10 reasons to trust iVendi on security

- iVendi have achieved both the ISO27001 and Cyber Essentials certifications as part of our ongoing commitment to security. We build on the foundations of these standards to ensure our systems can withstand attack.
- Our managed detection and response (MDR) solution monitors our information systems 24/7 to detect and mitigate threats at the start of the attack chain.
- Security is ingrained into our development processes at iVendi, security requirements are discussed during feature scoping and new features are subject to internal penetration testing.
- Automated vulnerability scans are performed continuously against our codebase and infrastructure to ensure our platform is built and configured securely, reducing our attack surface.
- We adhere to web application hosting best practice by hosting our infrastructure across multiple availability zones. This, along with other elements of resilient design, protects us against outages at the equipment, application and data centre levels.
- iVendi uses a wide range of technologies to monitor the end-user experience across applications, network and infrastructure layers to pre-empt issues and improve service delivery. Our Network Operations Centre identifies any performance degradation or service unavailability in an instant and will take corrective action before any end users become aware of an issue.
- Our R&D and procurement functions work closely to ensure we only select the best and most reliable service delivery partners. We closely monitor our supply chain and carry out extensive up-front due diligence and on-going audits on our key suppliers. We also maintain detailed Business Continuity plans which cater for worst case scenarios.
- With the potential high cost in both financial and reputational terms, we take data security and GDPR very seriously, as you would expect. We employ a range of techniques and technologies that meet the very highest standards. Data is encrypted both at rest and in transit throughout our technology stack.
- We use a CREST accredited, third party to conduct external penetration tests annually. These tests are designed to simulate real-world attacks on our applications and infrastructure. On an ongoing basis our web applications are scanned by a leading vulnerability scanning platform to catch security vulnerabilities before they can be made live in production systems.
- Our 24/7 365 ITIL Certified Support team has been recognised internationally by the global Service Desk Institute. The support team adhere to best industry practice and are ISO20000-1 accredited.

UPDATED: 30th April 2024