HCLSoftware

HCL iObserve

Security Trust Center Document

Version 1.0

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcltechsw.com.

Table of Contents

1 Preface ..... Error! Bookmark not defined.

1.1 Intended Audience ..... Error! Bookmark not defined.

1.2 About this Guide ..... Error! Bookmark not defined.

1.3 Conventions ..... Error! Bookmark not defined.

2 HCL iObserve Trust Center 6

2.1 Commitment to Security and Trust 6

2.2 Secure Product Development 6

2.3 Secure Product Support 6

2.4 Vulnerability Management and Incident Response 6

2.5 Transparency and Supply Chain Security 7

2.6 Certifications and Compliance 7

2.7 Product Security Features 7

2.8 Customer Data Protection and Privacy 7

2.9 Security Resources 7

3 Conclusion 8

4 Support 9

List of Tables

Table 1 – Certifications and Compliance Standards 7

Document Revision History

This guide is updated with each release of the product or when necessary.

This table provides the revision history of this Guide.

Version Date	Description
September, 2025	HCL iObserve Security Trust Center v1.0

1 HCL iObserve Trust Center

At HCLSoftware, we are fundamentally committed to earning and maintaining your trust. Security, privacy, and compliance are the foundations of our products. The HCLSoftware security strategy covers all aspects of our business, including corporate and organizational security policies, incident management and response, business continuity and disaster recovery, secure software development processes, and privacy.

1.1 Commitment to Security and Trust

HCL iObserve delivers comprehensive observability for hybrid IT environments with a core focus on security, privacy, and compliance in alignment with global standards. Our approach integrates secure engineering, transparent operations, and rigorous adherence to best practices, ensuring stakeholder confidence.

1.2 Secure Product Development

Industry-Leading Secure Build Process

- **Secure by Design:** HCL iObserve's development lifecycle aligns with NIST SSDF and EO 14028. We enforce a zero-trust model requiring multifactor authentication and conditional access.
- **Layered Build Environments:** Builds occur in three isolated environments—standard, validation, and production—with administrative separation and cryptographic artifact signing.
- **Consensus-Attested Builds:** Artifacts are built in parallel across environments with peer-reviewed integrity verification.
- **Ephemeral, Hardened Builds:** Environments are recreated per building. All actions are logged and stored immutably.
- **Automated Security Validation:** Static analysis, dynamic testing, and composition scans are integrated across the lifecycle.

1.3 Secure Product Support

- **Minimal Data Collection:** Only necessary diagnostic and contact data is collected.
- **Data Encryption:** Data is encrypted at rest and in transit using AES-256 and secure protocols (e.g., TLS).
- **Strict Access Control:** Role-based access with multifactor authentication is enforced.
- **Secure Communications:** HTTPS, TLS, and SFTP protocols ensure secure exchanges.

1.4 Vulnerability Management and Incident Response

The **HCL Product Security Incident Response Team (PSIRT)** manages the receipt, investigation, and internal coordination of reported security vulnerabilities for HCL Software product offerings. The PSIRT coordinates with product development teams who investigate reported vulnerabilities and identify the appropriate response plan. For more information, visit the HCLSoftware PSIRT page.

The HCL PSIRT publishes Security Bulletins describing any relevant CVEs and pointing to additional details and remediation. A list of security bulletins for HCL iObserve can be found on the official HCL Software support and community forums.

1.5 Transparency and Supply Chain Security

- **Regular Audits:** Security assessments, penetration testing, and red-team exercises are conducted.
- **SBOM Generation:** Every building produces a Software Bill of Materials (SBOM) for audit and traceability.
- **Artifact Verification:** All components are cryptographically signed, verified, and integrity checked.

1.6 Certifications and Compliance

Table 1 – Certifications and Compliance Standards

Certification / Standard	Description	Status
Common Criteria	International IT security standard	Certified (EAL2+ for iObserve v2022.4.1)
ISO/IEC 27001	ISMS certification	Achieved
SOC 2	Security, availability, confidentiality	Achieved for relevant modules
TAA Compliance	U.S. federal Trade Agreements Act	Met
SBOM Availability	Software Bill of Materials	Provided upon request

1.7 Product Security Features

- **Full-Stack Monitoring:** Correlates events across networks, apps, systems, and databases.
- **Risk-Based Prioritization:** CVE-based asset scoring improves remediation workflows.
- **Integration Ready:** Supports OpenTelemetry and third-party security tools.
- **Immutable Audit Trails:** Critical actions logged in tamper-proof repositories.

1.8 Customer Data Protection and Privacy

- **Access Policies:** Enforced via least-privilege and fine-grained roles.
- **Encryption:** All PII and sensitive data is encrypted at rest and in transit.
- **Privacy by Design:** Compliance aligned with GDPR and other global regulations.

1.9 Security Resources

HCL iObserve's Trust Center represents our unwavering commitment to proactive defense, industry compliance, and transparent security practices—empowering you to operate with confidence in a hybrid IT world.

- **Security Bulletins:** Regular updates and advisories.
- **Customer Assistance:** Secure channels for incident reporting and documentation.
- **SBOM & Attestation:** Available upon request for audits and compliance.

2 Conclusion

Our valued clients can rest assured that we keep security foremost in our minds as we develop, test and deliver effective and secure endpoint management solutions to our commercial and government customers.

3 Support

For any product related queries, drop an email here - ifso-pmg@hcl-software.com

HCLSoftware

hcltechsw.com