HCLSoftware

HCL BigFix
Runbook AI

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 Introduction 5

2 HCL BigFix Runbook AI Overview 6

2.1 GenAI Feature Overview 6

2.2 Azure Open AI based LLM Model Integration 6

2.3 AI/ML Feature Overview 6

2.4 Core AI/ML Technologies 7

3 Enterprise Integrations 8

4 Security 9

4.1 Secure Distribution of Binary 10

4.2 Secure Product Support 10

5 Data Privacy 12

5.1 PII Minimization and Consent Controls 12

6 Chat Data Management 13

7 Human Resources and Risk Management 14

8 Generative AI Data Security & Responsible AI Controls 15

9 Secure MLOps Lifecycle Management 16

9.1 Model Governance 16

10 Summary 17

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
November, 2025	HCL BigFix Runbook AI Security Trust Center v1.0

1 Introduction

At HCLSoftware, we are fundamentally committed to earning and maintaining your trust. Security, privacy, and compliance are the foundation of our products. The HCL Software 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 provides a transparent overview of the principles and practices governing HCL BigFix Runbook AI Management, giving you the confidence to manage your hybrid-cloud environments with our platform.

2 HCL BigFix Runbook AI Overview

HCL BigFix Runbook AI is an Intelligent Runbook Automation product infused with Gen-AI, Machine Learning and Natural Language Processing capabilities for simplifying and automating the IT Operations resolution across datacenter and cloud landscape, for infrastructure and application-level issues.

2.1 GenAI Feature Overview

1. **Ansible Playbook Generation via Chat (Ticket Console)**
   Enables automatic generation of Ansible playbooks through chat-based interactions within the ticket console.
2. **Knowledge Base (KB) Article Generation via Chat**
   Allows users to create and publish KB articles to ServiceNow. Articles become available upon approval.
3. **Related Tickets**
   Displays incident tickets related to the current issue, providing better context and aiding resolution.
4. **Related Knowledge Articles**
   Retrieves relevant KB articles to assist in resolving incidents more efficiently.
5. **Document Summarization (Advanced Knowledge)**
   Summarizes internal documents to enhance response quality and reduce resolution time.
6. **Agent Assignment Automation**
   Automatically assigns agents based on Assignation Group logic. This feature is part of the Roster Module.
7. **Ad-hoc Playbook Generation via Script Analysis**
   Enables users to generate playbooks on an ad-hoc basis during script analysis when no predefined playbook exists.
8. **Knowledge Graph**
   Provides a node-based visualization of Configuration Items (CIs), KB Articles, SMEs, and related tickets, offering enhanced tracking and deeper insights into issue resolution.

2.2 Azure Open AI based LLM Model Integration

- GPT 4.0: Multimodal AI model

2.3 AI/ML Feature Overview

1. **Runbook Recommendation and Prediction:** This feature analyzes individual tickets, compares them against 4000 runbooks and 500 fixlets, and recommends best automation for resolution along with a confidence score.
2. **Ticket Clustering:** Runbook AI ingests ticket dumps provided by customer, automatically groups similar incidents into buckets, and then recommends appropriate runbooks to resolve all tickets in each cluster.

3. **Knowledge Analysis and Search:** This function allows Runbook AI to act as an intelligent search engine, querying its configured knowledge base to find and provide the most relevant articles for a given ticket or user search.

2.4 Core AI/ML Technologies

- **Sentence Transformer (Embedding Model)** A model that converts sentences into numerical vectors that capture their precise semantic meaning, ideal for contextual search and similarity tasks.
- **BM25 (Reranking)** A powerful keyword-based algorithm that scores and ranks documents (runbooks) by their lexical relevance to a query (ticket description), serving as the primary method for finding the most relevant matches based on term frequency and document statistics.
- **TextRank Algorithm** A graph-based algorithm that identifies and extracts the most important sentences from a text to create a concise summary.
- **Tf-Idf Vectorizer** A classic method that converts text into numbers by highlighting words that are important to a specific document but rare in the overall collection.

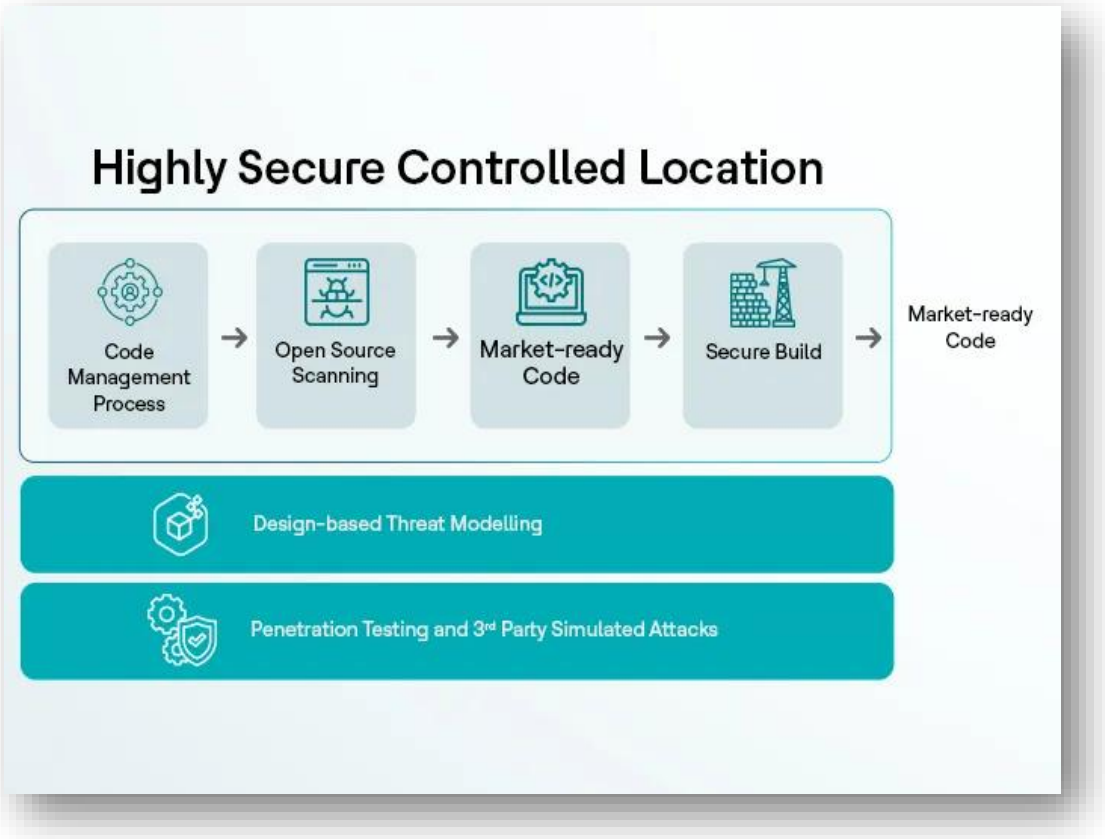
3 Enterprise Integrations

Over 20 integrations are available out-of-the-box, with the capability to create custom integrations.

- **ITSM Tools**: Integrates with leading platforms such as HCL BigFix Service Management, ServiceNow, BMC Remedyforce, Cherwell, and Jira.
- **IT Process & Runbook Automation (ITPA/RBA):** Connects with a wide range of automation engines, including Ansible, Jenkins, Azure DevOps, StackStorm, VMware vRO, Microsoft System Center Orchestrator, and BMC Atrium Orchestrator.
- **Event Management & AIOps:** Works with event correlation platforms like IBM NOI, Moogsoft, and Zenoss to trigger automated event remediation.
- **Data Repositories:** Capable of pulling information from platforms like ServiceNow, as well as from File Folders and Web URLs.

4 Security

HCLSoftware adheres to stringent development processes to protect the code we develop and provide secure products to our customers. HCL BigFix Runbook AI is built with security-first principles at every stage.



- **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.
  - **Quality Planning and Certification**: A Quality Planning and Certification Deck is prepared with key quality metrics and is approved by the QA Lead.
- **Design**
  - **Threat Modeling**: The process of identifying and prioritizing potential threats to a system and finding mitigation strategies.
  - **Secure Design Review**: Conducted by the HCL Software Security team to assess product architecture, deployment methods, and existing security measures based on industry standards.
  - **Secure-by-Design Architecture**: Adheres to best practices for data encryption, access controls, and secure authentication mechanisms.
- **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

- **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 BigFix Runbook AI 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.

4.1 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 manage the use of HCLSoftware products and services effectively.

- 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

4.2 Secure Product Support

Support for BigFix Runbook AI is designed to safeguard customer environments and data.

- **Authentication and Authorization:**
  - **Single Sign-On (SSO):** User authentication is managed via SSO, integrating with enterprise Identity Providers (e.g., ADFS, Azure AD, Okta) over SAML 2.0. BigFix Runbook AI does not store or handle user credentials.
  - **Role-Based Access Control (RBAC):** A fine-grained RBAC model ensures users and services have access only to the resources necessary for their roles.
- **API Security:** All API endpoints require authentication through API keys.
- **Session Management:** Idle user sessions are automatically terminated after 15 minutes of inactivity to mitigate the risk of unauthorized access.
- **Data Encryption:**

- **Data at Rest:** All stored data is encrypted using AES-GCM 256-bit encryption, ensuring confidentiality and integrity.
- **Data in Transit:** If logs are shared, they are transmitted over secure channels using TLS 1.2/1.3 protocols.

- **Access Control & Auditing:** Support access is tightly controlled and logged, ensuring complete visibility and traceability for all actions.

5 Data Privacy

Data privacy (or information privacy) is the right of individuals to control how their personal information is collected, used, shared, and stored. For the HCL BigFix Runbook AI Platform, this refers to the protection of customer data through robust security controls and processes.

- **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. 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:

- **Contact Information**: Organizational Email Address
- **Personal Identification**: First Name, Last Name, Full Name
- **User Account Information**: Login ID
- **Browsing Information**: Session Time and IP Address
- **Organizational Information**: Business Unit Name / Company Name
- **Ticket Information**: Ticket Summary/ Description

5.1 PII Minimization and Consent Controls

- **Customizable Disclaimers**: Customers can configure a disclaimer to instruct users not to enter personal or sensitive information unless required.
- **Data Redaction:** The product supports configurable, regular-expression-based redaction to automatically detect and replace PII elements with generic placeholders in stored conversations.

6 Chat Data Management

Chat data constitutes the majority of data processed or stored in BigFix Runbook AI. A conversation includes both user queries and the responses from the BigFix Runbook AI bot.

- **User Data:** The user's query is typically plain text. While BigFix Runbook AI supports voice input in Chrome, the voice is converted to text and only the text is processed and stored. User queries should not contain sensitive data. While users may type sensitive information, this data is not actively extracted or processed but may be retained in historical logs for auditing and training purposes.
- **Chatbot Data:** The chatbot's response can be in many formats, including HTML articles, images, PDFs, videos, links, and forms. Responses may be a direct solution or a question to gather more information from the user or integrated applications.

7 Human Resources and Risk Management

- **Human Resources Security:** Secure hiring practices, background checks, and security training are managed by the HCL Software team.
- **Risk Management:** HCL Software has a formalized risk management program aligned with ISO 31000, ISO 27005, and ISO 27001/27002 best practices. Senior executives have overall responsibility as risk owners, and every HCL Software staff member is responsible for the effective management of risk.
- **AI Risk Management:** HCLSoftware has defined processes and procedures for managing and assessing information systems and operational security risks. HCL BigFix Runbook AI 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 BigFix Runbook AI systems and customers. Risks are categorized in accordance with a formally documented procedure.

8 Generative AI Data Security & Responsible AI Controls

BigFix Runbook AI takes a defense-in-depth approach to securing Generative AI systems.

- **User Data Protection**: All user inputs and outputs are encrypted in transit (TLS 1.2/1.3) and at rest (AES-256). Sensitive inputs are not retained unless explicitly approved by the customer.
- **Access Control & Identity**: RBAC and SSO are enforced for AI services. All access and activity are captured in audit logs.
- **API & Model Access Security**: API keys are securely managed, rotated, and stored in encrypted vaults. APIs are protected with least-privilege permissions and rate-limiting.
- **Content Filtering & Prompt Validation**:
  - Real-time content moderation checks for toxic or harmful content.
  - Input sanitization helps protect against prompt injection attempts.
  - Output filtering blocks sensitive data or prohibited topics.
- **Secure Development Practices**: Regular testing is conducted against the OWASP Top 10 for Large Language Models (LLMs).
- **Responsible AI and Ethical Safeguards**: AI outputs are traceable, critical actions can include human-in-the-loop validation, and users are transparently informed when interacting with AI systems.
- **AI Governance & Risk**
  - AIMS scope and policy: Follows HCLSW AI policy and scope for the AI Management System (AIMS) with defined accountable roles and human oversight for safety-critical use cases.
  - AI risk register: Risk register covering model theft, inference leakage, and over-reliance risks.

9 Secure MLOps Lifecycle Management

- **Data Sourcing & Preparation**
  - Access control to data sources via RBAC
- **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.

9.1 Model Governance

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

10 Summary

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. For more information, please contact us.

HCLSoftware

hcltechsw.com