Security Foundry

Your **trusted** cyber security partners

Security Foundry

Contents

Security Foundry

Your **trusted** cyber security partners

CYBER SECURITY MANAGED SERVICES

Security Foundry provides **trusted** cyber security solutions and managed services delivered from secure UK datacentres with purpose-built security operating centres (SOC's) which have services tailored to your environment to address the threat from malicious activities designed to impact your business profitability and integrity.

At the same time these expert services deliver compliance services for regulatory standards in data protection. These are delivered by specialist experienced consultants as a managed service.

Security Foundry's Cyber Security Managed Service utilises next generation solutions which have machine-based learning or AI at their centre, allowing automated and pro-active threat identification.

In addition to the deployment of the latest cyber security technology, Security Foundry completes the 360-degree service by providing professional consultancy services that address all the obligations required by government and industry regulators such as GDPR to protect personal and business data.

Security Foundry with its strategic partners have created services that are integrated to provide businesses with a cyber 'immune system' designed to ensure compliance and protection.

Our Cyber Security Managed Service includes Security Information and Event Management (SIEM) delivered by specialist security consultants.

This offers complete and comprehensive threat detection for all your data and every component in your IT estate whether they are;

✓ Mobile ✓ Cloud ✓ Hybrid

The service always starts with an ***Initial Consultation*** so that customers can understand their current level of protection and compliance as well as the likely threat level to the business with recommendations for what is required to achieve the appropriate standard and industry best practice.

The **Cyber Security Managed Service** includes the deployment of IBM Security QRadar and other security software best in class tools. The combination of these offer an 'immune system' for your business.

For those customers looking for specific cyber solutions for individual use cases within their business, Security Foundry are authorised technology partners for ObserveIT for Insider Threat Management and Meta Networks for software defined perimeter and remote access management, (now both part of Proofpoint), Okta for Identity Management and Yubico for two-factor and multi-factor authentication needs.

VULNERABILITY SCANNING SERVICE

Our Managed Vulnerability Scanning Service provides customers with both cloud and on-premise coverage. Eliminate blind spots with the industry's most comprehensive visibility into traditional and modern assets, such as cloud, mobile devices, containers and web applications.

Live Discovery

Dynamically discover every modern asset across any digital computing environment (even the ones you aren't aware of) and as the elastic attack surface expands and contracts, you can keep pace with a live view of your assets.

Continuous Visibility

Automatically analyse each asset to identify its exposure and security posture - enabling you to identify and address issues before an attacker does - think of us as your "Google Maps" for live Cyber Exposure.

Focus and Prioritise

We can add context to the asset's exposure to prioritise remediation based on the business criticality and severity. We also provide architectural advice for incorporating compensating security controls particularly within legacy environments where testing and applying patches could be challenging.

For example:

- The asset's business use and value
- The asset's connectivity – and who is authorised to access it
- Whether the vulnerability is currently being exploited

Strategic Insight

Translate raw security data into a common language for accurate representing and communicating cyber risk to the business – in business terms.
Creating a metrics-driven program where Cyber Exposure is quantified and measured alongside every other business exposure.

Security Foundry

SECURITY OPERATIONS SERVICE

Cyber attackers are becoming increasingly more sophisticated and are continuing to challenge security teams. For most organisations who aspire to have security monitoring and incident response services but may not have the resource and budgets, our Managed SOC service significantly reduces the organisational overhead.

Our Service provides the following features:

- Security Architecture guidance for integration
- Proactive monitoring and detection on unusual/suspicious network traffic
- Initial triage and analysis
- Vulnerability Management as a service integration – to provide further context and focus on business-critical services
- Security Change Management integration – align and integrate with any existing ITIL Change Management processes – to help further identify and detect abnormal behaviour/changes from expected behaviour/changes
- SIEM as a Service integration – to correlate events against unusual or suspicious behaviour and Indicators of Compromise (IOC's)
- Incident Management Service integration – managing and supporting security incidents through to resolution
- Security metrics and executive reporting
- Access to our Cyber Response support platform
- Threat hunting – integration with our Endpoint Security Service to further utilise our Remote Live Forensics capabilities to hunt for suspicious behaviour and further analyse files within our sandbox environment.

Our Service provides 3 key elements:

- Log Collection
- Log Aggregation/Correlation
- Log Archiving

These services ensure that business critical systems are monitored and unusual patterns of behaviour are identified and correctly followed up. Beyond any compliance requirements that your organisation may have, we also continuously look back over historical past events and further look for other signals or indicators that could lead to a potential security incident.

Our service provides context for a detected event:
What happened? • Who was involved? • Where did the event happen?
When did the event happen? • Why? Was this a scheduled change?
Or an unauthorised change?

INCIDENT MANAGEMENT SERVICE

Our Incident response capability includes four main phases:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-Incident Activity

Our Incident Management Service aligns with both ISO 27035 and NIST SP 800-61 and aims to integrate with your existing Information Technology Infrastructure Library (ITIL) services.

Our Incident Management Service also integrates and compliments our other services such as Managed Endpoint Device Service and Managed Security Operations – enabling us to detect, protect and respond.

Key tasks:

- **Develop and operate Incident response policies and plans**
- **Agreeing, identifying and exercising procedures for performing incident handling and reporting (including stakeholder communication guides for third party and external engagement)**
- **Root Cause Analysis (RCA) / Post-Incident Activity**
- **Perform Red/Blue team activities to test readiness and the effectiveness of procedures.**

We manage the problem throughout its life cycle through to recovery and post-incident analysis.

ENDPOINT SECURITY SERVICE

Our Endpoint Security Service provides a fully managed Endpoint protection for Apple MacOS, Microsoft Windows and Linux Systems by using an Artificial-Intelligence based protection to provide a quantum leap over traditional malicious software signatures, heuristics, or behavioural methods by taking advantage of sophisticated math models to identify malicious software.

Instead of reactive signatures, threats are blocked automatically in real-time.

What is included?

The service offers ongoing support and management, deployment aid and configuration support. We provide Security Architecture recommendations while being pragmatic to any legacy systems that you may have.

We also include entry level access to our Cyber Network Defence (CND) Team for Threat and Malicious software (Malware) Analysis, Trending and Intelligence – the CND will provide Remote Live Forensics for entry level hunting – this can be extended to our full Managed Security Operations Service which includes our Full Digital Forensics and Incident Response services, and our Advanced Suspicious Behaviour Engine.

This service is available to organisations with 50 compatible devices or more.

Following the initial configuration, the system will be monitored with recommended changes suggested by our technical team as necessary. Features of this service include:

- Market leading Anti-Malware technology by Cylance
- Deployment guidance including detailed prerequisites
- Policy to ensure the optimal security settings are deployed across the covered devices
- Advice and guidance on effectiveness of implemented security
- Change recommendations and alerts on new features and agent updates
- Active threat monitoring and alerting
- Monthly health check and service report
- Unlimited whitelisting changes
- Remotely monitored and managed
- 10 policy change requests per month
- Security Architecture reviews and guidance of your environment
- Our Cyber Network Defence (CND) Team with our Remote Live Forensics capability will provide entry level proactive Threat Hunting by searching for Indicators of Compromise (IOCs)

Security Foundry

WEBSITE SECURITY SERVICE

For many organisations their website is their brand and reputation, and they rely on their Internet presence to help them communicate with others. Unfortunately, criminals are focusing more on the Internet as a major channel for Cybercrime through means such as extortion, using your system as a mule to attack others, or to serve malicious/ inappropriate content to aid in masking their identity.

Our Web Security Service consists of several key focus areas, which include:

1. Exposure

Helping prevent harmful attacks from impacting you:

Distributed Denial of Service (DDoS) mitigation.

Content Acceleration through a Content Delivery Network (CDN) – accelerating the performance of the content served from your website by caching content in over 150 data centres globally – making your website load faster.

Domain Name System (DNS) plays a vital part in nearly all Internet communications and is often overlooked – we can help secure your DNS using DNSSEC, to help ensure your customers are not sent somewhere else.

We provide resilient and robust Anycast DNS hosting ensuring you're online and working.

Website application firewall management and Virtual Patching – in combination with our Cyber Network Defence (CND) team and integration with your change management processes – preventing unauthorised changes and preventing attacks from reaching your system.

System hardening reviews with exposure limitation – e.g. website administrative sections for updates.

Internet facing vulnerability scans – to discover potential application and server weaknesses.

Internet facing weekly malicious code scans.

2. Detection

We offer a Remote Live Forensics capability from our Cyber Network Defence (CND) Team to monitor your Internet facing servers for unusual behaviour.

•Configuration Management & File integrity monitoring

•Website Application – the systems that run your environment:

•End-to-End Security Architecture reviews including the supply chain from developer to production system.

•Detect and Report-on unauthorised changes – linking in with any service management system that you may have – enabling the identification of a potential insider threat

•Website systems – that may exchange information with your website and/or data systems

•Malicious software scanning - we utilise a number of highly sophisticated mechanisms of spotting suspicious behaviour occurring from your website

Artificial-Intelligence analysis of website activity

Ability to proactively block or redirect known 'Threat Actors'

Zero-Day proactive detection

Website Application Code

Security Foundry

WEBSITE SECURITY SERVICE

Our service also includes:

- Daily and/or Weekly website and Internet facing system security scans – to discover potential weaknesses and malicious code.
- Detect and report on unauthorised changes – linking in with any service management system that you may have.
- Patching and overall hardening recommendation.
- Security Architecture reviews with exposure limitation/remediation.
- Website supply chain – code to website security process review.
- Website application code security review – identifying weaknesses or defects within the website code or website logic.
- Establishment of a Secure SDLC (Software Development Lifecycle) including static code analysis etc.
- Guidance on Multifactor authentication implementation and exposure limitation.
- Web Application Firewall implementation with processes around testing and change management.
- Guidance on often overlooked security controls specifically in DNS (DNSSEC, SPF, DKIM etc), including information disclosure.
- HTTP/S header hardening.

EMAIL SECURITY SERVICE

Email is still a significant attack mechanism for Cyber Criminals – many organisations are moving to Microsoft's Office 365 or Google's G Suite –and while these do help, they need to be configured and monitored correctly.

Our Managed Email Security Service provides an additional award-winning multi-layered security addressing malicious messages, phishing and spear phishing attacks.
We incorporate advanced behavioural analytics and artificial intelligence mechanisms to learn how people compose emails and further identify those which are abnormal.

The service includes Data Loss Prevention (DLP) filtering which can help in preventing information from being sent to the wrong individual or organisation. We can match based on patterns such as Credit Card Numbers and other forms of Personally Identifiable Information (PII).

Enforced or opportunistic encryption for secure communications can be defined by policy. We can also provide an end-to-end assessment over your email environment to ensure that no legacy or misconfigured services are in place which could be abused.

Managed Email Archiving

Your data is critical to your business, so your message archiving solution should be backed up by people who take your data security as seriously as you do.

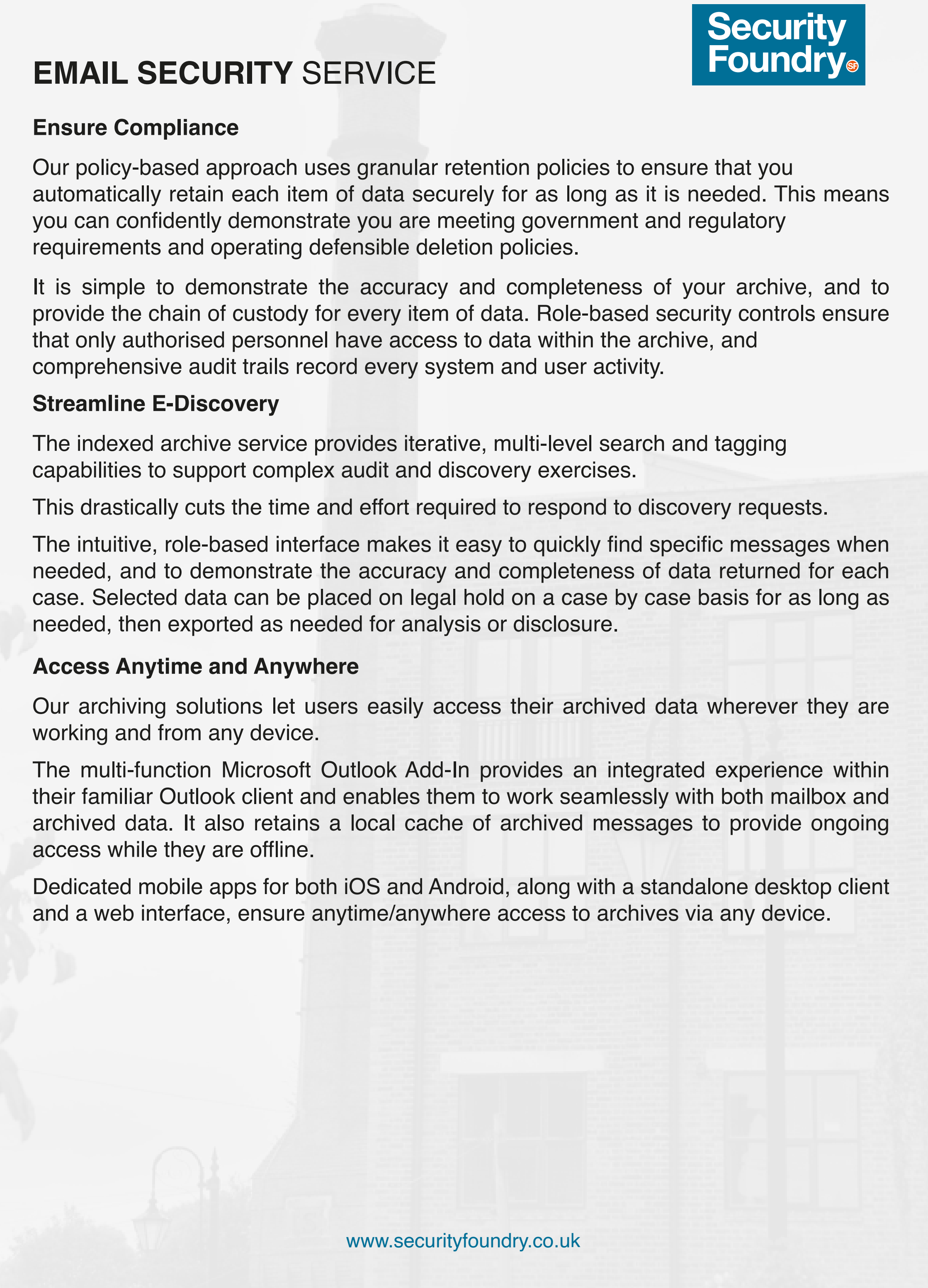
Our award-winning 24x7 technical support is staffed by in-house security engineers. Help is always a phone call away.

Hundreds of thousands of organisations around the globe rely on others protecting their applications, networks and data. Our archiving solutions are part of a comprehensive line of backup, archiving, firewall, and security products and services designed for organisations seeking robust, affordable, easy-to-use protection.

Store Securely

Data is archived outside your operational email environment in a dedicated tamper-proof repository, ensuring it will be retained securely for as long as you need it without risk of corruption or deletion.

Reducing the volume of data managed by your email server can reduce costs dramatically while increasing operational efficiency. Users stay within storage limits without exporting PST files or purging data possibly putting your regulatory status at risk.



EMAIL SECURITY SERVICE

Ensure Compliance

Our policy-based approach uses granular retention policies to ensure that you automatically retain each item of data securely for as long as it is needed. This means you can confidently demonstrate you are meeting government and regulatory requirements and operating defensible deletion policies.

It is simple to demonstrate the accuracy and completeness of your archive, and to provide the chain of custody for every item of data. Role-based security controls ensure that only authorised personnel have access to data within the archive, and comprehensive audit trails record every system and user activity.

Streamline E-Discovery

The indexed archive service provides iterative, multi-level search and tagging capabilities to support complex audit and discovery exercises.

This drastically cuts the time and effort required to respond to discovery requests.

The intuitive, role-based interface makes it easy to quickly find specific messages when needed, and to demonstrate the accuracy and completeness of data returned for each case. Selected data can be placed on legal hold on a case by case basis for as long as needed, then exported as needed for analysis or disclosure.

Access Anytime and Anywhere

Our archiving solutions let users easily access their archived data wherever they are working and from any device.

The multi-function Microsoft Outlook Add-In provides an integrated experience within their familiar Outlook client and enables them to work seamlessly with both mailbox and archived data. It also retains a local cache of archived messages to provide ongoing access while they are offline.

Dedicated mobile apps for both iOS and Android, along with a standalone desktop client and a web interface, ensure anytime/anywhere access to archives via any device.

CLOUD ACCESS SECURITY SERVICE

Our Managed Cloud Security Platform protects data where it lives today, with a solution that was built natively in the cloud, for the cloud. **It's cloud-native data security.**

Detect

Gain complete visibility into data, context, and user behaviour across all cloud services, users, and devices

Protect

Apply persistent protection to sensitive information wherever it goes inside or outside the cloud.

Correct

Take real-time action deep within cloud services to correct policy violations and stop security threats. Enforce data loss prevention (DLP) policies across data in the cloud.

The content engine automatically classifies sensitive information. It enforces controls to remove or quarantine sensitive data in the cloud and prevent data loss via cloud-based email and messaging.

Prevent unauthorised sharing of sensitive data to the wrong people.

The content engine detects granular file and folder permissions, including all owners, editors, and viewers.

The solution enforces collaboration policies in real-time by downgrading permissions, removing permissions and revoking links.

Understand cloud services in use and their risk profile

We summarise cloud usage including cloud services in use by user, along with a risk profile of those services with a 1-10 'CloudTrust Rating'.

Leverage the largest and most accurate cloud registry to enforce risk-based policies.

Block sync/download of corporate data to personal devices.

CLOUD ACCESS SECURITY SERVICE

We understand access context including device operating systems, device management status, and location. We enforce access policies that prevent the download of sensitive data from corporate cloud systems. We can set policies to govern services to untrusted devices.

Our service will detect compromised accounts, insider threats, and malware.

We use Machine Learning to build behaviour models that detect active account compromise and insider threat. Our solutions also leverage signatures and sandboxing to identify malware in the cloud and stop threats.

Encrypt cloud data with keys that only you can access

We enable you to encrypt your sensitive data in the cloud using encryption keys you control, so no third parties, not even the cloud provider, can access your data.

Protect your data while preserving functions such as search.

Audit and tighten the security settings of cloud services.

We automatically audit the security configuration of cloud services and suggest modifications to improve your security posture based on industry best practices.

You can also audit user permissions and tighten excessive permissions.

Security Foundry

IBM i & AIX **PROTECT**

Security Foundry through its trusted strategic partners provide automated Cyber Security Services for the IBM i, AIX and Linux platforms regardless of whether the deployment is on premise or in a private cloud environment. The service combines the use of industry best in class tools from HelpSystems and IBM to guarantee both data protection and regulatory and vendor compliance. The services are delivered to servers on premise or in the Cloud and are managed from a dedicated Security Operations Centre (SOC).

Anti-Virus Services

Utilising the PowerTech StandGuard software for the IBM i, AIX & Windows powered by industry leading provider McAfee. Security Foundry's anti-virus service protects your servers from viruses, worms, and malware threats. The scan engine is backed by battle-tested technology, advanced heuristic analysis, and detection, quarantine and cleaning.

Network Security Services

Prevents unauthorised access to data on the iSeries from any access point. The monitoring and management service provide a host of features designed to protect data and maintain compliance. This includes transaction recording, real-time notifications, dynamic rules access and multi-level access control.

Automated Security Administration Services

Provides simplified data and application access whilst maintaining security and compliance by utilising the PowerTech Policy Minder & Compliance Monitor tools. The service includes Policy management, script design and management services, compliance checking and reporting.

Secure File Transfer Services

Providing an enterprise-level solution that secures, automates and streamlines file transfers for organisations of all sizes. Deployable on-premise, cloud or a hybrid environment, this managed file transfer solution helps organisations to achieve regulatory compliance with ease, improve data security and streamline manual processes.

Risk Assessment Services

Utilising the PowerTech Risk Assessor software allows Security Foundry to provide a comprehensive diagnosis of an organisation's security status and provides a detailed report on over 100 areas of potential vulnerability. The service can be run as often as required to ensure continued safety and compliance.

MANAGED **COMPLIANCE**

Security Foundry through its strategic partners provides a Data Security Compliance Service which integrates with the business' overarching cyber security strategy.

The consultancy service delivers GDPR, ISO and financial regulatory compliance for organisations needing to achieve and maintain these standards throughout their business.

The service also includes an independent cyber security governance service which helps companies to ensure that their policies, processes and technology deployment remains fit for purpose.

Policy Definition Service utilises industry specialists to help define a company's key objectives and the policies, processes and technology required to achieve them. This includes all those policies required to meet statutory regulatory standards such as GDPR, ISO 27001, ISO 9001 and FCA standards.

Gap Analysis Service provides an audit function to business which measures the gap between a company's defined policies and the current reality. The Gap analysis service is an independent service, the output of which can be used to determine immediate and long term action required to achieve consistent compliance.

The service identifies gaps in processes, technology and infrastructure deployment and areas of vulnerability not just in data security compliance but cyber security overall with recommendations of how to achieve a company's objectives.

Statutory Compliance Service is carried out by specialists that know how to implement the required best practice to achieve the key regulatory standards for GDPR, ISO and the FCA.

The Consultants work with clients to implement the technology and processes that ensure statutory compliance and data security which include providing training, documentation and ongoing support. Delivered as a Service by Security Foundry means that each of the Compliance Services can be provided independently of each other or together as an integrated program of activity with the appropriate tools and specialist consultants with the maintenance and support of the compliance program provided on an ongoing service basis.

Security Foundry

Ready to secure your business? **Call us today on 01978 345247**

Email: **readytosecure@securityfoundry.co.uk**

Follow us on Twitter and Company Pages on LinkedIn

@SecurityFoundry **Security Foundry**

Security Foundry Limited, The Foundry, 15 Yorke Street, Wrexham, LL13 8LW