Bridewell

Services Guide

Bridewell provides information assurance and cyber security advice under the specialist cloud services of the G-Cloud framework. Bridewell focuses on providing high quality information security and risk consulting services at competitive prices.

We provide, if required, industry-proven consultants with the highest levels of security clearance. We are able to quickly and efficiently provide solutions by simply focusing on the best qualified consultants to meet your needs.

Bridewell

About Bridewell

Bridewell works together with our customers to support their digital transformation agenda by ensuring we improve cyber security, together.

Cyber security is critical for your business, and we work with you to embed it throughout your organisation to protect your people, processes and systems.

Creating a secure business empowers confident transformation, enabling you to open new markets and revenue streams while proving the ROI of your cyber investment.

With our team of award winning, industry leading experts, and cyber security, penetration testing, data privacy and managed security services, you can create competitive advantage and enable long-term business growth.

Established in 2013, Bridewell is a leading cyber security partner for organisations of critical national importance and is an Assured Service Partner working with the NCSC.

Bridewell is the UK's leading cyber security partner for organisations operating within Critical National Infrastructure (CNI), as well as companies in other highly regulated sectors who require the highest standard of cyber security.

Providing end-to-end cyber security services, including consulting, 24/7 managed security, data privacy and penetration testing, Bridewell work in continuous partnership with clients to implement robust security solutions which defend and protect against threats and attacks and allow organisations to operate safely and efficiently.

Bridewell

Our Accreditations

We currently offer more NCSC assured services than any other company.

Assured Service Provider — in association with National Cyber Security Centre — **Cyber Advisor** (Cyber Essentials)

Assured Service Provider — in association with National Cyber Security Centre — **Cyber Incident Exercising**

Assured Service Provider — in association with National Cyber Security Centre — **Consultancy: Risk Management**

Assured Service Provider — in association with National Cyber Security Centre — **Consultancy: Audit & Review**

Assured Service Provider — in association with National Cyber Security Centre — **CHECK Penetration Testing**

Assured Service Provider — in association with National Cyber Security Centre — **Cyber Incident Response: Standard Level**

Assured Service Provider — in association with National Cyber Security Centre — **Consultancy: Security Architecture**

Assured Service Provider — in association with National Cyber Security Centre — **Cyber Resilience Audit**

Member of Microsoft Intelligent Security Association — Microsoft Security — Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner — Security — Specialist: Cloud Security; Identity and Access Management; Data Security; Threat Protection

AICPA SOC — aicpa.org/soc4so — SOC for Service Organizations | Service Organizations

Crown Commercial Service *Supplier*

CYBER ESSENTIALS — CERTIFIED

CYBER ESSENTIALS — CERTIFIED PLUS

The Certification Group Limited — TCG 27701:2019

CfA Centre for Assessment — ISO 27001 — 23/2183 — UKAS MANAGEMENT SYSTEMS 0120

CfA Centre for Assessment — ISO 9001 — 23/2157 — UKAS MANAGEMENT SYSTEMS 0120

CREST MEMBER — Security Operations Centre; Incident Response; Incident Exercising; Intelligence-led Pen Test; Penetration Testing; Vulnerability Assessment

Ecologi | climate positive workforce

PCI Security Standards Council®

UK Civil Aviation Authority — ASSURE

IASME CONSORTIUM

Fair Payment Code — Gold Until 2026

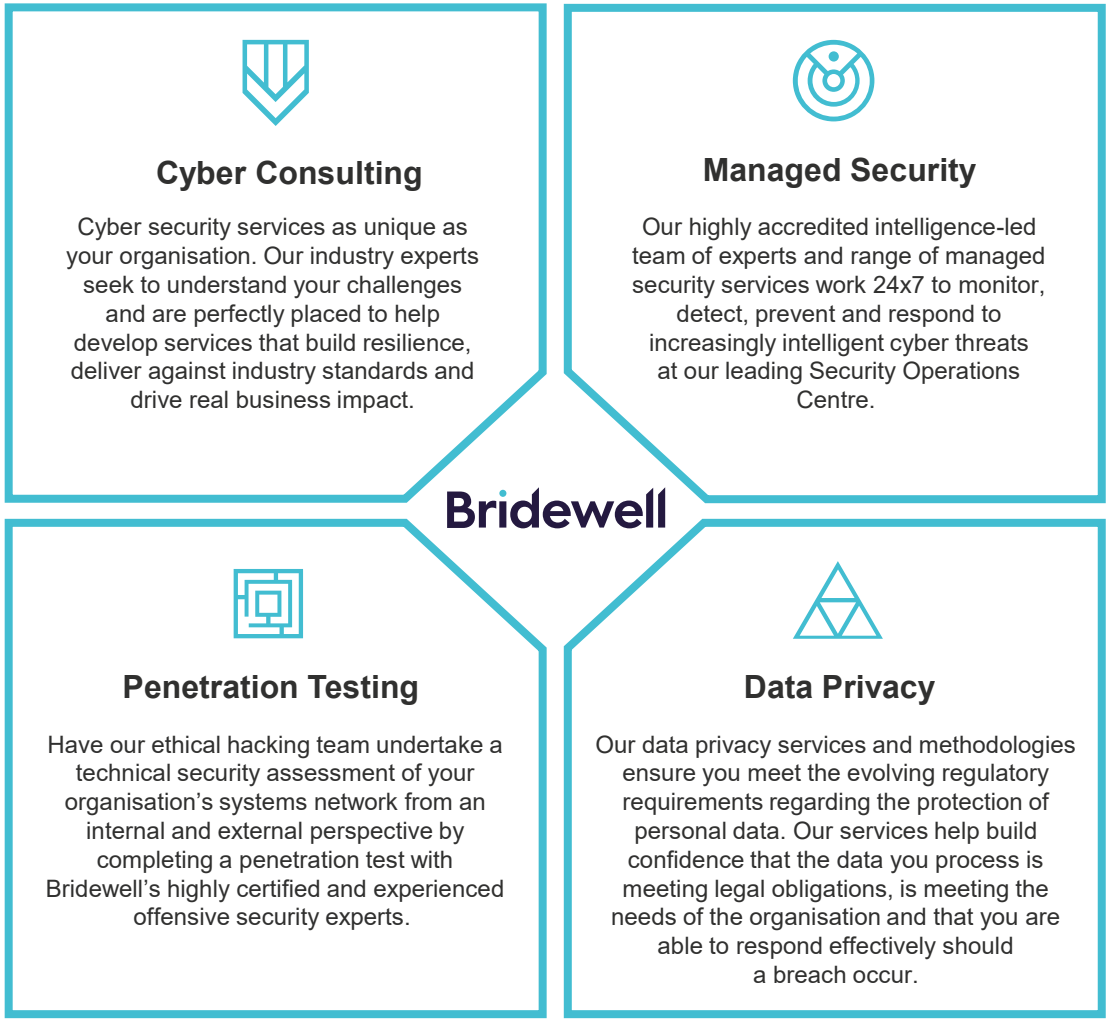
INVESTORS IN PEOPLE | Gold

Cyber and Fraud Centre Scotland — MEMBER

What We Do

Bridewell's services are grouped into four high level areas, which are used to encapsulate the vast range of capabilities that are tailored to meet each client's specific requirements.

Whether you're looking to assess your cyber security posture, implement an international framework or seeking a partner with to provide 24x7 security operations, the section on the right will help you understand the benefits of each area in detail and the possibilities for your business.



Complete, Cutting-Edge Security Services

Clients trust us to deliver comprehensive, flexible and end-to-end services, rooted in the immediate and long-term strategic needs of their business.

Cyber Consulting

- Compliance Frameworks
- Cloud Security
- Cloud Security Assessment
- Security Architecture
- NCSC Certified Services
- PCI QSA Services
- ASSURE Cyber Audits
- Cyber Security Maturity
- Cyber Security Risk
- ICS/SCADA Cyber Security
- Target Operating Model level

Managed Security

- 24/7 Security Monitoring
- 24/7 Managed XDR Services
- Active Threat Hunting
- Cyber Threat Intelligence
- Incident Response
- Digital Forensics
- Continuous Threat Exposure Management
- SOC Automation
- Purple Team Engagements
- SOC Maturity Assessment

Penetration Testing

- Red Team
- Web Application
- IoT & Industrial Control Systems
- Infrastructure
- MITRE ATT&CK Simulation
- Mobile Application
- Source Code Analysis
- SSDLC Advisory
- SecDevOps

Data Privacy

- DPO as a Service
- GDPR Maturity Assessment
- GDPR Gap Analysis
- Breach Response Support
- Programme Leadership
- E-Privacy & PECR Advisory
- Cookie Compliance Management
- OneTrust Implementation
- E-Discovery & SAR Support
- Policy Review & Development

Cyber Consulting

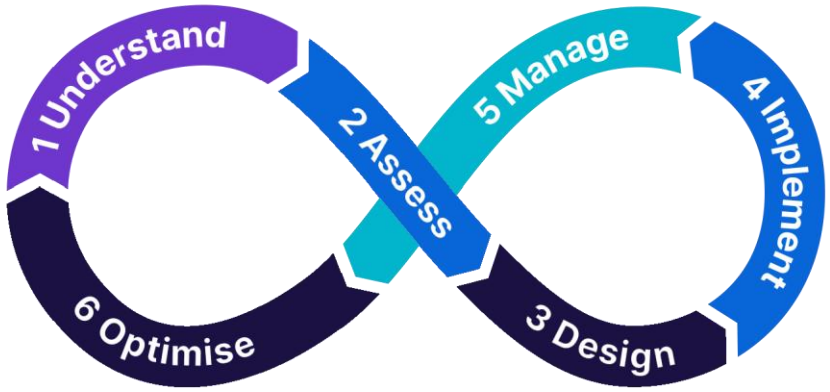
Protect against cyber threats, mitigate risk, and meet legal and compliance requirements in partnership with a leading cyber security services provider.

Bridewell has vast expertise and experience in delivering the range of people, process and technical competencies needed to help organisations meet their cyber security goals - even as they evolve over time.

Approach

Bridewell follows an adaptive, customer-first philosophy that ensures we act as an extension of your organisation.

Understanding your organisation's unique processes, challenges, and objectives is core to our approach. With this insight, our consultants can provide trusted advice that provides true value to your business.



1

Understand

We listen and learn about your business challenges, goals and ambitions, strategic drivers and culture.

2

Assess

We assess your current position relative to your needs and goals, developing a roadmap for optimising your cyber security.

3

Design

We design services, processes and strategies that allow you to achieve the desired state of security and effectiveness.

4

Implement

We draw on our experience and expertise to implement the agreed technical services, governance, compliance frameworks and migration processes.

5

Manage

We operate as an extension of your own cyber security team, delivering tangible, value-added cybersecurity on a 24/7 basis.

6

Optimise

We use our agile yet focused methodology to evolve and optimise you solution over time, to maximise value.

Managed Security

Secure your organisation 24/7 with the industry-leading expertise, methodologies and cyber threat intelligence of a managed detection and response provider.

Our managed security services (MSS) are trusted by industry leaders from critical sectors to protect their organisations and augment their security capabilities.

Managed Security Services

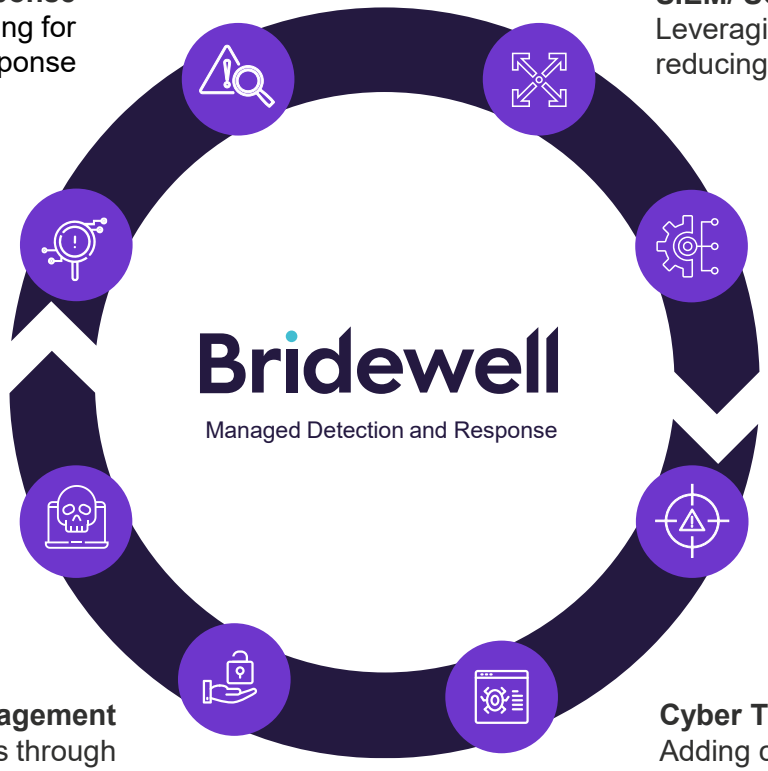
Our threat-informed approach to cyber security has helped our customers increase the effectiveness of their cyber defences, manage risk and prioritise budgets. To deliver this, Bridewell has a complete set of modern security operations services that include the following key components.

Threat Detection and Response
Highly skilled analysts with 24/7 monitoring for triage and rapid response

Digital Forensics and Incident Response
A deep investigation during or after a breach with forensic analysis to ensure the chain of custody for digital evidence

Attack and Breach Simulation
Purple team simulation for continual improvement and breach simulation to embed and improve response practices

Exposure Management and Vulnerability Management
Managing the exploitable surface of customer assets through continuous and scheduled analysis



SIEM/ SOAR Enhancement
Leveraging cloud-native SIEM and scaling operations, and reducing MTTR with SOAR

XDR Technology
Incorporating Detection and Response technology across endpoint, cloud and identity

Threat Hunting
Proactive hunting to identify threats already within the environment

Cyber Threat Intelligence
Adding contextual information to alerts with our mixture of OSINT and commercial intelligence

Managed Detection and Response (MDR)

Bridewell's Managed Detection and Response (MDR) service delivers a leading 24/ 7, threat intelligence-led cyber defence service, delivered from the UK by a leading SC Cleared cyber security experts.

By leveraging the latest in cloud-based SIEM and XDR technology, Bridewell provides a highly effective solution that addresses threats regardless of technology footprint.
This is supported by Bridewell's continual growing security content library that integrates with and takes ownership of the incident response across on-premise equipment, OT, ICS, applications and DevOps.

Features

- 24/7 UK-based, CREST-registered SOC with security cleared individuals.
- CREST and GIAC certified staff.
- Tiered service levels to provide optimal service requirements.
- Analysis and correlation of security information from cloud, on-premise and ICS systems.
- Inclusive of custom detection content development.
- Threat intelligence led security content development.
- Threat intelligence advisories.
- Threat hunting.
- Integrated threat intelligence feeds.
- Intrusion analysis.
- Intelligence integrated incident response.
- Blended human analysis and automated response.
- Supports a wide range of security technology.
- Clear depiction of coverage with MITRE ATT&CK.
- Cloud based SIEM technology, with UK data sovereignty.
- Proactive ownership of the incident response process.
- OT and ICS experience.
- Highly experienced in the delivery of a hybrid/ co-managed SOC to extend internal teams.
- SOC2 accredited service

Managed Detection and Response (MDR)

Bridewell's Managed Detection and Response (MDR) service delivers a leading 24/ 7, threat intelligence-led cyber defence service, delivered from the UK by a leading SC Cleared cyber security experts.

By leveraging the latest in cloud-based SIEM and XDR technology, Bridewell provides a highly effective solution that addresses threats regardless of technology footprint.
This is supported by Bridewell's continual growing security content library that integrates with and takes ownership of the incident response across on-premise equipment, OT, ICS, applications and DevOps.

Features

- 24/7 UK-based, CREST-registered SOC with security cleared individuals.
- CREST and GIAC certified staff.
- Tiered service levels to provide optimal service requirements.
- Analysis and correlation of security information from cloud, on-premise and ICS systems.
- Inclusive of custom detection content development.
- Threat intelligence led security content development.
- Threat intelligence advisories.
- Threat hunting.
- Integrated threat intelligence feeds.
- Intrusion analysis.
- Intelligence integrated incident response.
- Blended human analysis and automated response.
- Supports a wide range of security technology.
- Clear depiction of coverage with MITRE ATT&CK.
- Cloud based SIEM technology, with UK data sovereignty.
- Proactive ownership of the incident response process.
- OT and ICS experience.
- Highly experienced in the delivery of a hybrid/ co-managed SOC to extend internal teams.
- SOC2 accredited service

Managed SIEM and SOC

Bridewells Security Operations Centre (SOC) aims to ensure our customers obtain the maximum value and performance from their investments in security technology through the integration of a highly experienced cyber defence team and established processes.

Our managed SIEM and SOC services enable organisations to partner with Bridewell to build an effective SOC strategy that can also incorporate hybrid/ co-managed operating models.

Features

- Analysis and correlation of security information from cloud, on-premise and ICS systems.
- Threat intelligence-led security content development.
- Integrated public and private threat intelligence feeds.
- 24/7 UK based, CREST-registered SOC with security cleared individuals.
- Supports a wide range of security technology. Clear depiction of coverage with MITRE ATT&CK.
- CREST and GIAC certified staff. OT and ICS experience.
- Highly experienced in the delivery of a hybrid/ co-managed SOC to extend internal teams.
- SOC2 accredited threat hunting
- Blended human analysis and automated response.

Managed Cyber Threat Intelligence

Bridewell's Cyber Threat Intelligence (CTI) gathers information from our own threat research in addition to a range of open, private and trusted sources about current or potential attacks that are relevant to your organisation's sector and operations.

The information is analysed, refined, organised and prioritised by our cyber threat intelligence team so it can be used within your SOC, managed services and organisation to prioritise, minimise and mitigate cyber security risks.

Features

- Threat landscape report generated and maintained.
- MITRE ATT&CK navigator report.
- Threat advisories.
- Analysis and correlation of data tracking malicious actors, campaigns, and breaches.
- Malicious infrastructure tracking provided by Bridewells proprietary platform.
- Threat hunting.
- Provision of security content in sharable languages based upon TTP's observed within the threat landscape and MITRE ATT&CK reports.
- Monthly threat report.
- Request for intelligence.

Incident Response Retainer

Bridewell has a true, UK based 24/7 incident response function. An incident response retainer with Bridewell enables customers to have rapid, SLA backed access to Bridewell's SC-cleared incident response team whenever they are needed.

The service will integrate and enhance your existing Incident Response processes and capabilities.

Features

- NCSC Cyber Incident Response Level 2.
- NCSC assured Cyber Incident Exercising.
- CREST registered SOC.
- CSIRT Team comprising of responders, analysts, intelligence, incident management, testers and DevSecOps specialists.
- Investigations underpinned by intelligence bases analysis methodologies.
- Technical analysis including forensics, cloud, network and malware analysis.
- 24/7 SOC phoneline.
- Service Level Agreement for response times.
- CREST and GIAC certified staff.
- Incident tabletop Exercises
- OT and ICS experience. Readiness assessment

Emergency Incident Response (CSIRT)

Bridewell have a true, UK based 24/7 incident response function that are multi-disciplined and SC Cleared.

The Bridewell team have extensive experience of incident response in cloud, application and on-premise breaches, providing support to companies when emergencies arise.

The Bridewell CSIRT team will enrich active incident investigations with expert advice, management, analysis and investigation to restore operations quickly and effectively and minimising long-term risk.

Features

- NCSC Cyber Incident Response Level 2.
- CREST-registered SOC.
- CSIRT Team comprising of responders, analysts, intelligence, incident management, testers and DevSecOps specialists.
- 24/7 SOC phoneline.
- CREST and GIAC certified staff.
- OT and ICS experience.

Benefits

- Reliable and experienced incident responders and analysts.
- Multi-discipline CSIRT team with cloud and application security experience.
- Integration of threat intelligence into the intrusion analysis and investigation.
- Never lose out. Repurpose unused time.

Pricing

- Pricing for Emergency Incident Response is fixed at £2,200 per 8 hours/ day consumed.

Incident Response tabletop Assessment

The frequency and breadth of cyber security threats continues to grow as adversaries are finding increasing success in exploiting complex business environments. Bridewell's incident response tabletop assessment is designed to leverage threat intelligence and intrusion analysis to test your incident response readiness in a safe environment.

Throughout the engagement, Bridewell will share all data, scenarios, playbooks and learnings to ensure the assessment provides a valuable rehearsal that improves coordination during an active incident response situation.

With "Lessons Learnt" being a key stage in the IR process, your team will develop alongside Bridewell and prioritise activities that would improve the overall resilience of your organisation by improving your ability to respond to incidents effectively.

Features

- Assured NCSC Cyber Incident Exercising provider.
- Scenarios that mimic real world intrusions.
- CREST and GIAC Consultants
- Collaborative table-tops that are designed to improve incident response readiness.

Benefits

- Test your Incident Response effectiveness ahead of time in a safe environment.
- Leverage the experience and intelligence from a leading cyber defence team.
- Identify areas for improvement across people, technology and process.

Pricing

- Please see SFIA Rate Card.

Penetration Testing

Assess the security of your organisation’s network from an internal and external perspective by completing a penetration test with Bridewell’s highly certified and experienced offensive security experts.

Our consultants are accredited by all major industry bodies and have extensive experience using multiple manual and automated enumeration techniques to systematically compromise systems and provide remediation advice.

Purple Team Engagement (Simulated Attack and Response)

The assurance of your cyber defence capabilities is important to develop maturity and manage the risk of active cyber threats. By leveraging threat intelligence and adversary information, Bridewell offers a Purple Team Engagement led by a combination of our incident response, SOC, threat intelligence, and offensive security teams.

Working closely with your existing teams and providers, our methodology allows for a transparent and collaborative approach to testing and a supportive environment for the identification and testing of improvements.

Features

- Adversarial-led purple team engagement.
- Collaborates with existing teams and providers to measure effectiveness and highlight areas for improvement.
- OCSP, CREST, and GIAC-certified consultants.

Benefits

- Improve resilience to active cyber threats.
- Gain assurance of your defensive capabilities.
- Increase leadership confidence in cyber security initiatives.
- Integration of red and blue team specialists with existing teams.

Pricing

- Please see SFIA Rate Card.

Data Privacy

Keep pace with evolving regulatory and compliance demands and build trust in the personal data being used by your organisation with Bridewell's data privacy services.

Our team of highly accredited and deeply experienced consultants will work as an extension of your organisation to build a data privacy programme that meets your specific regulatory requirements and goals.

Managed Digital Risk Protection

Unwanted exposure leads to digital risks. Traditional perimeter-based approaches to security no longer work for today's organisations who are increasingly cloud-based, reliant on expanding third-party ecosystems, and use digital channels to engage with customers. It's only a matter of time until your organisation's digital exposure is unearthed by a customer, competitor, researcher, attacker or manager. Organisations need threat intelligence to manage their digital exposure and minimise their digital risk.

Bridewell leverages the platform capabilities of Digital Shadows to deliver a managed digital risk protection service that integrates our Cyber Threat Intelligence and response capabilities to help manage and reduce the risk from your organisation's external exposure.

Features

- **Brand Protection.** Impersonating domains, mobile apps, and social media profiles.
- **Data Leakage Detection.** Detection of exposed company data, including employee credentials.
- **Dark Web Monitoring.** Identification of threats across criminal forums and dark web markets.
- **Attack Surface Monitoring.** Weaknesses in internet-facing infrastructure.
- **Technical Leakage Detection.** Technical leakage from developers and contractors.

Our Awards


2025 WINNER
UK IT INDUSTRY
AWARDS
Services Company of the Year
>100 Employees


Best
Workplaces
in Tech
Great Place To Work.
UK
2025


Best
Workplaces
for Women
Great Place To Work.
UK
2025


Best
Workplaces
for Wellbeing
Great Place To Work.
UK
2025


Best
Workplaces
for Development
Great Place To Work.
UK
2025


Great Place To Work.
Certified
MAR 2025-MAR 2026
UK

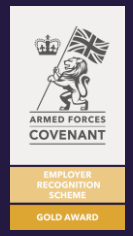

Excellence
Awards 2025
Microsoft Intelligent Security Association
WINNER
Bridewell
Endpoint Management Trailblazer


Top 40
Cyber Security
Companies
2025
TechRound Winner


Cyber Security Awards
2025
WINNER
BEST CYBER SECURITY
SERVICE PROVIDER
OF THE YEAR
Bridewell


FAST
GROWTH
INDEX
2024
SUPPORTED BY UBS
FAST GROWING FIRM IN THE SOUTH


THE NATIONAL CYBER AWARDS 2024
WINNER
The Cyber Business
of the Year Award
trowers & hamlins
BAE SYSTEMS


ARMED FORCES
COVENANT
EMPLOYER
RECOGNITION
SCHEME
GOLD AWARD


Heathrow
Thriving Together Award 2024


the business magazine
THAMES VALLEY
TECH & INNOVATION
AWARDS
2024
WINNER
THAMES VALLEY
TECH COMPANY
OF THE YEAR
Bridewell


GROWING
BUSINESS
AWARDS
2023


LDC
THE TOP 50
2023


2023 WINNER
BEST SECURITY COMPANY OF
THE YEAR –OVER 150 STAFF
Bridewell


CYBER
SECURITY
EXCELLENCE
AWARDS
★ WINNER ★
2022


the business magazine
THAMES VALLEY
SME GROWTH
100
WINNER


THE NATIONAL
CYBER AWARDS
The Cyber Business
of the Year 2021