SECURE NEXUS
Your digital defence partner.

WorKing Flexispaces & King Street ApartHotel

Secure Nexus, Case Study

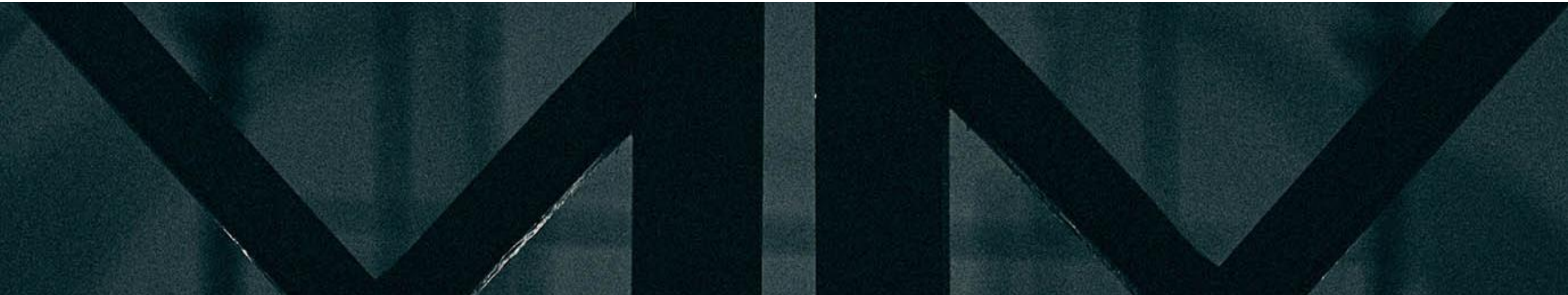
Client Overview

WorKing Flexispaces, part of NOMM Properties, operates a modern, mixed-use building that brings together flexible office space and hospitality services within a single environment. The site includes shared collaboration areas, private offices, hot-desking facilities, and the King Street ApartHotel, supporting both business tenants and short- and long-stay hotel guests.

This model creates a complex operating environment where tenants, hotel guests, staff, and building systems all rely on shared digital infrastructure, while requiring clear separation for security, privacy, and performance. Guest Wi-Fi, business networks, hotel systems, and internal operations must coexist without introducing risk or impacting user experience.

To support this, WorKing Flexispaces required an IT and network foundation capable of securely supporting both commercial workspace and hospitality operations. The solution needed to provide strong isolation between user groups, centralised management, and the resilience required to deliver consistent service across a multi-tenant, customer-facing environment.

NOMM Properties operates technology-enabled, flexible workspaces designed to support modern, high-growth businesses. The operating model is intentionally lean, with minimal on-site IT or facilities staff, placing a greater dependency on secure, reliable technology to underpin tenant operations, building services, and day-to-day management.



The Challenge

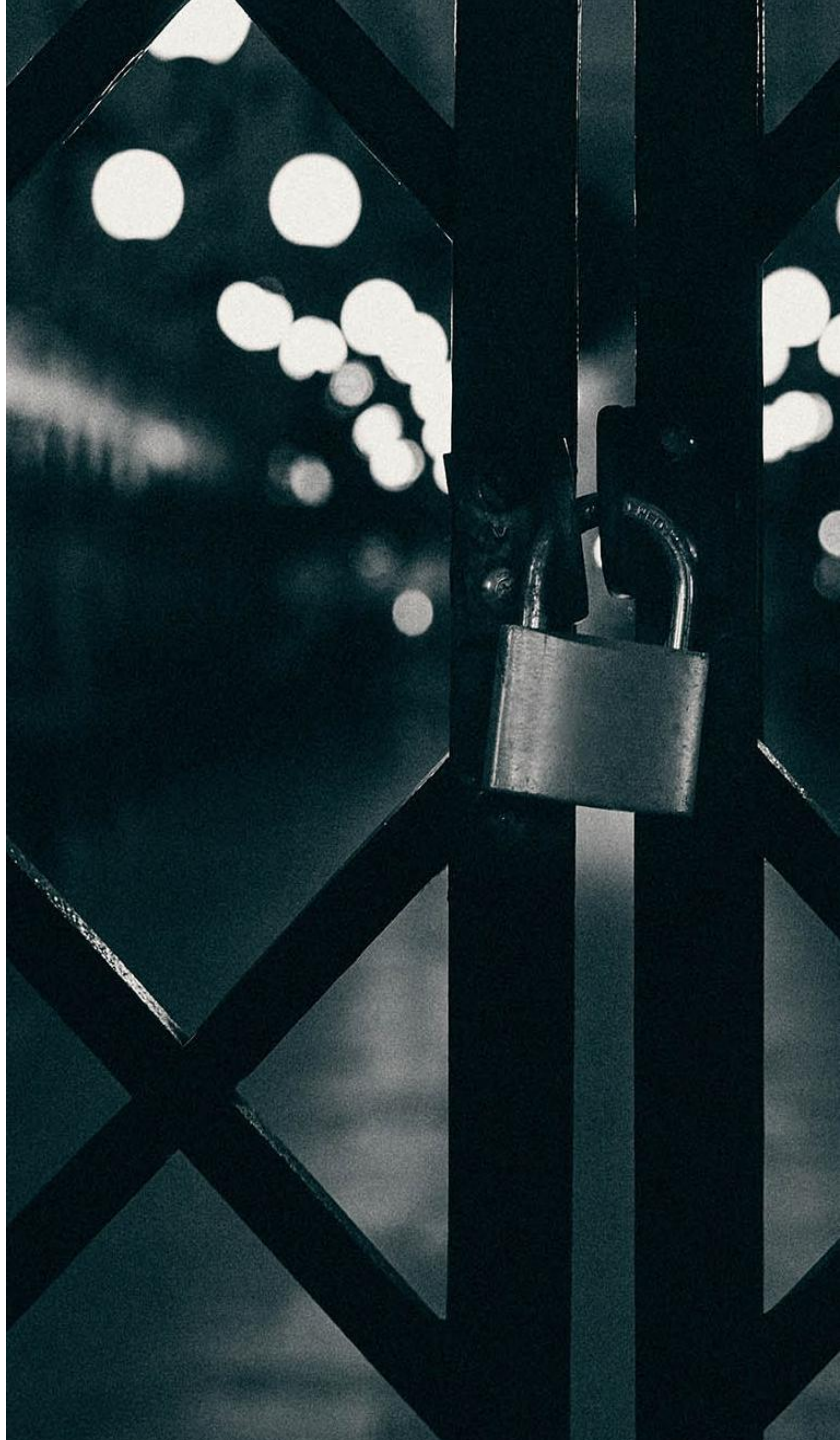
Operating a mixed-use building that combines flexible workspaces and hospitality introduced several interconnected technical and security challenges for WorKing Flexispaces and King Street ApartHotel. Multiple independent tenant organisations, hotel guests, and internal teams all relied on the same underlying infrastructure, yet each required a different level of access, security, and assurance.

A core challenge was supporting multiple independent tenants on shared network infrastructure without introducing the risk of cross-tenant visibility or data exposure. This was further complicated by the need to deliver public and private Wi-Fi services across the building, ensuring hotel guests and visitors could connect easily, while business users and operational systems remained securely isolated.

The organisation also needed to support hybrid working across staff, directors, and mobile devices, with users regularly accessing systems both on-site and remotely. Ensuring secure access to email, files, and applications without increasing administrative overhead or weakening security controls was a key concern.

Over time, the IT environment had become dependent on multiple third-party suppliers, creating fragmented responsibility, inconsistent standards, and limited visibility across the estate. This made it harder to manage risk, respond quickly to issues, or maintain a consistent level of service across both workspace and hotel operations.

From a security perspective, the growing threat of phishing, ransomware, and account compromise required a more proactive and structured approach to cyber resilience. The organisation needed better protection across Microsoft 365, endpoints, and user identities, alongside improved monitoring and incident response capability.



Objectives

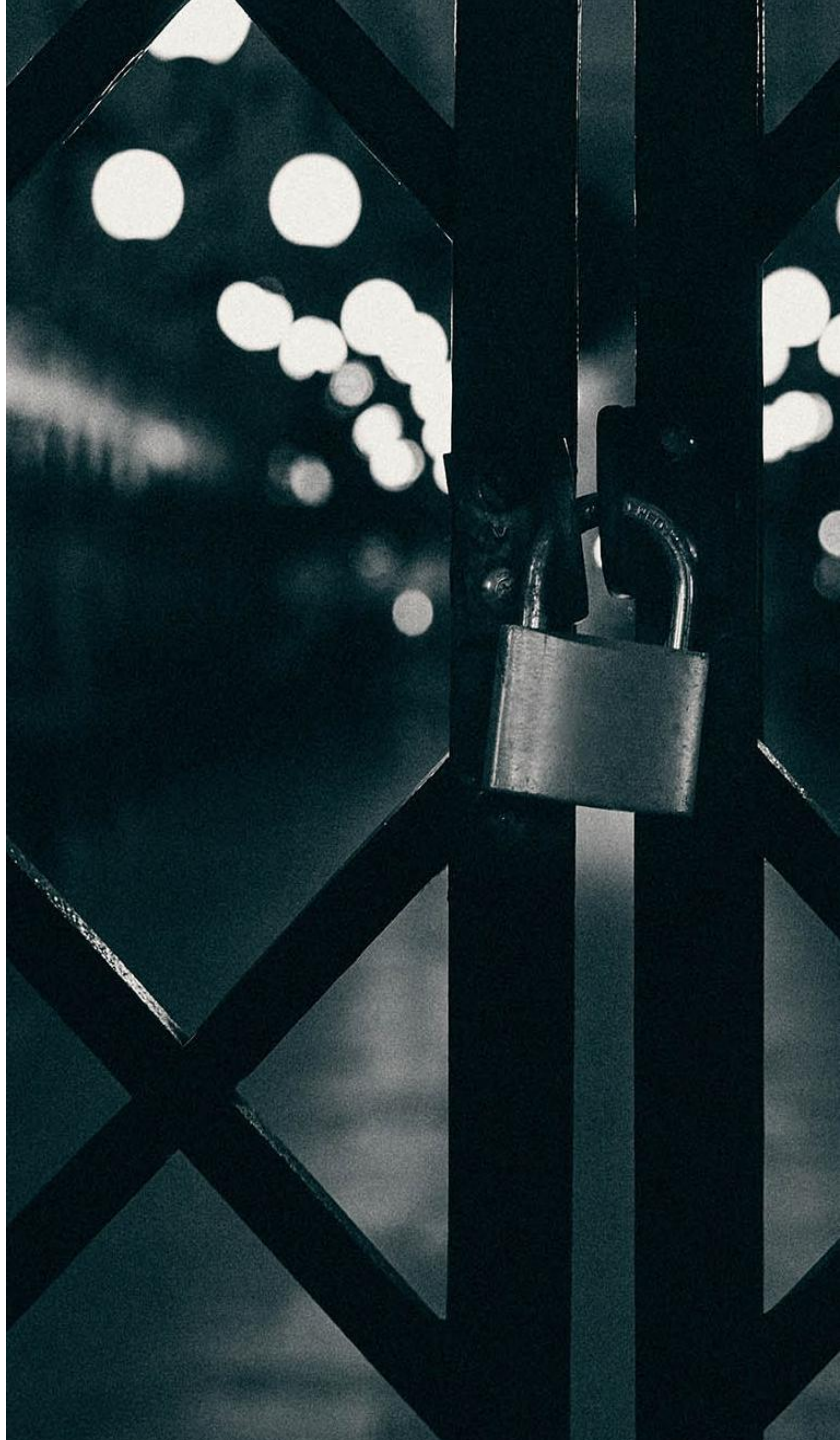
WorKing Flexispaces partnered with Secure Nexus with the objective of establishing a secure, resilient, and centrally managed technology foundation capable of supporting both flexible workspace and hospitality operations within a single environment.

A key priority was the implementation of a secure Microsoft 365 platform, providing consistent identity management, collaboration, and data protection across staff, tenants, and operational users. This needed to be centrally managed, with clear visibility and control, while remaining flexible enough to support hybrid and remote working.

The organisation also sought to move towards identity-driven access control, ensuring that access to systems and services was determined by user identity, device posture, and role, rather than location alone. This approach was essential to supporting mobile users while reducing the risk of unauthorised access or account compromise.

Improving cyber resilience was a core objective. WorKing Flexispaces required layered protection across email, endpoints, and cloud services, reducing exposure to phishing, ransomware, and other common attack vectors. This was to be complemented by 24×7 security monitoring, enabling early detection of threats and rapid response before incidents could impact tenants or hotel operations.

From a network perspective, the goal was to securely segment traffic so that tenants, hotel guests, and internal systems could operate safely on shared infrastructure without visibility or risk between environments. This was critical to maintaining both security and service quality in a multi-tenant, customer-facing building.



Secure Nexus Approach

Secure Nexus delivered a security-first managed IT and network platform designed for a mixed-use environment combining flexible workspaces and hospitality. The solution unified identity, endpoint, cloud, and network controls into a centrally managed architecture, providing consistent security and visibility across the site.

A securely configured Microsoft 365 environment formed the foundation of the platform, enabling collaboration through Exchange, Teams, SharePoint, and OneDrive. The tenant was hardened using security best practice to support hybrid working while protecting email and business data.

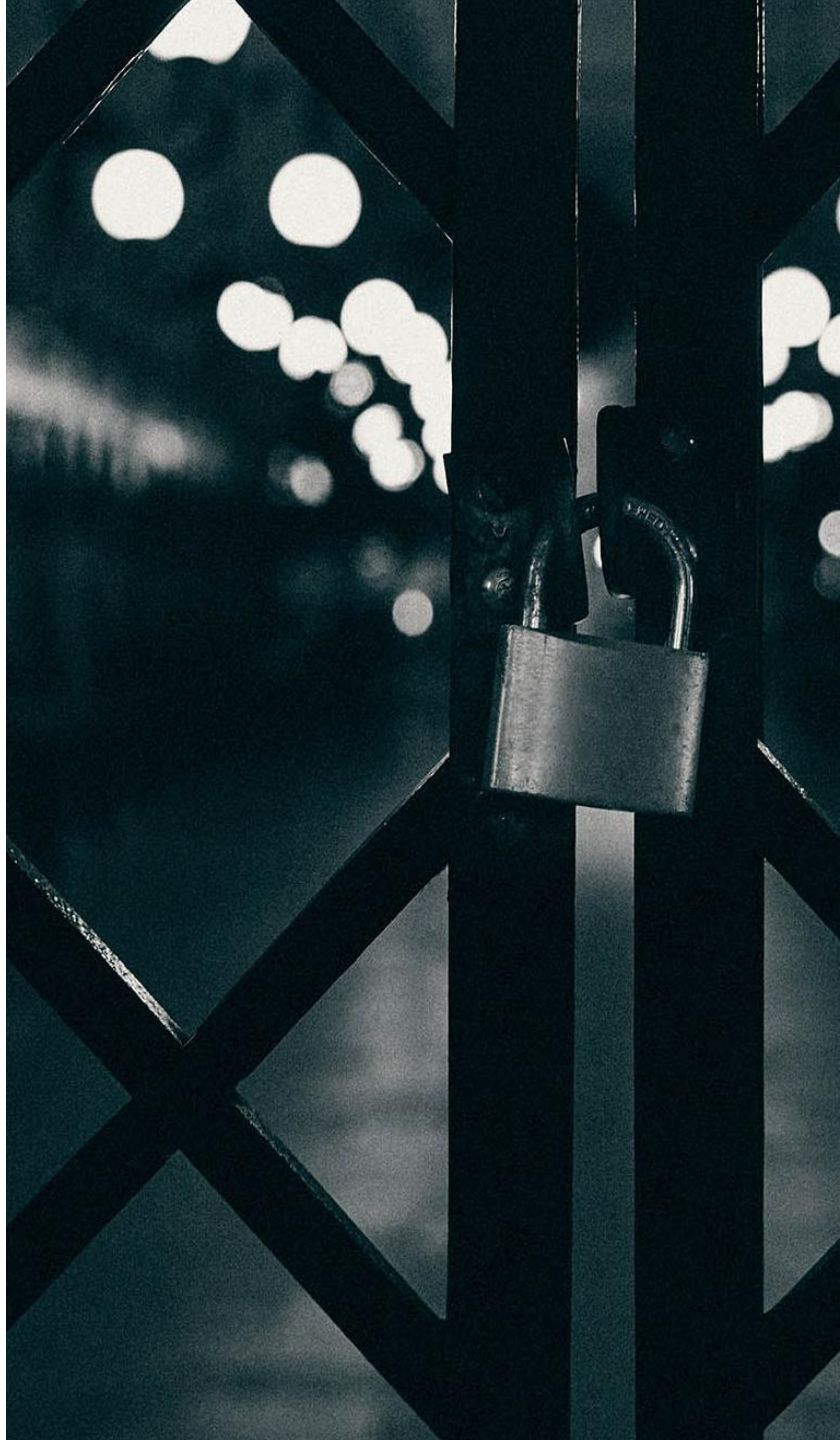
Centralised identity and access management was implemented using JumpCloud, introducing single sign-on, multi-factor authentication, and device trust. Access was driven by user identity and device posture, reducing the risk of account compromise and simplifying administration.

Email security was strengthened with advanced phishing and impersonation protection, while endpoint protection combined antivirus, EDR, and MDR with automated containment to limit the impact of security incidents.

The environment was integrated with the Secure Nexus 24×7 Security Operations Centre (SOC), providing continuous monitoring, threat triage, and incident response across endpoints, Microsoft 365, and network activity.

To ensure data resilience, immutable Microsoft 365and Network configuration backups were deployed and regularly tested, enabling rapid recovery from accidental deletion, ransomware, or service disruption.

Finally, segmented wired and wireless networks were implemented to securely separate tenants, hotel guests, and internal systems, supported by ongoing user security awareness and phishing simulations to reduce human risk.



Architecture Overview

The solution architecture was designed around the principles of segmentation, least privilege, and zero trust, ensuring that all users and systems could operate safely on shared infrastructure without unnecessary access or exposure.

At the network layer, Secure Nexus implemented clearly defined and isolated network zones to separate tenants, hotel guests, building operations, and management systems. This approach ensured that each environment could operate independently, preventing lateral movement and reducing the risk of cross-tenant or guest-to-business access, while still maintaining reliable connectivity across the site.

Access to systems and services was governed through a centralised identity platform, rather than relying on network location. User identity, device trust, and role determined what users could access, whether they were on-site or working remotely. This allowed consistent enforcement of least-privilege access across devices, applications, and administrative functions.

All security and operational telemetry from endpoints, Microsoft 365, identity systems, and the network was fed into the Secure Nexus Security Operations Centre (SOC). This centralised visibility enabled correlation across multiple data sources, allowing potential threats to be identified early and responded to quickly.

By combining network segmentation with identity-driven access control and continuous monitoring, the architecture delivered strong tenant isolation while maintaining full operational visibility and control, supporting both secure day-to-day operations and long-term scalability.

Solution Delivered

To support a mixed-use environment combining flexible workspaces and hospitality, Secure Nexus delivered a layered, security-first managed IT and network solution providing continuous protection, visibility, and operational assurance across the site.

The solution unified identity, endpoint, cloud, network, and monitoring controls into a single platform. This ensured security aligned with real-world risk in an environment where tenants, hotel guests, staff, and building systems share common infrastructure.

Identity-Centric Access Control
Identity was established as the primary control plane, governing access to systems, applications, and privileged functions based on user role and device trust. This enabled consistent least-privilege enforcement while supporting hybrid and mobile working.

Segmented Network Architecture
The network was designed with clear separation between tenant environments, hotel guest access, building operations, and management systems. while maintaining reliable connectivity throughout the building.

Endpoint, Email, and Cloud Protection
Layered protection was deployed across endpoints, email, and Microsoft 365 to reduce exposure to phishing, ransomware, and account compromise. Automated containment limited the impact of security incidents without disrupting operations.

Continuous Monitoring and Response
Telemetry from identity, endpoints, cloud services, and the network was integrated into the Secure Nexus 24×7 SOC, enabling early threat detection, correlation across layers, and rapid incident response.

Data Resilience and Assurance
Immutable Microsoft 365 backups were implemented and regularly tested, ensuring rapid recovery from data loss, ransomware, or service disruption and providing confidence in business continuity.

Outcomes & Benefits

+ Improved visibility of users, devices, and network activity across a shared, multi-tenant environment, providing clearer insight into operational and security risk.
+ Reduced cyber risk across tenant, guest, and internal systems through segmentation, identity-driven access control, and layered security controls.
+ Faster detection and response to security incidents through 24×7 monitoring and centralised threat correlation, minimising impact to tenants and hotel operations.
+ Increased confidence in the protection of Microsoft 365, endpoints, and business-critical data through continuous monitoring and tested recovery processes.
+ Simplified IT and security governance by consolidating responsibility under a single, accountable security partner, reducing operational complexity.
+ Strengthened overall security posture without compromising tenant experience, guest connectivity, or day-to-day workspace and hospitality operations.
+ The security architecture aligns with Cyber Essentials requirements, enabling NOMM Properties to offer a workspace environment that meets recognised UK cyber security standards.

“Secure Nexus have fundamentally strengthened the resilience and security of our mixed-use environment. Their ability to design a segmented, identity-driven architecture that protects both our business tenants and hotel guests without disrupting day-to-day operations has been exceptional.

What sets them apart is their balance of deep technical capability and operational pragmatism. Where they simply don't just deploy technology; they delivered clarity, assurance, and confidence. We now have full visibility across our estate, stronger cyber protection aligned to recognised UK standards, and a trusted long-term security partner who understands the realities of operating a modern, multi-tenant building.”

Neil Munday – Managing Director of NOMM Properties

Secure Nexus, your digital defence partner

Secure Nexus works as a long-term security partner, not simply a technology provider. By combining deep technical capability with a strong understanding of multi-tenant, mixed-use environments, Secure Nexus delivers security that is practical, defensible, and aligned to real operational needs.

The focus remains on reducing risk, improving resilience, and providing clear assurance enabling organisations to operate with confidence without compromising service quality, user experience, or business growth.

Multi-Tenant & Mixed Use

Proven experience delivering secure IT and cybersecurity services within flexible workspace, hospitality, and shared infrastructure environments, where tenant isolation, guest access, and operational continuity are critical.

Risk-Led Design

A security-first design philosophy that prioritises risk reduction, least privilege, and resilience, ensuring solutions are built around real-world threat scenarios rather than tool deployment alone.

Operational Pragmatism

A strong balance between technical depth and operational practicality, delivering meaningful security outcomes without disrupting live services, tenants, or guest experience.

Defensible Assurance

A clear focus on assurance over complexity, providing visible, auditable security controls and insight that supports governance, accountability, and informed decision-making.

SECURE NEXUS

Your digital defence partner.

enquires@securenexus.co.uk
01786 236 632

Trusted. Certified. Recognised.