Fast-Track Security

30/90/180+ day Plan

0–30 days (quick wins)

- Enable MFA for all admin and user accounts and cloud services.
- Turn on automatic OS and major app patches for managed devices.
- Change default credentials on routers and firewalls; check firmware versions.
- Create separate SSIDs or VLANs for corporate, guest and IoT traffic.
- Deploy DNS filtering to block known malicious domains.
- Begin basic logging: enable VPN/authentication logs, firewall flow logs and DNS query logs locally.
- Draft one-page incident playbooks for the most likely events (compromised laptop, phishing click) and assign owners.
- Back up critical business data and device configurations; verify a basic restore.

90–180+ days (mature posture)

- Roll out cloud-managed endpoint protection to company devices.
- Implement centralised identity (SSO) and role-based access controls for key applications.
- Configure centralised log collection (cloud log store or managed logging) and forward VPN/firewall/DNS events.
- Pilot SD-WAN or ZTNA for critical remote users or a branch site to validate performance and security benefits.
- Refine incident playbooks and run a short tabletop exercise based on a real scenario; document lessons learned.
- Integrate EDR response capabilities into playbooks (isolate device, run scan, collect forensic artefacts).

30–90 days (operational hardening)

- Evaluate managed detection & response (MDR) or SOC-as-a-Service for continuous monitoring and alerting.
- Introduce microsegmentation around sensitive servers and data.
- Automate containment steps via EDR and integrate detection into incident workflows.
- Conduct formal incident exercises and update playbooks; test recovery from backups.
- Measure and report MTTD/MTTR improvements and drive continuous optimisation.

0844 856 3301
www.spectrum-coms.co.uk
spectrumcustomerservices@spectrum-coms.co.uk