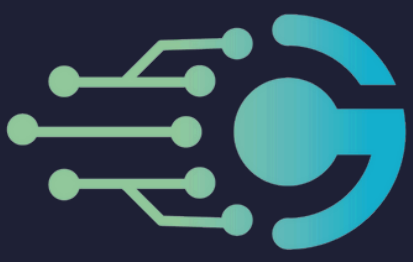
GUIDE

Securing Your Digital Perimeter

A Practical Guide for Financial Firms



Chapman Technology Partners

Why Your Digital Perimeter Matters

In financial services, trust is everything. Yet that trust is constantly under threat from cyber criminals exploiting the weakest point in your defences, your digital perimeter.
The digital perimeter includes:

- Laptops, desktops, tablets and smartphones
- Remote workers and hybrid setups
- Cloud storage and SaaS platforms
- Firewalls, routers and network entry points

Any gap in your perimeter is an open door to data breaches, ransomware, phishing attacks and regulatory violations.

Common Threats Facing Financial Firms

Phishing Attacks
A single click on a rogue email link can expose sensitive client data and credentials.

Unpatched Devices
Outdated software is like leaving your front door unlocked, vulnerabilities are easily exploited.

Poor Password Hygiene
Weak or reused passwords create risk across all cloud apps and accounts.

Unsecured Remote Access
Hybrid working increases exposure unless access is encrypted and authenticated.

91% of cyber attacks begin with a phishing email, making employees the most common entry point into a firm's digital perimeter.

Source: UK National Cyber Security Centre (NCSC)

How to Secure Your Digital perimeter

1. Start with a Security Audit

Map every entry and exit point of your network. Include:

- Remote access methods (VPN, RDP, remote desktop tools)
- Devices (company and personal)
- SaaS platforms (Microsoft 365, CRM tools, cloud backups)

A managed IT provider can help uncover blind spots you didn't know existed.

---

2. Deploy Endpoint Detection & Response (EDR)

EDR tools continuously monitor devices for suspicious behaviour, blocking threats in real time, far beyond what traditional antivirus software can do.
Essential for:

- Accountants working on sensitive spreadsheets
- Mortgage advisors accessing cloud databases
- IFAs handling client portfolios from laptops

---

3. Use a Zero Trust Model

Zero Trust means: "Never trust, always verify."
Assume every login attempt is hostile until proven otherwise.
Use:

- Multi-factor authentication (MFA)
- Conditional access policies
- Role-based access controls

Especially important where client data is stored in the cloud.

4. Secure Your Remote Access

- Replace insecure remote desktop tools with encrypted VPNs
- Enable MFA on all remote logins
- Monitor all remote sessions for anomalies

---

5. Harden Your Firewalls and Routers

Make sure your routers and firewalls are:

- Configured by professionals (not out-of-the-box)
- Regularly updated
- Supported by intrusion detection systems (IDS)

---

6. Regular Staff Training

Cyber security isn't just an IT problem, it's a people problem.
Train staff regularly on:

- Spotting phishing emails
- Safe password practices
- Reporting suspicious behaviour

Even one trained team member spotting a phishing attempt can stop a major breach.

---

7. Partner with a Cyber security-Focused IT Provider

Ongoing monitoring, patch management, threat detection and compliance support can't be handled ad hoc. You need a partner who understands the unique pressures of FCA-regulated firms.

What's the Risk of Doing Nothing?

- Fines from the ICO or FCA
- Loss of client trust
- Financial theft or ransom demands
- Reputational damage that lingers for years

Securing your digital perimeter isn't a one-time project, it's a continuous process. And in a sector as sensitive as financial services, the risks of neglecting it are simply too high.

Want to Know Where Your perimeter Is Weak?

Book your free cyber security assessment with Chapman Technology Partners.

We'll help you:

- ✅ Identify gaps
- ✅ Strengthen your defences
- ✅ Sleep easier at night

www.chapmantechnologypartners.co.uk

Chapman Technology Partners

Strategic IT, Cyber Security & AI Solutions for Regulated Firms

Strawberry Fields Digital Hub, Chorley, PR7 1PS | enquiries@ctpartners.co.uk 01257 542388

CYBER ESSENTIALS CERTIFIED