HCLSoftware

HCL IntelliOps
Event Management

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 Our Commitment to Security & Trust 6

2 Introduction 7

3 HCL IEM 7

3.1 Security 7

3.1.1 Secure by Design 8

3.1.2 Secure Product Development 8

3.1.3 Secure distribution of binary 10

3.1.4 Compliance and Certifications 10

3.1.5 Human Resources Security 10

3.1.6 Infrastructure and Physical Security 10

3.2 Risk management 11

3.2.1 Responsibility for Risk Management 11

3.2.2 AI Risk Management 11

3.3 Responsible AI 11

3.3.1 Secure MLOps Lifecycle Management 13

4 Data Privacy 14

4.1.1 PII Data 14

4.1.2 Storage Backup and Restore 14

4.1.3 Disaster Recovery 15

5 Summary 16

6 Support 17

Table of Figures

Figure 1 - Secure Product Development 9

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
October, 2025	HCL_IEM_Security_Trust_Center_Document_V1.0

1 Our Commitment to Security & Trust

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.

2 Introduction

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.

This Trust Center document provides a transparent overview of the principles and practices governing HCL IntelliOps event management (HCL IEM), giving you the confidence to leverage the AI-powered real-time event intelligence platform to manage your hybrid-cloud environments.

3 HCL IEM

HCL IntelliOps Event Management (IEM) is a cutting edge, AI-powered, IT event management product which empowers organizations with industry leading capabilities such as real-time topology-based alert correlation, ML-Based alert correlation and efficient noise reduction.

The product offers seamless integration with an organization's existing element monitoring tools. This is achieved using the Integration Management Module (IMM), a component of HCL IntelliOps Event Management that offers single-click connectors for seamless integration with leading element monitoring solutions.

With AI-driven capabilities, HCL IntelliOps Event Management identifies root causes, predicts outages, and reduces mean time to resolution, fostering collaborative teamwork and delivering real-time actionable insights. This streamlined approach enhances cost savings, system resilience, and the end-user experience, making it an invaluable asset for optimizing IT operations on a global scale.

IEM applies AI/ML techniques to suppress alert noise, perform topology-aware event correlation, and accelerate triage and root-cause analysis.

The Generative AI capabilities of IEM are delivered through a native Gen AI add-on component, which brokers enterprise foundation models and enforces model governance.

- **ML capabilities in IEM**: Metric-based anomaly detection, topology-aware/dynamic correlation, and feedback loop that continuously improve correlation precision and signal quality.
- **GenAI features offered by HCL IEM**: IEM's GenAI engine leverages Azure OpenAI's GPT 4o-mini model to provide features like natural-language alert analysis and summaries, root cause analysis (RCA) hypotheses, next-best-action recommendations, automatic knowledge article creation, and workflow-based remediation that integrates with runbooks and change records.

3.1 Security

We integrate security into every phase of the product lifecycle, from concept to deployment, to protect your data and infrastructure.

3.1.1 Secure by Design

HCL IntelliOps Event Management (HCL IEM) is developed in-house following a secure software development lifecycle. The product undergoes a comprehensive threat modeling assessment to proactively identify, evaluate, and mitigate potential security risks from the ground up.

- Authentication and Authorization:
  - **Single Sign-On (SSO)**: User authentication is managed via SSO, integrating with enterprise Identity Providers (Azure AD, Okta) over SAML 2.0.
  - **Role-Based Access Control (RBAC)**: A fine-grained RBAC model is enforced to ensure users and services have access only to the resources necessary for their roles.
  - **API Security**: All API endpoints require authentication, using OAuth 2.0.
  - **Session Management**: Idle user sessions are automatically terminated after 60 minutes of inactivity to mitigate the risk of unauthorized access from unattended sessions.
- **Secure-by-Design Architecture**: Adheres to best practices for data encryption, access controls, and secure authentication mechanisms.
  - **Data encryption at rest** – HCL IntelliOps Event Management and IMM database are encrypted at rest using the AES 256-bit encryption. Additionally, data stored in Object storage (GCP Cloud) and Secret Vault (GCP) are encrypted at rest using Cloud native features.
  - **Data encryption in transit** – All access to your instance over the internet is encrypted using Transport Layer Security (TLS) with TLS1.2 cipher suites. All HTTP requests are automatically redirected to HTTPS. We also recommend using encryptions for all integrations.
- **Third-Party Component Vetting**: All dependencies and GenAI integrations undergo rigorous vulnerability and license compliance checks.

3.1.2 Secure Product Development

HCLSoftware adheres to stringent development processes to produce the code and provide to our customers. All Development practices incorporate change control and are the key criteria assessed at release approval stage including key practices around following

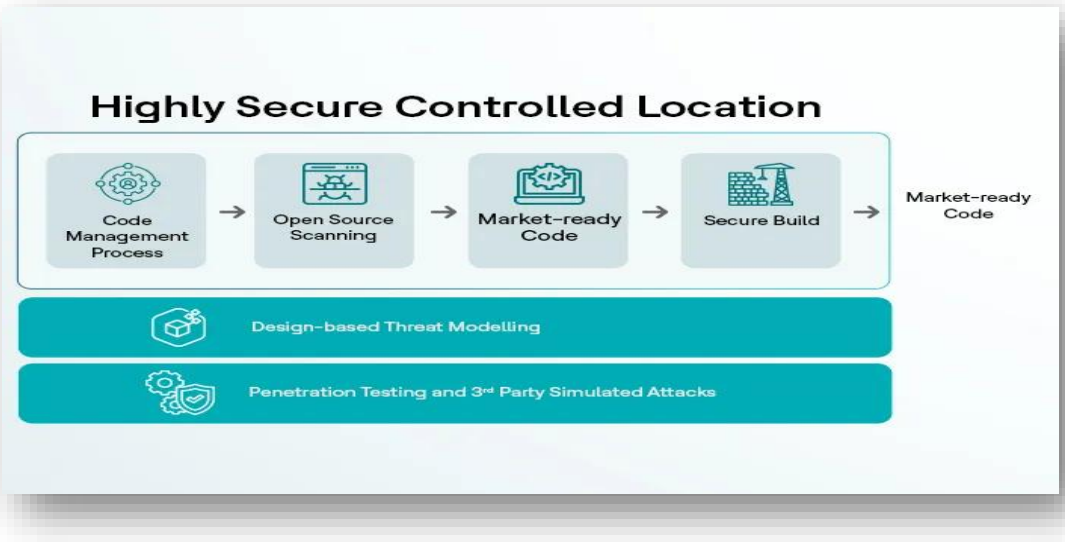

Figure 1 - Secure Product Development

1. **Requirements & Planning**
   - **Data Privacy Assessment**: HCL's Privacy and Data Protection by Design and Default (PbD) addresses privacy requirements during design and verification phases. HCL Software uses the OneTrust Platform to perform Data Privacy assessments for products, platforms, and operations support.
2. **Design**
   - **Threat Modeling**: The process of identifying and prioritizing potential threats to a system and finding mitigation strategies.
   - **Secure Design Review:** Secure Design Review is an assessment done for a product by the HCLSoftware Security team to understand the product architecture, means of deployment / delivery and various other security measures which are in place, as per the industry standards
3. **Development**
   - IDE-Level Code Linting
   - Open-Source Code Composition and Vulnerability Analysis
   - Static and Dynamic Application security testing
   - Penetration Testing - Internal penetration testing is done for every release, and external testing is conducted annually.
4. **Maintenance**
   - Security Bulletins & Vulnerability Management: 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 IntelliOps event management (HCL IEM), can be found on the official HCL Software support and community forums.

- Product Security Training: Periodical training sessions are conducted for product teams on Secure Development, ISMS, Data Privacy, PSIRT Process, and more.

3.1.3 Secure distribution of binary

The binaries for the product are securely distributed via MHS Portal. My HCLSoftware (MHS) is a web application for HCLSoftware customers and partners that provides a new and improved way to find and quickly download the latest HCLSoftware product releases as well as supported older releases. All binaries are cryptographically signed. MHS provides seamless access to resources and tools designed to effectively manage the use of HCLSoftware products and services.

- Active license enforcement
- Usage metering and reporting
- Access-controlled content: users only see content appropriate for them
- Enables seamless access to resources and tools to help effectively manage the entire HCLSoftware experience

3.1.4 Compliance and Certifications

The HCL IntelliOps event management (HCL IEM), platform has the following compliance certification/attestation available:

- ISO 27001
- SOC 2 Type II

Security monitoring and incident response is provided by 24/7 * 365 HCL Software Security Team.

3.1.5 Human Resources Security

Human resources security practices, background checks, and training processes are taken care of by the HCL Software team.

3.1.6 Infrastructure and Physical Security

IEM leverages the robust physical and environmental security controls of its cloud partner, Google Cloud, Network and Perimeter Security

The IEM network is designed to protect against external threats and ensure secure communication.

- **DDoS Mitigation & perimeter Defence**: We utilize GCP Cloud Armor and Firewall as a protective layer at the network edge to protect against both volumetric and application-layer Distributed Denial-of-Service attacks, ensuring service availability.
- **Network Isolation**: All application and data services communicate over a secure, private internal network within the GCP Cloud environment. This isolates critical components from the public internet, reducing the attack surface.
- **Secure Transport**: All data in transit, both externally and internally between microservices, is encrypted using Transport Layer Security (TLS) 1.2 or higher with industry-approved cipher suites. All HTTP traffic is strictly redirected to HTTPS.

- **Cloud Provider Data Security**: GCP Cloud manages infrastructure-level data security, compliance, and physical safeguards. More details can be found in GCP Cloud's Data Security Overview.
- **24 * 7 Security Monitoring**: The Entire platform is under observation with a Security Information and Event Management (SIEM) using Exabeam solution managed by HCL SW.

3.2 Risk management

HCL Software has a formalized risk management program that aligns with ISO 31000 and ISO 27005 best practices, as well as ISO 27001/27002.

Risk management processes are integrated with other management systems, such as the Information Security Management System (ISMS). Security controls are implemented in accordance with our ISMS to manage risk across the organization.

3.2.1 Responsibility for Risk Management

To drive the remediation of risks, our program reports risk status and escalates where necessary to senior management to inform business decision-making. Senior executives have overall responsibility as risk owners for mitigation, avoidance, transference, or acceptance of the risk.

HCL Software uses a combination of weekly, monthly, and quarterly meetings and reports to ensure communication of risks.

Every HCL Software staff member is responsible for the effective management of risk, including the identification of potential risks, the development of risk mitigation plans, and the implementation of risk reduction strategies.

3.2.2 AI Risk Management

HCLSoftware has defined processes and procedures for managing and accessing information systems and operational security risks. HCL IntelliOps event management (HCL IEM) undergoes regular assessments to identify and assess the likelihood and impact of risks.

These potential risks include unauthorized access, use, disclosure, or disruption to HCL IntelliOps event management (HCL IEM), systems and customers. Risks are categorized in accordance with a formally documented procedure.

Any identified risk is managed in a timely manner to safeguard the confidentiality, integrity, and accessibility of HCL IntelliOps event management (HCL IEM), systems and customer data.

3.3 Responsible AI

At HCLSoftware, we are committed to developing and deploying Artificial Intelligence in a manner that is ethical, transparent, and trustworthy. Responsible AI is a core principle that guides the design, implementation, and ongoing improvement of AI-powered capabilities in HCL IntelliOps Event Management (IEM).

- Our Approach to Responsible AI:

- **Ethical by Design:** All AI and machine learning features in HCL IntelliOps event management (HCL IEM), are developed in alignment with HCLSoftware's ethical AI principles, ensuring that technology serves human interests, respects user privacy, and upholds fairness and accountability.
- **Human Oversight:** While leveraging advanced automation, we ensure that all critical AI-driven actions remain subject to human review and intervention wherever necessary.
- **Data Privacy and Security:** AI capabilities in IEM operate on a foundation of strong data governance. Customer data used for AI-driven analytics is protected using the same rigorous security standards that apply across all IEM components, including encryption, access controls, and privacy-by-design practices.
- **Continuous Evaluation:** We regularly assess our AI systems to identify and mitigate risks of bias, inaccuracy, or unintended outcomes. Our AI models are monitored and updated to maintain high standards of accuracy, relevance, and fairness for all customers.

We take a defense-in-depth approach to securing Generative AI systems, covering user data, model interactions, infrastructure, and ethical governance.

1. **User Data Protection**
   - **Encryption in Transit and at Rest**: All user inputs, outputs, and metadata are encrypted using TLS 1.2/1.3 for data in transit and AES-256 for data at rest.
   - **Zero Retention of Sensitive Inputs**: User prompts or responses classified as sensitive are not retained unless explicitly required and approved by the customer.
2. **Access Control & Identity**
   - **Role-Based Access Control (RBAC)**: Fine-grained access is enforced to ensure only authorized users can interact with or configure AI services.
   - **Single Sign-On (SSO) & SAML 2.0 Integration**: Federated identity ensures authenticated access aligned with enterprise identity providers.
   - **Audit Logs**: All access and activity logs are captured and monitored for suspicious behaviour.
3. **API & Model Access Security**
   - **API Key Management**: API keys are securely generated, rotated, and stored in encrypted vaults (e.g., GCP Secret Manager).
   - **Scoped Access**: APIs are protected with least-privilege permissions and rate-limiting to avoid abuse or overuse.
4. **Content Filtering & Prompt Validation**
   - **Real-Time Content Filtering**: Built-in content moderation checks for toxic, harmful, or restricted content using classifiers and guardrails before generating output.
   - **Prompt Injection Protection**: Input sanitization and pattern recognition techniques are used to detect and neutralize prompt injection attempts.
   - **Output Filtering**: Sensitive terms, data leakage, or prohibited topics are blocked before reaching the user.

5. **Secure Development Practices**
    - **OWASP for GenAI**: Regular testing is conducted against OWASP Top 10 for Large Language Models (LLMs), including:
        - Prompt injection
        - Model denial-of-service (DoS)
        - Insecure plugin design
        - Sensitive information disclosure
        - Inadequate sandboxing
        - Supply chain vulnerabilities
    - **Defender for Cloud**: Continuous security posture management with Azure Defender for Cloud (or similar services) ensures compliance, threat detection, and remediation for AI workloads.
6. **Responsible AI and Ethical Safeguards**
    - **Explainability & Auditability**: All AI outputs are traceable with logs and rationales for key decision-making.
    - **Human-in-the-Loop Review**: Critical actions or high-risk decisions include human validation checkpoints.
    - **Transparent Use Notification**: Users are informed when they're interacting with AI systems, maintaining ethical transparency.

3.3.1 Secure MLOps Lifecycle Management

Data Sourcing & Preparation

- Access control to data sources via RBAC

1. **Model Training**
    - Model training is conducted on cloud infrastructure, which improves both security and data privacy.
    - Outlier data is handled by required transformations implicitly for good model fitting.

Model Governance

1. **Model Lifecycle Management**
    - **Version control**: Tracking different versions of models and features.
2. **Model Explainability & Interpretability**
    - Use of integrated model-specific explainers.
    - Model cards
3. **Model Performance Monitoring**
    - Accuracy degradation tracking: E.g., AUC, F1-score over time.

4 Data Privacy

Data privacy (also called information privacy) refers to the right of individuals to control how their personal information is collected, used, shared, and stored. It's about ensuring that personal or sensitive data is handled in ways that protect people's rights and maintain their trust.

Data privacy for the HCL IntelliOps event management (HCL IEM) Platform refers to the protection of customer data by implementing strong technical and organizational controls.

The platform is designed to secure customer-owned data through encryption, strict access controls, and secure cloud infrastructure.

- Data Roles and Responsibilities:
  - In our relationship, the customer is the data controller, retaining full ownership and control over the data collected and determining the purpose of its use. HCL Software acts as the data processor, processing data only on behalf of the controller and in accordance with our contractual agreement. For more information visit HCL Software Privacy
- Purpose Limitation and Data Minimization:
  - The platform is designed to process personal data for the sole purpose of product administration and fulfilling our contractual obligations. We practice data minimization, and the product is not designed to process any special categories of sensitive personal data.
- Customer Information Processed:
  - The platform may process the following customer information as part of its standard functionality:
    - **Contact Information:** Organizational Email Address
    - **Personal Identification:** First Name, Full Name, Last Name
    - **User Account Information:** Login ID

4.1.1 PII Data

In HCL IEM, we collect the following types of information from Customers, and the overall purpose of the data is to provide operations Support and to improve the end user experience for that particular customer.

a. **First Name/Last Name/Full Name**: We collect information about the end user from the Customer for First Name/Last Name and Full Name for general maintenance, support, and to improve the Support Services for the customer. Data is collected via integration with Customer SSO.
b. **Organizational Email Address/Login ID** - We collect information about the end user from the Customer for Organizational Email Address and Login ID for general maintenance, support, and to improve the Support Services for the customer. Data is collected via integration with Customer SSO.
c. **Conversation chat data** - The chat data from the user comprises mostly the user query, where the user can type their query as part of the Chatbot interface, and the text will be stored in an encrypted manner.

4.1.2 Storage Backup and Restore

As part of the base Service, HCL provides storage snapshot backups for data protection of file systems. Storage snapshot backups include supporting data availability, configuring snapshot and replication schedules, and facilitating restore of data from snapshots. Application logs are retained for up to 30 days

and access logs are retained up to 1 year. Additional backup and restore capacity and services are available upon request and for an additional charge.

4.1.3 Disaster Recovery

In the event of an HCL declared Disaster, HCL will communicate with Customer as to the status of the recovery process, including progress regarding the Recovery Point Objective ("RPO") and Recovery Time Objective ("RTO"). The defined RPO/RTO duration is 8 hours RPO, 8 hours RTO.

- HCL provides the ability to failover a full copy of Customer data to a designated standby environment at a geographically disperse DR location within the defined RPO and RTO. HCL manages storage disaster recovery utilizing a replication of storage snapshots to achieve the required RPO/RTO.
- Storage snapshots provide a point-in-time capture of Customer data using the HCL managed storage infrastructure. Differential data changes between snapshots are replicated to offsite storage for maintaining synchronization of the Customer data. Snapshot and replication frequency is determined by the defined RPO/RTO. Storage capacity is allocated per Gigabyte as necessary to meet the Customer contracted disaster recovery requirements.

5 Summary

Our valued clients can rest assured that we keep security foremost in our minds as we develop, test and deliver effective and secure AI-powered real-time event intelligence platform to our customers. For more information, please contact us.

6 Support

For any product related queries, drop an email here - hcl-bigfix-aex-core@hcl-software.com

HCLSoftware

hcltechsw.com