Security Whitepaper

Introduction

Insights have invested in a comprehensive redevelopment of our technology platforms, with a focus on security and compliance. The New Customer Platform which is the next iteration of Insights Online focuses on enhanced user experience and, more importantly, robust security measures built into the system. Our customer applications have been redeveloped using secure coding practices, a secure development lifecycle, and security engineering principles, including measures such as encryption and multi-factor authentication. This privacy and secure-first approach also extends to our supporting infrastructure.
We value user feedback and have integrated insights from our customers into the redevelopment process. Looking ahead, we are committed to continuous improvements and updates to ensure that our platform remains secure and complaint, meeting industry standards.

Security Certification

ISO 27001:2022 Certification
Since this redevelopment, Insights has successfully completed the ISO 27001:2022 certification. This prestigious certification is a testament to our commitment to maintaining the highest standards of information security.

Why ISO 27001:2022 Certification is Important?
ISO 27001:2022 is an internationally recognised standard for information security management systems (ISMS). Achieving this certification demonstrates that our organisation has implemented a robust framework to manage and protect sensitive information. It involves rigorous assessment and continuous improvement of our security practices, ensuring that we effectively identify, manage, and mitigate risks.

What This Means for Our Customers?
ISO 27001:2022 certified company provides several key benefits:

- **Enhanced Trust and Confidence:** Customers can be assured that their data is handled with the utmost care and security, reducing the risk of data breaches and cyber threats.
- **Compliance with Regulations:** Many industries require compliance with specific security standards. Our ISO 27001:2022 certification helps customers meet these regulatory requirements.
- **Risk Management:** The certification signifies that we have a proactive approach to identifying and managing potential security risks, ensuring business continuity and resilience.
- **Competitive Advantage:** Working with a certified company can enhance your reputation and provide a competitive edge in the market, as it reflects a commitment to best practices in information security.
- **Continuous Improvement:** The ISO 27001:2022 framework encourages ongoing evaluation and improvement of security measures, ensuring that we stay ahead of emerging threats and vulnerabilities.

By achieving ISO 27001:2022 certification, Insights demonstrates its dedication to safeguarding customer data and providing a secure environment for all business operations.

Cyber Essentials Certification
While Cyber Essentials is a UK government-backed and owned, it is not strictly limited to only UK-based organisations.
Here is the breakdown of its scope:

- **Origin and Focus**: The scheme was launched in 2014 by the UK National Cyber Security Centre (NCSC) to establish a minimum, foundational standard for cyber security. It is primarily designed for UK organisations and is mandatory for suppliers bidding on certain UK government contracts.
- **Global Recognition**: It is increasingly recognized worldwide as a trusted standard for cyber security, particularly for international suppliers working with UK-based partners.
- **Applicability**: The five technical controls (firewalls, secure configuration, user access control, malware protection, security update management) are universal and relevant to organizations regardless of their location.

Summary: The scheme is UK-specific in ownership and contract requirements, but it is **globally applicable** as a certification.

Both Insights ISO 27001: 2022 & Cyber Essentials can be viewed via insights.com under Security and Compliance section on the landing page footer.

Penetration Testing

How We Approach Penetration Testing?
Insights is committed to delivering secure solutions to our customers. We regularly conduct penetration tests on our applications using a CREST approved third-party vendor. Additionally, we apply the right security principles throughout these tests.

The latest New Customer Platform was subjected to an external web application penetration test and had ZERO vulnerabilities.

Security Highlights

Below are the key security features we have implemented to ensure the highest level of protection for our customers:

Access Control and Authentication

Zero Trust
Zero Trust is a security framework requiring all users, whether inside or outside the Insights network, to be authenticated, authorised, and continuously validated for security configuration and posture before being granted or retaining access to the New Customer Platform. This approach aligns with the ISO 27001:2022 standard control objectives, including access control and privileged access rights to ensure "least privilege" access.

One Time Token
The One Time Token prevents identity theft by ensuring that a captured email address cannot be reused, avoiding the need to store usernames and passwords.

Single Sign-On
Single Sign-On (SSO) allows customers to use their own identity providers to secure their users within the application, handing off all security measures to the organisations' own systems.

Network and Infrastructure Security

Principle of Least Privilege
This principle ensures that employees, systems, and applications have **only** the access necessary to fulfil their roles and responsibilities. Access rights are carefully determined to align with operational needs and security policies.

No Public IP
Insights servers have no direct connection to the internet, providing a perimeter security solution that protects against external threats. Traffic passes through an outbound proxy which contains a whitelist of allowed domains.

Application Load Balancer
Our application Load Balancers manages internet traffic, acting as a barrier between the internet and the servers. It ensures that only permitted traffic can communicate with the Insights Portal and always uses the latest security SSL/TLS ciphers and protocols.

Suspicious Traffic Monitoring & Rejection
All incoming HTTP traffic passes through a Web Application Firewall (WAF) & suspicious traffic is automatically rejected, notifications are raised with our technology team to investigate, ensuring proactive threat management.

Rapid Software Patch Management
All our infrastructure and application hosting environments are updated every 24 hours using the very latest versions of operating systems and application ensuring the latest security patches are applied to also ensure

compliance with the latest security standards and to protect against emerging threats.

Data Encryption
All data stored within our databases is encrypted using the industry-standard AES-256 encryption algorithm. This ensures that even if data is accessed without authorisation, it cannot be read or tampered with.

Data in Transit
Data exchanged between databases and applications are protected using Transport Layer Security (TLS) protocols. This encrypts data during transfer, safeguarding it against interception and eavesdropping.

Development and Operational Security

Secure by Design
Our Secure by Design approach ensures that Insights Development Teams own the cybersecurity risk from concept to production, managing it effectively throughout the lifecycle. This leads to the delivery of a secure product through clearer accountability, simplified processes, and adherence to security standards.

System Block Mode
Our systems blocks all applications and users by default, allowing access only to those specified in the security policies. These policies establish permissions for each user, process, and resource.

Separation of Server Roles
Servers have separated roles, reducing the impact of any system breach to a single part of the product.

Separation of Evaluator and Learner Data
Evaluator research data is anonymised and stored separately from learner data, ensuring privacy and security for both types of information.

Hardened Client and Server Encryption
All web applications are served using TLS 1.2/1.3 and HTTP/2/3, resulting in A+ scores from SSL Labs. This ensures robust encryption and secure communication.

Comprehensive Audit Trails
All technology changes provide a comprehensive audit trail and require an approval process, ensuring accountability and traceability.

Customer Interaction Auditing
Auditing is applied to all customer interactions, allowing us to specifically identify any misuse of data upon request.

Rate Limiting
Rate limiting caps how often actions can be repeated within a certain timeframe, helping to prevent malicious bot activity and reduce server strain.

Cross-Site Scripting (XSS) Protection
The New Customer Platform blocks XSS attacks through use of hardened Content Security Policies, preventing potential leaks of customer data.

SQL Injection Protection
New Customer Platform mitigates against SQL injection attacks through use of dynamic query construction & execution via parameterised statements, protecting client data from compromise.

Customer Queries
We care about data privacy and security and strive to keep our security practices on par with industry leaders. Read our most frequently asked questions about data privacy and security.

Where is the data stored?
Under EU Data Centre Residency, the compute infrastructure and all Customer Content (production data, backup data, and metadata) is hosted within the EU.

Do you offer the same level of data protection to all of your users?
Yes, rest assured your data is securely managed and held. With TLS 1.2 or higher for transit and AES 256 at rest, in compliance with GDPR and CCPA standards, your data is secured to the highest levels at no additional cost.

Third Party Vendors

Do you sell data to third-party vendors?
No, we do not sell our user data as stated in our Privacy Policy.

Insights has made significant strides in enhancing its technology platform, focusing on user experience and security measures. The successful attainment of ISO 27001:2022 certification underscores our commitment to maintaining high standards in information security management. This certification not only reinforces customer trust but also ensures compliance with industry regulations and promotes effective risk management.

Our proactive approach to security is further demonstrated through regular penetration testing, which has shown no vulnerabilities in our latest New Customer Platform. Key security features, such as Zero Trust access, One Time Tokens, and stringent network protections, exemplify our dedication to safeguarding customer data.

As we continue to prioritise security, we encourage our customers to engage with us regarding any questions or concerns they may have about data privacy and security practices. We remain committed to continuous improvement and adapting to emerging threats, ensuring a secure environment for all our users.
For further inquiries or to access legal information, customers are invited to reach out to our Security Team (security@insights.com) or Legal Team (legal@insights.com) as needed.