Solution Brief

Secure and Scalable Home Networking for the Enterprise
Increasing Risk of the Hybrid Workforce

According to a recent report, employees are spending 60% of their working time at home compared to 5% before the pandemic. With ransomware activity up 10.7x and e-mail phishing on the rise, there is a significant increase in the risk of cyber threats targeting employees connected to their home networks. Organizations must re-think their security strategy for protecting work from home (WFH) employees and the corporate networks they access. To complicate matters, 39% of employees report that their cybersecurity practices at home are less thorough than at work.

Protecting Employees and Corporate Assets

With millions of employees working from home more frequently, the home office has become the new edge of the corporate network. Unlike the corporate network, the home network lacks enterprise layered network defenses such as network segmentation, firewalls, threat detection, and monitoring. Additionally, because employees share their home networks with family members who may not have strong endpoint security controls, everyone on the network is more vulnerable to malware and lateral cyber-attacks. An infection on one home computer could compromise an employee’s computer that accesses the corporate network, leading to a security breach.

Governance, Risk, and Compliance

Hybrid work is here to stay, and businesses must strengthen their WFH security measures to address governance, risk, and compliance considerations. For their internal policies and standards to be consistent throughout, organizations need to address this greater attack surface and meet privacy and cybersecurity guidelines.

Requirements for a Scalable Hybrid Workforce

Scaling a hybrid workforce requires implementing security solutions that are strong and easy to manage remotely. Without onsite tech support in the home office, businesses need a solution that does not rely on the technical expertise of the employee. Enterprises should consider the following requirements for secure home networking:

- Network segmentation to separate work and personal traffic
- Network visibility and control
- Remote automation and management
- Home network reliability and performance
- Employee privacy

For more information on securing home networks, read our white paper on Enabling Hybrid Workforce Productivity.
Linksys and Fortinet Partner to Secure WFH Networks

Linksys and Fortinet have partnered to provide an advanced networking solution that protects employees working from home. Well-suited for collaboration, Linksys HomeWRK for Business | Secured by Fortinet is a best-in-class Wi-Fi networking solution for the home that provides enterprise-grade security, visibility, centralized management, and high-performance.

Introducing HomeWRK for Business

HomeWRK for Business provides the security, visibility, control, performance, and manageability that businesses of all sizes require. HomeWRK includes a high-performance Wi-Fi 6 Mesh router for the home that embeds Fortinet’s industry-leading Next Generation Firewall (NGFW) and FortiGuard Security Services to provide enterprise-grade security. The solution was designed to simplify and scale the deployment and management of secure home networking.

Security

HomeWRK for Business includes dual-SSID network segmentation to keep business and personal traffic separate. The solution includes the following security controls:

- Network segmentation
- Next generation firewall
- Antivirus protection
- Web and application filtering
- Intrusion protection services (IPS) that leverage Fortinet's FortiGuard IPS Library
- IPsec virtual private networking (VPN)
Visibility, Control and Compliance

HomeWRK for Business provides real-time visibility tools to monitor and respond to cybersecurity threats, vulnerabilities, and incidents. The Linksys Cloud Manager is a web-based tool that allows IT administrators to configure and manage HomeWRK devices remotely. HomeWRK also integrates with log management, analytics, reporting, and SIEM platforms. The solution enables compliance with NIST 800-53, CMMC, HIPAA, SOX, and IEC 62443.

Performance and Manageability

HomeWRK for Business supports Wi-Fi 6 and wireless mesh for high-speed whole-home coverage. HomeWRK includes application optimizations that improve the performance of on-line collaboration tools such as Zoom and Microsoft Teams. Linksys also improves manageability by simplifying provisioning, centralizing device management, and scaling distribution and fulfillment.

Why HomeWRK for Business

- Ensures only authorized employees can access the corporate network from home
- Provides for network auditability for access from home
- Ensures the confidentiality of data
-Protects against anticipated threats, such as phishing, ransomware, botnets, and MITM attacks
- Improves proof of compliance by reducing the reliance on the employee for following network security policies at home

Get Started with HomeWRK for Business