PROTEC

MAKING IT SIMPLE

Cyber Security

protecit.co.uk

In today's connected world, businesses face an ever-growing range of cyber threats - from data breaches and ransomware to phishing attacks and system vulnerabilities. Our cyber security services are designed to protect your business at every level, combining advanced technology, expert monitoring, and proactive defence strategies to keep your operations secure.

Partnering with us means more than just protection. It means **peace of mind**. Strong cyber security safeguards your sensitive data, ensures business continuity, strengthens customer trust, and helps you stay compliant with industry regulations. By securing your environment, you're setting your business up for resilience and stability.

Service Offerings

Our EDR covers the detection, investigation, and response to cyber threats on endpoints, which includes devices such as your laptops, desktops, mobile phones, and servers. Continuously monitors these devices for suspicious behaviour to identify and contain threats such as ransomware, malware, and advanced persistent threats in real-time.

Benefits of our EDR solutions:

- **Endpoint monitoring:** It continuously logs and analyses data from endpoints to detect malicious activity.
- **Threat detection:** It identifies threats that traditional antivirus might miss, including sophisticated and unknown (zero-day) attacks.
- **Automated response:** It can automatically perform actions like quarantining a device or killing malicious processes to contain threats instantly.
- **Forensic analysis:** It provides detailed information about an incident, allowing security analysts to investigate the "what, where, and how" of a breach.
- **Real-time visibility:** It provides a continuous, 24/7 view of what is happening on your endpoints, which is crucial for early threat detection.

Firewall Management

Firewall security management is the ongoing process of configuring, monitoring, and maintaining a firewall to protect a network from unauthorised access. It involves setting security rules, updating software (firmware), and monitoring traffic and logs to detect and respond to threats. Effective management ensures that only legitimate traffic is allowed through the network's barrier between your trusted network and the outside world.

Benefits of firewall security management:

- **Policy and Rule Configuration:** Defining, creating, and enforcing the rules that determine what network traffic is allowed or blocked, based on factors like IP address, port, and protocol.
- **Monitoring and Logging:** Continuously analysing traffic logs and alerts to identify suspicious activity, detect potential threats, and understand network behaviour.
- **Updates and Maintenance:** Regularly updating the firewall's software firmware to patch vulnerabilities and ensure devices operates at peak efficiency.
- **Change Management:** Implementing strict processes for documenting and reviewing any changes to firewall rules or policies to prevent misconfigurations.
- **Compliance:** Ensuring that the firewall's configuration and operations meet relevant security and regulatory standards (Cyber Essentials / Cyber Essentials Plus).

Why this important for your business

- **Protects against threats:** It acts as a primary defence against cyber attacks, malware, and other malicious traffic attempting to gain access to your network.
- **Ensures access control:** It prevents unauthorised users from accessing sensitive internal networks and resources.
- **Supports business operations:** It ensures that necessary, authorised traffic can flow uninterrupted, allowing employees to work efficiently.
- **Maintains compliance:** It helps organisations meet industry regulations and security mandates.

Securing and Protecting Azure / Office 365

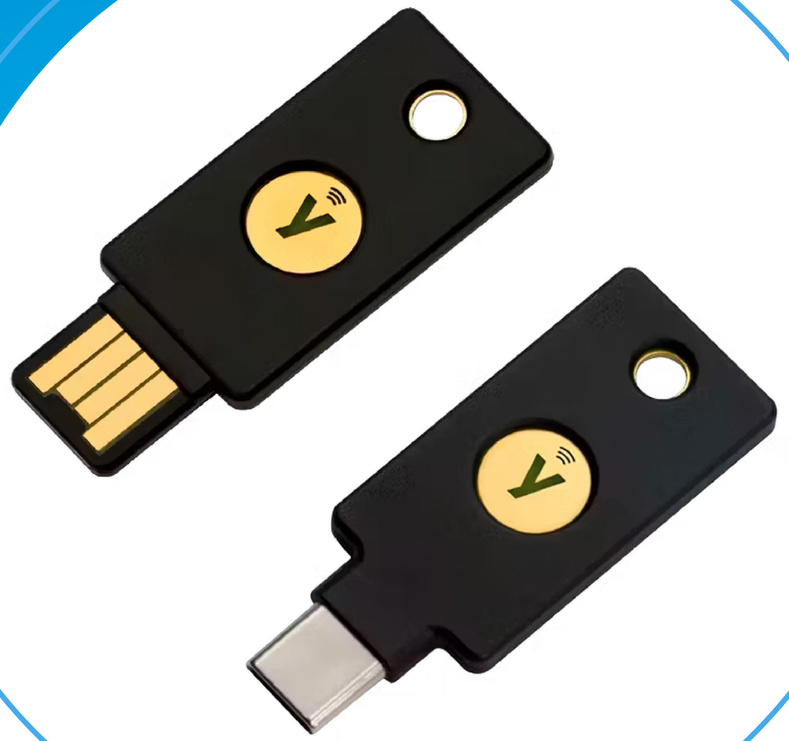
Cloud security protection uses policies, controls, and technologies to safeguard data, applications, and infrastructure in the cloud from threats like unauthorised access, data breaches, and malware. Key protection strategies include strong access controls with multi-factor authentication, data encryption at rest and in transit, threat detection and response systems, and security posture management tools to identify and fix misconfigurations.

Key protection strategies:

- **Access Control:** Implement strong identity and access management, including multi-factor authentication and role-based access, to limit who can access cloud resources.
- **Data Security:** Encrypt data while it is being transmitted across networks (in transit) and while it is stored (at rest). This is crucial for protecting sensitive information.
- **IP whitelisting and geo-blocking** (blocking traffic from countries not related to the locations of businesses user base).
- **Dedicated secure VPN connectivity** to ensure only authorised users can authenticate to your Azure / Office 365.
- **Regulatory Compliance:** Ensure that security measures meet relevant regulatory and industry standards.

Microsoft 365 Azure

Proven Expertise
Tailored Solutions
Compliance Assurance
Innovation at the Core



FiDO2 and Yubi Keys. Hackers locked out for good

One of the strongest and most hacker resistant protection methods available. Yubi Keys are designed to eliminate the vulnerabilities associated with passwords, SMS and Microsoft Authenticator-app code authentication, greatly strengthening an organisation's overall security posture and protection.

True Phishing Resistance
In the all too common instance a user is tricked into visiting a fake Azure or Office 365 login page, the login will not authenticate as the Yubi Key is locked to only authenticate to the genuine Microsoft login page. In addition, the Yubi Key must be physically plugged into the device the user is logging in from.

How will the users login once Fido2 and Yubi Key are deployed?
The users insert their Yubi into their device, press the button on the key, enter their PIN, that's it. Simply then remove the Yubi Key from your device. This procedure only needs to be performed once by your users, as once authenticated the users Yubi Key and the server create a secure cryptographic pairing.

Which devices are supported?
Fido2 and Yubi Keys can be used on all types of devices (computers, laptops, smart phones, tablets) across your organisation. Any device with a USB (USB-A or USB-C) port and the ability to attempt to login to Azure / Office 365.

Advantages of Fido2 and Yubi Keys within your organisation.
This protection prevents potential credential theft and remote account takeover, which in most instances is also unknow to the user until it's too late.

Hackers are no longer able to use these common tactics:

- Weak or reused passwords
- Credential stuffing
- Password spraying
- Keyloggers
- Social engineering targeting users for passwords

Which type of businesses is the protection for?
Any business with an Azure/Office 365 environment however, industries such as finance and healthcare especially benefit from FIDO2 keys ensuring they meet strict compliance and security requirements, including phishing-resistant MFA mandates, Cyber insurance obligations and Cyber Essentials requirements.

Cyber Awareness Training

Our Cyber awareness training solutions helps organisations protect themselves from cyber threats by recognising risks like phishing, social engineering, and malware across your userbase. Training aims to reduce human error, a common cause of security breaches, by teaching best practices for online safety, secure password management, and data protection. This knowledge is crucial for complying with regulations and creating a more secure online and internal environment for your business.

Areas of education:

- **Threat identification:** Recognising common attacks like phishing emails, vishing (voice phishing), and social engineering attempts.
- **Risk mitigation:** Learning how to prevent attacks by using strong passwords, identifying malware, and practicing safe internet use.
- **Data protection:** Understanding how to safeguard sensitive information, including company data, client data, and personal data.
- **Security best practices:** Following secure communication methods, proper device security, and understanding network security.
- **Incident response:** Knowing what to do when a security incident occurs, such as reporting suspicious activity.

Why this important for your business

- **Reduces human error:** Employees are often the first line of defence, training helps them avoid making costly mistakes.
- **Ensures compliance:** Many regulations, such as GDPR, require organisations to provide cybersecurity training.
- **Minimises financial and reputational damage:** By preventing breaches, training helps avoid the financial and reputational harm that can result from a security incident.
- **Empowers employees:** Training gives staff the knowledge to protect themselves both at work and in their personal online lives.
- **Builds a security culture:** It fosters an organisation-wide culture of security awareness and responsibility.

Phishing Testing

Our phishing testing simulations, are cybersecurity exercises where employees are sent realistic but harmless phishing emails to assess their ability to recognise and report fake emails. The results help organisations measure the effectiveness of their security training and identify areas for improvement. Employees who click on the simulated links or provide information are not harmed, but their actions are recorded to help train them for future, real-world threats.

How it works:

- **Simulated attacks:** Protec works with you to create fake emails to employees, designed to look like a genuine, urgent, or enticing message. These messages can be customised to appear to originate from service providers (Microsoft, Google, etc) or more bespoke such as your clients or supplier.
- **Action and response:** The test measures whether an employee clicks a malicious link, opens an attachment, or enters credentials.
- **Safe environment:** Employees who are not at risk. Instead of a data breach or infection, they are redirected to a landing page with information about what to look for in a real phishing email and then onto a training module to help increase their cyber security awareness.
- **Reporting and feedback:** The test tracks which employees failed the test, allowing Protec to provide targeted additional online training. Protec also tracks how many employees correctly report the email.

Purpose and benefits

- **Assess training effectiveness:** Phishing tests provide concrete data on how well security awareness training is working. We provide routine updates to the organisation to track the ROI effectiveness.
- **Improve employee awareness:** The tests act as a real-time learning opportunity, reinforcing the importance of vigilance against phishing attempts.
- **Identify vulnerable employees:** Results can highlight specific individuals or departments that may need more training.
- **Mitigate risk:** By making employees more aware, companies can reduce the likelihood of a successful attack that could lead to data breaches, financial loss, or other damages.
- **Demonstrate compliance:** Regular phishing tests can help an organisation demonstrate its commitment to security to auditors and insurance providers.

Mobile Device Management (MDM)

Our MDM solutions allows organisations to remotely manage and secure mobile devices like smartphones, tablets, and laptops. It enables IT departments to enforce security policies, monitor device compliance, and protect corporate data by controlling the devices that connect to the company network.

Key functions of MDM:

- **Security enforcement:** MDM allows for the remote enforcement of security policies, such as strong passwords, encryption, and the ability to remotely track, lock or wipe a device if it is lost or stolen.
- **Policy management:** It can standardise device configurations and ensure devices and applications are up to date with security patches.
- **Application management:** Our MDM solutions can push out and manage applications for employees, which can be useful for both corporate-owned and personal devices under a Bring Your Own Device (BYOD) policy.
- **Monitoring and compliance:** IT administrators can monitor devices for compliance with organisational rules, and check for things like outdated software or unauthorised apps.
- **Remote configuration:** MDM allows administrators to send configurations and profiles to devices wirelessly to set up email, Wi-Fi, and other settings.

Purpose and benefits

- **Enhanced security:** By managing and securing mobile devices, MDM helps protect corporate networks from potential threats and data breaches.
- **Increased productivity:** It enables employees to work from their mobile devices securely, which increases productivity and flexibility, especially with BYOD policies.
- **Simplified IT administration:** MDM provides a centralised way to manage devices, reducing the burden on IT staff and helping to scale device management with business growth.
- **Data protection:** It helps secure sensitive corporate data by enforcing policies and allowing for remote data sanitation if a device is compromised or lost.

PROTEC

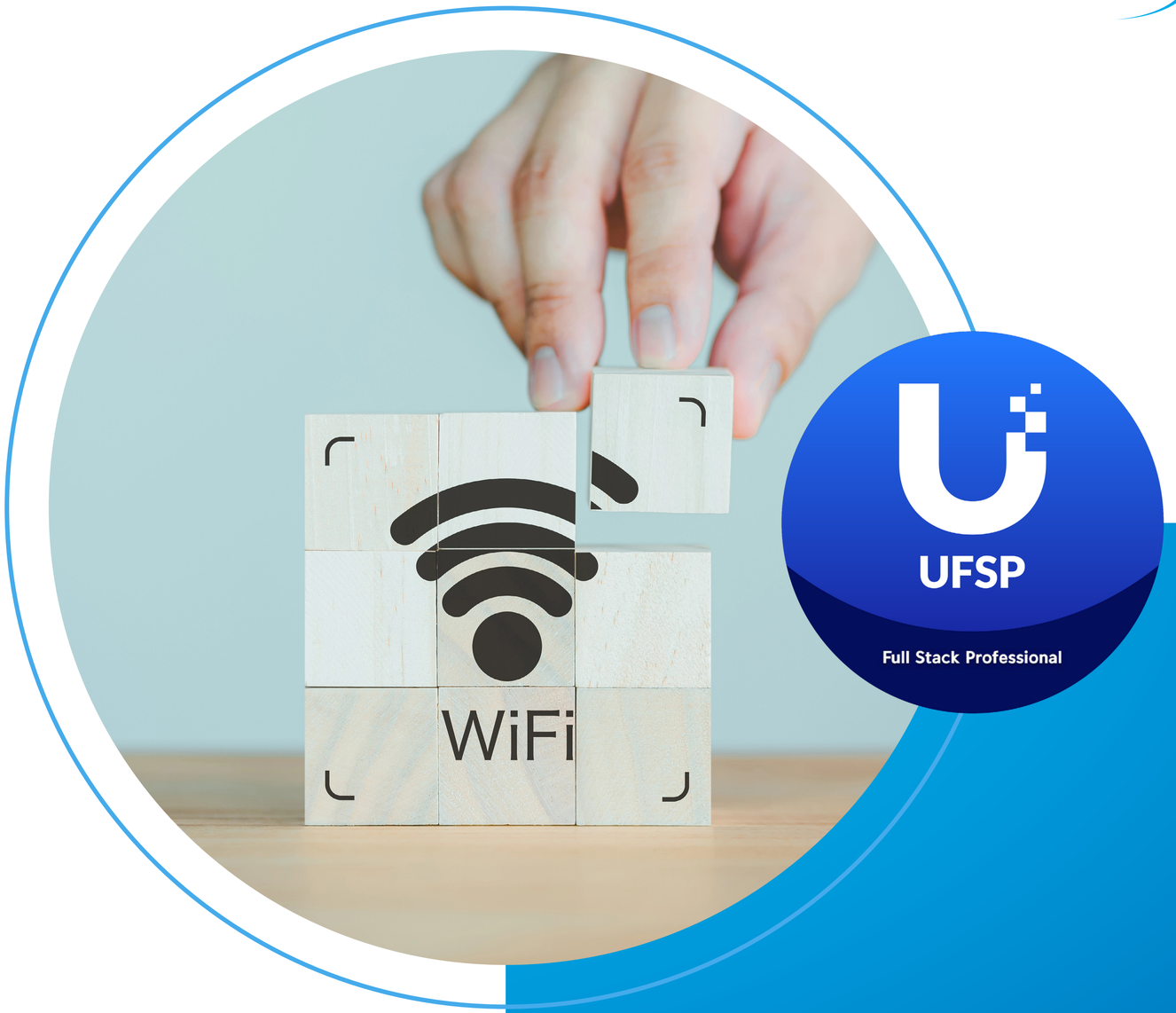
WiFi Security

Securing your wireless network is essential to protecting your data, your devices, and your business. Our WiFi security services are designed to provide strong, reliable protection without complicating your network experience. By implementing features such as VLANs to segment sensitive systems and dedicated guest networks to keep visitors safely isolated from internal resources, we create a secure, efficient, and well-organised wireless environment. Whether you're enhancing an existing setup or building a secure network from the ground up, our solutions ensure your WiFi remains fast, safe, and fully optimised.

Protec is proud to carry the Ubiquiti Full Stack Professional and Ubiquiti Wireless Admin certifications.

WiFi Network management:

- **Create a guest network:** Use a guest network for visitors. This keeps their devices separate from your trusted devices and sensitive company data.
- **Separate IoT devices:** Set up your smart devices (like speakers, lights, etc.) on a separate network, such as the guest network, to isolate them from your main network and devices with sensitive information.
- **Firmware and security patching:** Protec can monitor and manage and maintain your WiFi infrastructure. Ensuring access points and switches are optimised and running securely to ensure uptime and performance.



[See our full list of Ubiquiti services]

Penetration Testing

Our penetration testing is a simulated cyberattack, also called ethical hacking, that identifies vulnerabilities in computer systems. Our tools and techniques allow us to find and exploitable weaknesses. The goal is to provide a comprehensive security risk assessment and actionable recommendations to fix the vulnerabilities before they are exploited by real threats.

Key aspects of penetration testing:

- **Simulated attacks:** It involves a planned an authorised simulation of real-world attacks to test an organisation's security defences.
- **Proactive security:** It is a proactive approach to cybersecurity that helps organisations strengthen their security posture and reduce risk by finding and fixing vulnerabilities.
- **Comprehensive scope:** A test can be broad or specific, focusing on areas like networks, web applications, wireless systems, and even employees' susceptibility to social engineering.

Purpose and benefits

- Identifies exploitable vulnerabilities in systems, applications, and networks.
- Tests the effectiveness of existing security controls.
- Helps organisations comply with various industry standards and regulations.
- Can provide valuable insights for improving overall security resilience.

PROTEC

Get in touch: 01344 876 123 | hello@ProtecIT.co.uk