pragmatism

A strong balance between technical depth and operational pragmatism, enabling meaningful security outcomes without disrupting day-to-day business operations.

Defensible Assurance

A clear focus on delivering ongoing assurance not just implementation providing defensible insight that supports governance, compliance, and informed decision-making.

SECURE NEXUS

Your digital defence partner.

enquires@securenexus.co.uk
01786 236 632

Trusted. Certified. Recognised.