NETWORK SECURITY
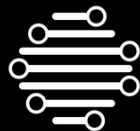
ABOUT SECURE NEXUS

At Secure Nexus, our mission is to empower small and medium-sized businesses with affordable and cutting-edge Cyber Security solutions. We are dedicated to fortifying your digital assets, connecting your operations securely, and defending your infrastructure against evolving cyber threats.

By building a Secure Nexus for your organisation, we strive to ensure that every business, regardless of size, can navigate the digital landscape with confidence, knowing their data and operations are safeguarded. Our commitment lies in making Cyber Security accessible, reliable, and tailored to the unique needs of each client, because your security is our priority. Fortify, connect, defend – together, we create a resilient foundation for your business in the digital age.

OUR CORE VALUES

- **DELIVER WOW THROUGH CYBERSECURITY**
- **GIVE & TAKE RESPONSIBILITY**
- **BE REAL (WITH YOURSELF AND OTHERS)**
- **COLLABORATION**
- **PURSUE GROWTH & LEARNING**
- **BE ADVENTUROUS, CREATIVE, AND OPEN MINDED.**
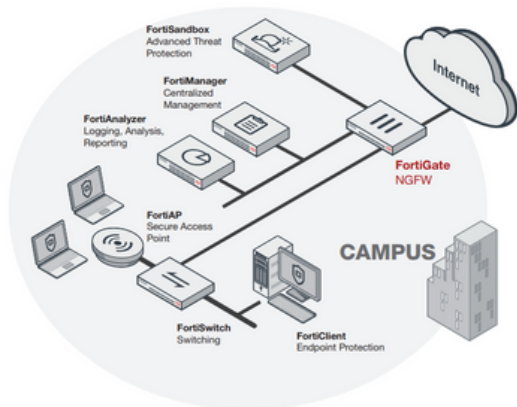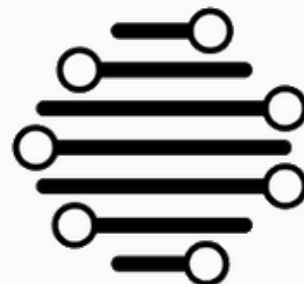
NETWORK SECURITY
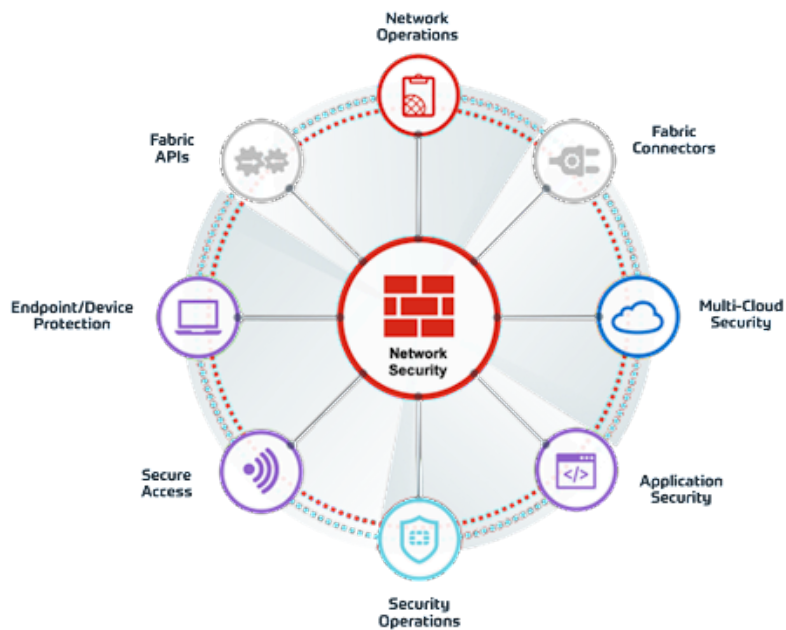
Growing and scaling digital business while protecting a distributed infrastructure has never been more critical or complex. Networks today are centre of innovation and enable digital acceleration using network modernisation. Fortinet's Secure Networking converges networking technologies with AI-powered security across all edges to close security gaps and help organisations achieve better user experience.

Digital acceleration has led to a rapid expansion of attack surfaces and creation of new network edges, including LAN, WAN, 5G, remote workers, and clouds. Fortinet's Secure Networking approach is the industry's only converged networking and security platform. This convergence enables AI-powered defence of today's highly dynamic environments while enabling better productivity and user experience.

NETWORK SECURITY

IMPORTANCE OF NETWORK SECURITY

The threat landscape has evolved significantly in recent years, with cybercriminals increasingly targeting networks as a means of gaining access to sensitive and valuable data. As decentralised networking is driven by cloud technologies, the attack surface has diversified away from a traditional local area network, increasing risk by now incorporating SD-WAN, edge networking, and even mobile or local Wi-Fi. This offers cyber criminals a much wider attack surface to access organisations.

Reduce the complexity and maximise your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)

Full visibility into users, devices, and applications across the entire attack surface, and consistent security policy enforcement irrespective of asset location

Protect against network exploitable vulnerabilities with industry validated IPS that offers low latency and optimised network performance

Automatically block threats on decrypted traffic using the industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers

Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport

Accelerated multi-cloud access for faster SaaS adoption with cloud-onramp

Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and realtime bandwidth compute-based traffic steering

Automated overlay tunnels provide encryption and abstracts physical hybrid WAN making it simple to manage

Simplified and intuitive workflow with SD-WAN orchestrator for management and zero touch deployment

Enhanced analytics both real-time and historical provides visibility into network performance and identifies anomalies

Strong security posture with next generation firewall and real- time threat protection
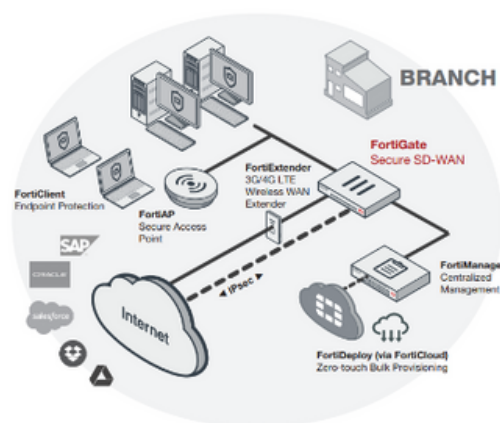
TEAM

DANIEL SCHROEDER – MANAGING DIRECTOR

An adept Azure Consultant with a decade-long track record, I specialise in architecting and implementing cutting-edge solutions within the Azure ecosystem. My proficiency encompasses Azure Infrastructure Migration, Network & Security, Virtual Desktops, and Virtual Compute. Serving as a Tech Lead, I've orchestrated seamless global deployments of Azure architectures, leveraging tools like Terraform to optimise Infrastructure as Code implementation and ensure code control efficiency.

Beyond infrastructure design, my expertise extends to Azure Active Directory and Virtual Desktop implementations, showcasing a holistic grasp of Azure services. Recognised as a Design Authority, I've become a sought-after specialist in Azure design, complemented by a versatile skill set in all technologies.

In high-pressure scenarios, I thrive, consistently delivering strategic insights and technical innovation. My proven ability to navigate complex technological landscapes positions me as a dynamic and results-driven professional, ready to contribute optimal outcomes for organisations seeking a forward-thinking cloud/networking expert.

RAYMOND SETCHFIELD – MANAGING DIRECTOR

Raymond has dedicated the past several years to the dynamic IT industry, gaining extensive experience in the demanding realms of ISP and Server Hosting. His focus primarily revolves around Linux, Storage, and Virtualisation Technologies, showcasing expertise in implementing, running, designing, and maintaining large-scale networks encompassing several hundred systems.

A pivotal contributor to the redesign of both the FlexiScale virtualization platform and SymetriQ's, Raymond played a crucial role in designing and creating a highly scalable PaaS during his tenure at Flexiant. In recent years, his focus has shifted towards AWS, where he specialises in designing scalable platforms tailored to meet the unique needs of clients.

With a recently completed master's degree in advanced security and digital forensics, Raymond looks to leverage this new skillset to complement his extensive IT background. His diverse range of certifications, including AWS Solutions Architect, AWS Certified Security - Specialty, Google Cloud Certified Architect, CCNP Network Security, Fortinet Certified Network Security and Certified Ethical Hacker v11, reflects his commitment to staying at the forefront of evolving technologies in the field of cybersecurity and cloud computing.

DEJI OSINOWO – HEAD OF GOVERNANCE

With an extensive 15-year tenure in the IT industry, Deji brings a wealth of experience to the table as a dedicated Cybersecurity Professional, with a concentrated focus on Information Security for the past 5 years. Specialising in implementing and overseeing security measures, he possess a deep understanding of critical frameworks, including NIST 800-53, ISO 27001, and familiarity with the Cyber Essentials government scheme. Proficient in Risk Management Framework (RMF), Cybersecurity Framework (CSF), and various risk management methodologies, his active involvement in Security Operations Centre (SOC) operations ensures a robust security posture.

His role extends beyond mere oversight, encompassing the meticulous conduct of 3rd-party risk assessments and the optimisation of onboarding processes for enhanced efficiency. In essence, his approach is grounded in a comprehensive skill set and practical experience, ensuring a resilient and secure digital environment. This proposal reflects my commitment to contributing substantively to your organisation's cybersecurity needs, leveraging my expertise to navigate the evolving landscape of cyber threats.