SoConnect

Cyber Security

Standard and **Advanced** bundles

Required licenses and certificates

SoConnect's Cyber Security bundles are underpinned with the licenses and certificates that give your business the best of the secure modern workplace.

All bundles

Microsoft 365 Premium Secure

Sold Separately

What is Microsoft 365 Secure?
Developed specifically for small and medium businesses, Microsoft 365 Secure delivers extra value by combining productivity, security and backup solutions that work seamlessly together. The Secure package includes: Microsoft 365 Premium, Vade email security and Acronis backup.

How does it help a company's cyber security posture?
Microsoft 365 Secure has all the benefits of the cloud - accessible anywhere, collaborative, flexible, scalable, secure and always up to date.

- **Microsoft 365:** All the 365 productivity apps such as outlook, OneDrive and Teams with added security.
- **Vade:** An email filter that defends against advanced spear-phishing, malware and ransomware attacks with global threat intelligence to predict zero-day threats.
- **Acronis:** Unlimited backup storage with agentless, cloud to cloud daily backups. All data is fully encrypted in transit and at rest, with point-in-time restoration.

Microsoft 365 applications provide best-in-class business productivity and collaboration, while providing an **extra layer** of email security and data backup capabilities.

We believe that all business should aim for Cyber Essentials accreditation and compliance. Developed by the National Cyber Security Centre, the scheme outlines the basic levels of security that all businesses should comply with.

All bundles

Cyber Essentials/Essentials Plus

What is Cyber Essentials?
Cyber Essentials is a government-backed scheme developed by the National Cyber Security Centre (NCSC). Ensuring you have the basic cyber-security measures helps prevent over 99.3% of common cyber attacks.

How does it help a company's cyber security posture?
Just five controls are needed to secure most vulnerabilities,:

- Firewalls and gateways
- Access Controls
- System updates
- Secure configs
- Malware Protections

Certification is available to businesses of all sizes across the UK. Once achieved, a business will demonstrate that they take cyber security seriously. They'll also gain a competitive advantage, opening up new revenue opportunities. Cyber Essentials Plus* requires the same five security controls but differs in one crucial aspect. The 'Plus' credential includes an independent assessment carried out by a licensed auditor.

Achieving Cyber Essentials certification shows you are **committed to protecting your data.** Not only that, it indicates you take securing your customers' and clients' data seriously too. The certification increases your business reputation and shows you take preventative actions to reduce the threat of cyber-attacks.

Cyber Security Bundles Comparison

Our cyber security bundles are designed to ensure ongoing compliance to the Cyber Essentials scheme, while providing extra security measures to protect your business from common, enhanced and advanced cyber threats.

Cyber Security Standard

- Endpoint Detection & Response
- Cyber Compliance Monitoring
- Password Manager
- Privileged Access Management
- User Security Awareness Training
- DNS Filtering
- SoConnect Cyber Security Support
- ---
- ---

from 20.5* per user/ per month

Cyber Security Advanced

- Endpoint Detection & Response + SOC
- Cyber Compliance Monitoring
- Password Manager
- Privileged Access Management
- User Security Awareness Training
- DNS Filtering
- Managed SIEM with SOC
- Managed Office 365 Security with SOC
- SoConnect Cyber Security Support

from £55* per user/ per month

The **Cyber Security Standard bundle** gives businesses enhanced protection against cybercrime. It offers everything required included in the Basic bundle, plus simplified user privilege management, security awareness training and web filtering. Cyber Security Standard gives businesses everything they need to be confident in their security posture against common cyber threats.

The **Cyber Security Advanced bundle** gives enterprises our full level of protection against cyber attacks. It offers everything required in the Standard bundle but adds SIEM (Security Information and Event Management) technology, advanced threat detection, 24/7 monitoring and access to an outsourced, highly qualified team of security analysts. Cyber Security Advanced gives businesses everything they need to be confident in their security posture against common and advanced cyber threats.

*Please note that some products are priced per device rather than per user. If you have more devices than users, additional charges will apply.

What is the Cyber Security standard bundle?

The Cyber Security Standard bundle gives you enhanced protection against cybercrime. It offers simplified user privilege management, security awareness training and web filtering. Cyber Security Standard giving you everything you need to be confident in their security posture against common cyber threats.

What's included?

The Cyber Security Standard bundle includes products and service that help to maintain ongoing protection from a whole host of cyber attacks.

These include:

- Endpoint Detection and Response
- Endpoint Compliance Monitoring
- Password Manager
- Privileged Access Management
- Cyber Security Awareness Training
- DNS Filtering

An overview of these services with how they help strengthen your cyber security posture will be detailed in this document. Read on and you'll know everything you need to know!

Scenario

The issue: An employee receives an email saying their Microsoft password has expired. So as not to lose access, the employee clicks the email link and updates the password. Now a hacker has access to your company data.

The solution: While Cyber Essentials compliance ensures you have rectified system and network vulnerabilities, it can't protect you from human error. That's where awareness training comes in. The solution will ensure your staff know all the tell-tale signs of a phishing attack with regular simulations and training videos.

Why should I consider the Cyber Security Standard bundle?

The Cyber Security standard bundle will significantly reduce the chance of falling victim to cybercrime. Network and systems have best practice security, and staff will be trained to avoid insider vulnerabilities like phishing and be prevented from accessing toxic websites. The standard bundle will also increase your business reputation by showing that you take preventative actions to reduce the threat of cyber-attacks.

Key features

- Complete malware protection
- Cyber Essentials Compliance
- User Privilege Controls
- Web Filtering
- Automated security awareness training
- Secure Password management
- Multi-factor Authentication

What is endpoint detection and response?

Endpoint provides best-of-breed security and includes security suite features for endpoint management. Control protects against known and unknown malware, Trojans, hacking tools, ransomware, memory exploits, script misuse, bad macros, and more.

How does it work?

Our EDR solution uses a patented Behavioural AI feature to recognize malicious actions and patterns. Threat detection is applied to detect file-less, zero-day, and nation-grade attacks. The integration of AI ensures threats are discovered in in a timely manner which reduces the effects of ransomware and phishing attacks.
Using EDR, SoConnect will monitor for infections at any endpoint on the console and work to determine if it's a false positive or an actual attack. Most of the time, EDR will automatically identify an attack, quarantining the process to block the attack. If it can't make that determination, SoConnect will further investigate the suspicious traffic.

How does it help your cyber security posture?

Our EDR solution gives you actionable threat detection without the noise. The ability to rapidly uncover and contain advanced threats means more time for SoConnect to understand the root cause and close existing gaps.

- **Incident Triaging Flow:** Security teams are commonly overwhelmed with alerts, a large percentage of which are false positives. EDR automatically triages potentially suspicious or malicious events, enabling security analysts to prioritize their investigations.
- **Threat Hunting:** Not all security incidents are blocked or detected by an organization's security solutions. Threat hunting activities enable security analysts to search for potential intrusion proactively.
- **Integrated Response:** With an intuitive interface, analysts can take immediate action to remediate security incidents with multiple response options, such as eradicating vs. quarantining a particular infection.

What is a password manager?

Our Password Manager, Keeper, allows your users to store online login credentials, documents and images, and other sensitive information in an encrypted digital web vault. Users can also store two-factor authentication codes safely for extra easy security.

How does it work?

Save employees time, frustration and eliminate the need for them to reuse and remember passwords. Keeper will generate strong, random passwords and automatically fill them for users. The Keeper vault, with a responsive and intuitive user interface (UI), is available to employees from any device and location. Everything Keeper does is geared towards quick user adoption and security.

Our Password manager includes:

- An encrypted vault for every user, with folder and sub-folder functionality
- The ability to created shared team folders
- Allows access from unlimited devices
- A strong policy engine with enforcement
- Built-in, continuous security audit
- Advanced activity reporting and an alerts module
- Two-Factor Authentication (SMS, TOTP, smartwatch, DUO, RSA and FIDO U2F)
- Single Sign-On (SAML 2.0) authentication
- Active Directory and LDAP sync
- SCIM and Azure AD provisioning
- Email auto-provisioning and ability for command-line provisioning

How does it help your cyber security posture?

Employees choose simple passwords that are easy to guess, they use the same password for every online account, or they write those passwords on sticky notes stuck to the side of their monitor. Such methods may seem like an easy way to avoid the work of creating and using secure passwords, but they make it easy for cybercriminals to do their damage. People need a far more secure and convenient way to protect their online accounts and other online assets.

Save employees time, frustration and eliminate the need for them to reuse and remember passwords. Keeper will generate strong, random passwords and automatically fill them for users. The Keeper vault, with a responsive and intuitive user interface (UI), is available to employees from any device and location. Everything Keeper does is geared towards quick user adoption and security.

What is privileged access management?

Privileged Access Management or PAM is a solution that solves many of the problems that stem from removing local admin rights – without frustrating the customer or creating more work for tech support. Privileged Access Management (PAM) is an information security (infosec) mechanism that safeguards identities with special access or capabilities beyond regular users. Like all other infosec solutions, PAM works through a combination of people, processes and technology.

How does it work?

PAM automates Windows UAC prompts. The software Agent service works in the background to apply proactive elevation rules to each UAC event or to notify a technician through one a PSA ticketing integration, Windows notifications, or via an AutoElevate Mobile App (or all 3). Technicians can quickly and easily evaluate the request and build rules to either accept or deny the requested installer, application, update, or system action which can be allowed just one time, for just this single computer, for a group of computers, a whole client, or for all of the computers under your management.

How does it help your cyber security posture?

Removing admin rights and monitoring requests for elevated privileges protects your systems, data, and users from many serious security threats, including:

- **Ransomware, spyware, and malware:** Many malware strains require tricking the user into running untrusted software, entering admin credentials, or approving a UAC request. AutoElevate gives your team the power to review all requests for elevation alongside detailed security information, preventing infections before they happen.
- **Unwanted or illegal software**: AutoElevate can keep your users focused on work by preventing the installation of non-work-related programs such as games and media applications. And you'll find out if anyone tries to install pirated software – before it turns into a security risk or legal liability.
- **Shadow IT:** Unapproved or insecure cloud collaboration apps present a major risk of data loss, whether accidental or intentional. Find out about the use of these apps before they develop into a problem for your organization.

What is uSecure Awareness Training?

uSecure is an automated Security Awareness platform. It reduces user-related security incidents caused by human error and drives resilience to phishing attacks through personalised staff training programmes.

How does it work?

Human Risk Management (HRM) is the new class of user-focused security that enables you to do just that through personalised security awareness training programs, periodic phishing simulation campaigns, simplified policy management and ongoing dark web monitoring - completely managed for you.

Awareness Training: Assess each user's security knowledge gaps and automate regular training courses that tackle their unique risk areas.
Dark Web Monitoring: Detect when stolen user credentials are found on the dark web that could be used to launch an attack.
Simulated Phishing: Automate periodic phishing simulations that assess your employees' ongoing risk to a range of attack techniques
Policy Management: Keep users well-versed on security processes with easy policy management and trackable eSignatures

How does it help your cyber security posture?

Over 90% of data breaches are caused by human error and over 36% of those are due to a phishing attack. There is no simple software you can install which can prevent human error. That's why training your staff is critical to cyber security.

- Drive user resilience to sophisticated phishing attacks.
- Reduce user-related security incidents caused by human error.
- Demonstrate compliance with key standards like ISO 27001 and GDPR.
- Understand your business's employee security posture with a human risk score.
- Dig deep into ongoing human risk with training, phishing and policy reporting.
- Save time with readily-made courses, phishing campaigns and policy templates.
- Simple setup, fast deployment and automated staff training reminders.

What is DNS Filtering?

DNS filtering is the practice of blocking access to certain sites for a specific purpose, often content-based filtering. If a site, or category of sites, has been deemed a threat, then its IP address is blocked with a DNS filter and access to it is prevented. Examples of sites that may be blocked include adult, gambling, productivity sinks, or those known to pose a significant malware risk.
DNS filtering is essential for businesses because it can severely limit the amount of threats a network is exposed to, helping to reduce significantly reduce the remediation workload for MSPs and IT pros. In fact, effective DNS filtering can stop up to 88 percent of internet-borne malware before it even reaches the network.

How does it work?

When an end user attempts to access a particular URL that does not violate an organization's acceptable Internet use policy, the request is honoured. Since there is no latency, the speed at which the website is loaded is the same as if no filtering mechanism is in place.
Unknown to the user, when an attempt is made to access a webpage, the DNS request is sent to our DNS Filtering solution which determines whether the request should be allowed or denied. If the user attempts to access a gambling website and the gambling category has been blocked, the user will be advised that their request has been denied and access to the site will be prevented.

How does it help your cyber security posture?

Many businesses choose to implement a web filtering solution to prevent employees from accessing inappropriate web content such as pornography or to stop work computers from being used to download illegal content such as pirated films, music, and TV shows. Web filtering also helps block malicious malware and phishing websites.

There are ten main web-based threats that DNS Filtering protects against:

- Malware distribution points
- Ad fraud
- Botnets
- Spyware and questionable software
- Phishing and other fraudulent sites
- Command and Control (C2) servers
- Malware call-home addresses
- Compromised sites and links to malware
- Spam URLs
- Cryptocurrency mining

What is the Cyber Security advanced bundle?

The Cyber Security Advanced bundle gives enterprises our full level of protection against cyber attacks. It offers everything required in the Standard bundle but adds SIEM (Security Information and Event Management) technology, advanced threat detection, 24/7 monitoring and access to an outsourced, highly qualified team of security analysts. Cyber Security Advanced gives businesses everything they need to be confident in their security posture against common and advanced cyber threats.

What's included?

The Cyber Security Advanced bundle includes products and services that help to maintain ongoing protection from a whole host of cyber attacks, while providing greater detection and response for advanced threats

These include, everything in the standard bundle, plus:

- Endpoint Detection and Response with SOC
- SIEM technology with SOC
- Office 365 Monitoring plus SOC

An overview of these services with how they help strengthen your cyber security posture will be detailed in this document. Read on and you'll know everything you need to!

Scenario

The issue: Unbeknown to you, a hacker has accessed your Office 365 account. For weeks they monitor your mailbox in preparation for a social engineering attack. The hacker has all of the information needed to succeed.

The solution: With 24/7/365 monitoring, a team of SOC experts will watch your Microsoft environment to detect unusual user activity, correlate events and alert you of real threats. That means the hacker accessing your Office 365 could not gather information undetected, and we would take steps to remove the unsolicited access immediately.

Why should I consider the Advanced bundle?

The Cyber Security Advanced bundle offers best possible cyber security protection. Network and systems have best practice security, and staff are trained to avoid insider vulnerabilities like phishing and are prevented from accessing toxic websites. The advanced bundle adds an extra layer of defence to catch the threats that would be otherwise undetected. It gives our security experts complete visibility and multi-source data analytics to detect events even when prevention fails.

Key features

- Automated security training.
- Secure Password management
- Multi-factor Authentication
- Threat detection, compliance and security incident management
- Complete malware protection.
- Cyber Essentials Compliance
- User Privilege Controls
- Web Filtering
- SIEM technology

What is Managed Endpoint protection and response (EDR) with SOC?

This solution consolidates vital security functions. Designed for businesses looking for enterprise-grade prevention, detection, response and threat hunting across endpoint and in the cloud. Managed EDR with SOC is made for companies that need modern protection and control plus advanced endpoint detection and response (EDR) features. This solution provides **SOC (Security Operation Centre)** analysts with the information needed to make assessments and respond quickly to developing threats.

How does it work?

Managed EDR with SOC uses technology that automatically contextualizes all Operating System process relationships [even across reboots] every second of every day and stores them for future investigations. This saves analysts from tedious event correlation tasks and gets them to the root cause fast. It is designed to lighten the load on security administrators, SOC analysts, threat hunters, and incident responders by automatically correlating information and mapping it into a framework.

How does it help your cyber security posture?

Managed EDR with SOC is our most advanced anti-virus and endpoint detection and response solution. The ability to rapidly uncover and contain advanced threats means more time for SoConnect to understand the root cause and close existing gaps.

- **Incident Triaging Flow:** Security teams are commonly overwhelmed with alerts, a large percentage of which are false positives. EDR automatically triages potentially suspicious or malicious events, enabling security analysts to prioritize their investigations.
- **Threat Hunting:** Not all security incidents are blocked or detected by an organization's security solutions. Threat hunting activities enable security analysts to search for potential intrusion proactively.
- **Integrated Response:** With an intuitive interface, analysts can take immediate action to remediate security incidents with multiple response options, such as eradicating vs. quarantining a particular infection.
- **Next generation anti-virus** and behavioural AI to stop known and unknown threats.
- Features include network control, USB device control, and Bluetooth device control.

SIEM explained

The Cyber Security Advanced bundle includes SIEM technology. SIEM stands for Security Information and Event Management and it gives businesses extensive protection across their entire IT infrastructure. Learn more about SIEM below.

Why SIEM?

In the past, perimeter security solutions were enough to keep the good guys in and the bad guys out of a business's network. The tools identified and blocked malicious code from infiltrating corporate networks, servers, workstations, applications, logins, and databases. Perimeter security tools like firewalls, Virtual Private Networks (VPNs), antivirus, and intrusion prevention systems served as a brick wall protecting the corporate network. While the wall may have had weak spots, continuous monitoring tools provided the stopgap, keeping organizations one step ahead of security breaches and in compliance. However, the enterprise landscape looks completely different today. Applications, users, and devices are moving outside the corporate network, and this shift is dissolving what was once the trusted enterprise perimeter. Maintaining regulatory compliance is also becoming more complex, requiring an organization's full-time attention. Security architecture evolved.

What can businesses do to protect themselves in today's cloud-based, mobile era?

The first step is setting up enterprise protections that extend beyond the firewall where applications, data, devices, and remote users are. The next step is putting tools and processes in place to manage the flood of information about security information and events generated across the enterprise: Enter SIEM. SIEM or Security Information and Event Management technologies offer organizations a holistic, 360-degree view of their technical infrastructure, looking at an extensive collection of security events or 'logs.' SIEM tools create reports about applications and activities and use event correlation and alerting to help analyze and remediate security events. SIEM platforms can also help to simplify IT tools, management, and compliance requirements.

What is SoConnect's SIEM solution?

Our SIEM solution is a co-managed threat detection and response platform backed by an in-house Security Operations Center (SOC). It is flexible, scalable to any size business and tailored to fit a business' specific needs. SIEM gives us a 360 degree view of your IT infrastructure at all times so that new and evolving threats can be caught earlier and remediated.

How does it work?

The solution uses security information and event management (SIEM) technology. SIEM technology supports threat detection, compliance and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources.

How does it help your cyber security posture?

- **Faster, more efficient SecOps.** With Perch sifting through millions of data points, Security Operations Centre analysts can quickly get a handle on what's happening. This saves valuable time in responding to a security threat and reduces the impact of a cyberattack. Perch can help us respond to incidents in real-time, potentially saving your company from data loss or worse.
- **Accurate Threat Detection and Security Alerting.** SIEM tools can leverage their extensive data sets to detect and identify threats more accurately than possible using individual security data streams.
- **Improved Security Data**. SIEMs aggregate security data, improving the potential for it to be analysed and used in incident response workflows. This can also result in better visibility over the entire security landscape in the enterprise.
- **Better Network Visibility**. SIEM log management and aggregation make it easier to get an overview of the network. Hackers look for dark spaces on networks. It gives them a place to hide persistent threats and move laterally across digital assets without being detected. SIEM mitigates this risk by collecting security event data from everywhere in the network.
- **Improved Compliance.** Regulations and compliance frameworks s invariably require logging of security data as a key control. SIEMs fulfil this role, easing the attestation process with pre-set compliance reporting templates that streamline the compliance process.

What is Office 365/Azure Security Monitoring?

This solution is a fully managed security monitoring and investigation of security incidents for Microsoft's SaaS services such as Microsoft 365, Azure AD, and OneDrive. Using this technology means we can lock down your business' cloud data to keep you secure should the worst happen. A fully staffed SOC team will constantly watch any network anomalies and unusual user behaviour morning, noon, or night.

How does it work?

With 24/7/365 monitoring, a team of SOC experts keep a watchful eye on the Microsoft environment to detect unusual user activity, correlate events and alert SoConnect on real threats. When an active threat is discovered, the SOC team will guide us on how to effectively respond to each threat to minimise damages.

How does it help your cyber security posture?

- **Earlier detection of threats.** With 24/7 monitoring analysts can quickly get a handle on what's happening. This saves valuable time in responding to a security threat and reduces the impact of a cyberattack. Fortify SaaS can help us respond to incidents in real-time, potentially saving your company from data loss or worse.

- **Simplified reporting and alerting**. An intuitive web UI lets us run reports, view status, search logs, export data, meet compliance log retention requirements, and investigate past and present incidents. Decision-maker friendly reports will also help our team understand the need for increased threat detection and remediation.

- We can detects threats that slip past traditional defences and offer **deeper insight into alerts generated by defences**. Office 365/Azure Security Monitoring combines the power of native Microsoft cloud monitoring with the security expertise of the SOC team to analyse threats real-time.

Adopting new technologies can sometimes be a little overwhelming, and it's often difficult to know where to begin. At SoConnect, we have a team of experts ready to talk you through every stage of building your cyber security protections. Our solutions are tailored to your needs to ensure your business goals are always met.

To start your journey, book an initial consultation with our expert team. During the consultation, we will carry out a gap analysis to establish a suggested roadmap and adoption plan, ensuring you transform your company into a successful and secure modern workplace.

About Us

SoConnect takes the stress away from IT with a comprehensive service built around your business requirements. We're here to make your life easier, keeping your IT system optimised and taken care of so you can focus on your day-to-day operations. We are IT, cloud and security experts that help businesses adopt and benefit from cutting-edge Modern Workplace technologies.

Our Services

- **Modern Workplace**
- **IT Managed Services**
- **Cyber Security**
- **Cyber Essentials Certification**
- **Cloud Solutions**
- **Business Connectivity**
- **Voice Solutions**

Certificate No:263722021