HCLSoftware

HCL BigFix AEX

Agentic AI Platform Security Trust Center Document

Version 2.1

Table of Contents

Table of Figures

List of Table

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	BigFix_AEX_Agentic_AI_Platform_Security_Trust_Center Document_V1.1
December, 2025	BigFix_AEX_Agentic_AI_Platform_Security_Trust_Center Document_V2.1

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 Document Summary

HCL BigFix AEX is HCLSoftware's proprietary, enterprise-grade Agentic AI platform that supports both SaaS and full on-premises deployments, enabling organizations to meet security, data residency, and regulatory requirements.

- AEX goes beyond a traditional cognitive virtual assistant by enabling LLM-driven, action-oriented AI agents that can reason, orchestrate workflows, and securely execute tasks across enterprise systems such as ITSM, HRIS, CRM, and other business applications. Through its agentic architecture, AEX enables unified access to enterprise capabilities via conversational, workflow, and automation interfaces while maintaining strong governance and control.
- This document provides a comprehensive overview of the security architecture, controls, and practices supporting the BigFix AEX platform. It describes how AEX ensures secure data exchange across channels and integrations, including agent-to-tool execution and external system access. The document also outlines the platform's secure-by-design approach, including continuous vulnerability scanning, prioritized remediation, GenAI-aware security testing, and structured change management processes designed to minimize risk and reduce exposure.

3 Introduction

The HCL BigFix AEX platform is an enterprise-ready, AI-driven automation and orchestration solution designed to be autonomous, flexible, and secure.

- Deployed on world-class cloud infrastructure, including IBM Cloud and On-premises, AEX provides a robust security posture designed to protect customer data, ensure service availability, and meet stringent compliance requirements.
- This SaaS enterprise application is a generative AI (GenAI) chatbot that leverages IBM Watson as the foundation model and Azure OpenAI or Google Vertex AI for enhanced LLM capabilities.
- AEX is designed as a platform where not only the interaction and solution are provided to users, but also automation can be performed as actions where AEX can create tickets on behalf of a user and gather information from an application that is integrated.

3.1 Data Sources

3.1.1 User:

- Concerning the data in the application or the project, user details are one of the sources of data which is analyzed by using cognitive services, and a relevant response will be provided.
- The response can be a direct solution or further prompt understanding the query better. AEX can respond in multiple ways, which can be a simple textual response, images, and media files like PDF, links, and even forms.

ITSM:

- In the context of an enterprise chatbot like AEX, ITSM platforms serve as dynamic and structured data sources.
- These systems manage the lifecycle of IT services—including incidents, requests, problems, changes, and assets—and hold critical operational data that the chatbot can use to perform actions or provide responses.

3.1.2 Knowledge Base:

- In enterprise environments, a **Knowledge Base (KB)** is a structured repository of information, including how-to articles, FAQs, troubleshooting guides, and policy documents.
- For a chatbot like AEX, the KB is a crucial **data source** that empowers it to provide **self-service, reduce ticket volume,** and offer **instant resolutions** without agent involvement.

3.2 HCL BigFix Deployment Models

- HCL BigFix AEX v12.1 offers flexible deployment models to support diverse enterprise security, compliance, and operational requirements. The platform can be deployed as an HCL-managed SaaS offering or as a fully customer-managed on-premises installation.

– The following table outlines the shared responsibility model across these deployment options, clearly defining ownership for infrastructure, security controls, operations, backup, and disaster recovery.

Table 1 - HCL BigFix Deployment Models

Responsibilities	SaaS	On -Premises
Multi Tenancy	Yes	No
Self-Heal Client support	Yes	No
On-premises Infrastructure Administration & Security Controls	N/A	Customer managed
IBM Cloud Administration & Security	HCLSW (HCL BigFix AEX Team)	N/A
Authentication & Authorization	Customer Provided SSO	Customer Provided SSO
Application Security Vulnerability Remediation	HCLSW (HCL BigFix AEX Team)	HCLSW (HCL BigFix AEX Team)
Data Backup & Restore	IBM Cloud based backup by HCLSW (HCL BigFix AEX Team)	Customer Managed Backup solution to be leveraged
BCP and DR	Backups restore based recovery by HCLSW (HCL BigFix AEX Team)	Customer Infrastructure to be used for Primary and DR setup.
Application Operations Support	HCLSW (HCL BigFix AEX Team)	HCLSW (HCL BigFix AEX Team)

3.3 Platform Security Highlights

– Our multi-layered security strategy is built on the principles of defense-in-depth, secure-by-design, and zero-trust, ensuring that every component of the platform from the physical data centers to the application code is protected.

3.3.1 For SaaS

Key features include:

– TLS 1.2 and 1.3 encryption for data in transit and AES-256 encryption for data at rest.
– IAM- and SAML-based authentication for identity federation.
– Encrypted data at rest and in transit.
– Strict role-based access controls (RBAC).
– Integration with Cloudflare DNS and Global Load Balancer, which also brings in layer 7 firewall capabilities, including WAF and DDoS protection for secure routing.

3.3.2 For On-Premises

Key features include:

– TLS 1.2 / TLS 1.3 encryption for data in transit and AES-256 encryption for data at rest.
– SAML 2.0–based SSO integration with customer-provided identity providers.
– Disk- and storage-level encryption for databases and object storage.

- Secrets and credentials managed using OpenBao Vault with AES-256 encryption.
- Strict role-based access control (RBAC) across platform components.
- Customer-managed network and perimeter security in alignment with enterprise firewall and security controls.

3.4 Artificial Intelligence (AI) Capabilities

BigFix AEX integrates AI responsibly to enhance automation, improve workflows, and deliver experiences. HCL Software promotes safe, transparent, and ethical AI usage.

AEX's AI components include:

- The HCL BigFix GenAI platform is a cloud-native, scalable AI platform hosted on IBM Cloud or on premises, designed to operate within a secure, hybrid cloud environment.
- It ensures seamless integration across public interfaces, on-premises systems, and cloud platforms and their services like Azure - Open AI, GCP - Vertex AI, and AWS Bedrock Nova.
- The HCL BigFix AEX Agentic Platform is an AI-driven automation and orchestration solution designed to streamline enterprise IT operations. It empowers organizations with intelligent, scalable, and secure automation capabilities through modular components.

4 Technical Architecture

4.1 Overview of Technical Architecture

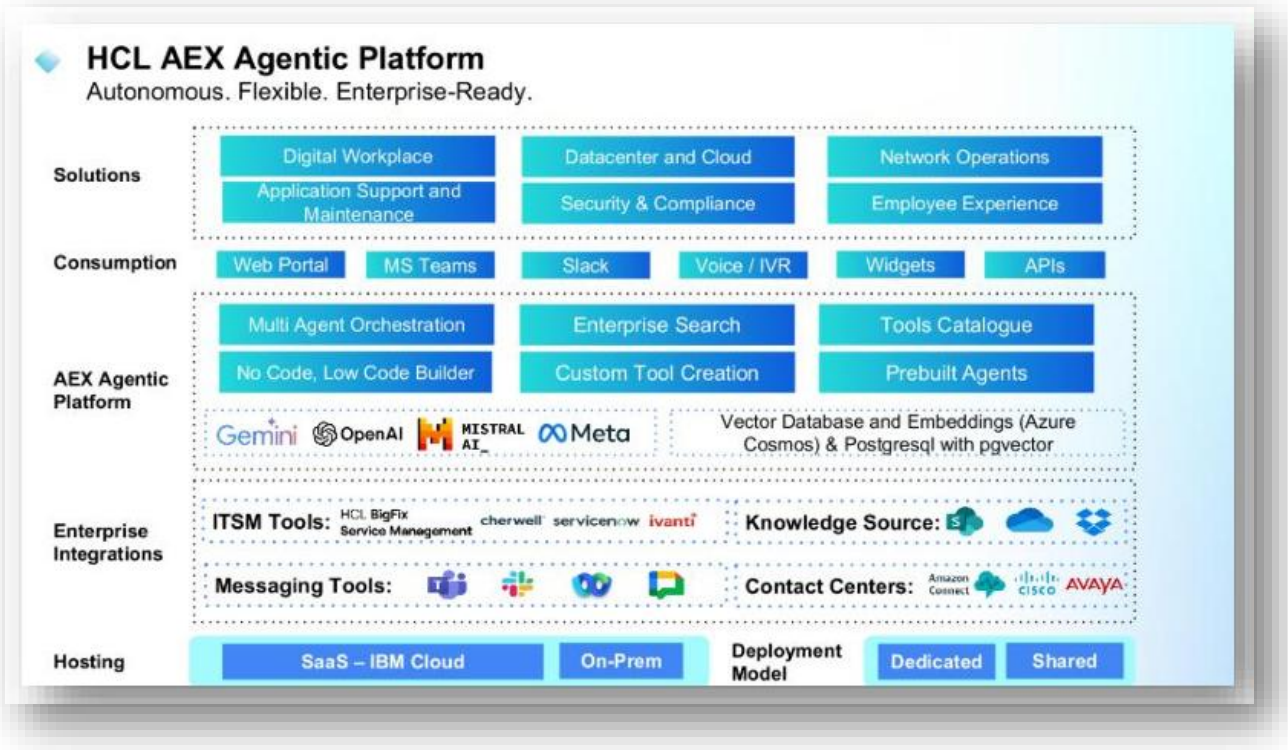

Figure 1 - Overview of Technical Architecture

4.2 Introduction

The HCL BigFix AEX Agentic Platform is an enterprise-grade automation and orchestration solution designed for autonomous, flexible, and secure operations. It enables organizations to integrate AI, IT service management, communication tools, and cloud deployment models to build responsive, intelligent ecosystems.

4.3 Solutions

These represent the core functional areas where AEX can be applied:

- **Digital Workplace**: Enhancing productivity through automation in workplace applications.
- **Application Support and Maintenance**: Automates ticket handling, diagnostics, and resolution.
- **Datacenter and Cloud**: Automation for hybrid and cloud infrastructure management.
- **Security & Compliance**: Enforces compliance policies and automates threat detection.
- **Network Operations**: Streamlines monitoring, configuration, and issue remediation.
- **Employee Experience**: AI-based support for employee needs and interactions.
- **Agentic use cases and automations:** Autonomous IT Incident Resolution, Automated Employee Onboarding and Workplace Support, Multi-Agent IT Operations Orchestration, Web Application Deployment and Rollback Automation, Automated Cross-Cloud Migration Analysis and Cost Optimization

4.4 Consumption Channels

Users interact with the AEX platform through various channels:

- **Web Portal:** Central access for users and admins.
- **MS Teams & Slack**: Chat-based interfaces to execute tasks and receive updates.
- **Voice / IVR**: Enables voice interaction via telephony systems.
- **Widgets**: Embed automation functionality into other UIs.
- **APIs**: Integration with external applications and tools for seamless automation.

4.5 AEX Agentic Platform Features

- **Multi Agent Orchestration**: Orchestrates multiple agents to carry out tasks autonomously.
- **Enterprise Search:** AI-based search engine across knowledge bases and systems.
- **Tools Catalogue:** A centralized repository of tools available within the platform.
- No Code, Low Code Builder: Simplifies app and workflow creation for business users.
- **Custom Tool Creation**: Enables building domain-specific solutions.
- **Prebuilt Agents:** Ready-to-use agents for frequent IT and business operations.

4.6 AI and Foundation Models Integration

The platform integrates with leading AI providers to power automation:

- **Gemini (Google):** Multimodal AI model.
- **Amazon Bedrock**: Access to a variety of foundation models via AWS.
- **Azure OpenAI:** Advanced LLMs for natural language understanding.
- **Anthropic Claude**: Premium models supported under Amazon Bedrock.
- **Mistral AI:** Lightweight and high-performance open models supported via Amazon Bedrock.
- **Meta**: LLAMA models and more supported via Amazon Bedrock

4.7 Enterprise Integrations

- 50+ Integrations are available out of the box with the capability to create custom integrations.
- **ITSM Tools**: Integrates with HCL BigFix Service Management, Cherwell, ServiceNow, and Ivanti.
- **Knowledge Sources:** Includes SharePoint, Confluence, OneDrive, Dropbox.
- **Messaging Tools**: Compatible with MS Teams, Outlook, Slack, and others.
- **Contact Centers**: Works with Amazon Connect, Cisco, and Avaya for call center automation.

4.8 Hosting and Deployment

- **SaaS (IBM Cloud):** Fully managed by HCL SW on IBM Cloud with enterprise-grade security.
- **On-Prem**: Deployment within Customer-owned infrastructure (data center or public cloud).

4.9 Data Storage (for HCL BigFix SaaS)

The NoSQL DB DBaaS is physically hosted on Tier-1 cloud infrastructure providers such as IBM Cloud and Amazon. Therefore, the data is protected by the network and physical security measures that are employed by those providers, including (but not limited to):

- Access and identity management.
- General physical security of data centres and network operations center monitoring.
- Server hardening.
- Cloudant NoSQL DB gives the flexibility to choose or switch among the different providers as customers SLA and cost requirements change.

A multitude of security features is built into Cloudant NoSQL DB, for you to control access to data:

- **Authentication**: Cloudant NoSQL DB is accessed by using an HTTP API. Where the API endpoint requires it, the user is authenticated for every HTTPS or HTTP request Cloudant NoSQL DB receives.
- **Authorization**: Grant read, write, and admin permissions to specific databases.
- "In-flight" Encryption: all access to Cloudant NoSQL DB is encrypted by using HTTPS.
- **At-rest Encryption**: Data that is stored on disk in Cloudant NoSQL DB can be encrypted.
- Data that is stored in a Cloudant NoSQL DB instance is always encrypted.
- API Access: Cloudant NoSQL DB is accessed programmatically by using an API over secure HTTP (HTTPS). API keys can be generated by using the Cloudant NoSQL DB dashboard.

More details on Security can be found in:
https://console.bigfixaex.com/docs/services/Cloudant/offerings/security.html#security
Compliances related to the DB can be found at:
https://console.bigfixaex.com/docs/services/Cloudant/offerings/compliance.html#compliance

4.10 Object Storage (for HCL BigFix SaaS):

IBM Cloud Object Storage is a highly scalable cloud storage service, designed for high durability, resiliency, and security.

- The service can be used to store, manage, and access data via a self-service portal and RESTful APIs. All data is encrypted at rest and in-flight by default.
- IBM Cloud Identity and Access Management (IAM) allows you to control who has access to the resources in your Cloud Object Storage buckets, as well as other IBM Cloud Services, such as IBM Compute instances.

The security and encryption on IBM Cloud Object Storage can be found at
https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-for
https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-for-datadata#objectstorage

5 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 BigFix AEX 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.

5.1 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 both SaaS and on-premises deployment models.
- HCL Software acts as a data processor for SaaS deployment model, processing data only on behalf of the controller and in accordance with our contractual agreement.

For more information, visit HCL Software Privacy.

5.2 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
- **Browsing Information** - Session Time and IP Address
- Business Unit name/Company/Customer Name
- Conversation chat data

5.3 PII Data

In BigFix AEX, 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 customer.

a. **First Name/Last Name/Full Name** - We collect information of 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 of 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. **Browsing Information – Session Time and IP Address** – We collect information of the end user from the Customer for Session Time and IP Address via the Request Header of the payload (for the conversation interaction between user and HCL BigFix AEX). The purpose of this data is to provide support and improve the support services in the case of issues like Latency, connectivity issues, or end-user experience improvement.
d. **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 in HCL BigFix AEX.

5.3.1 PII Minimization and Consent Controls

The product allows customers to configure a customizable disclaimer, which will be displayed as a notification within the Web interface to guide users on appropriate data usage.

- To prevent the ingestion of unnecessary PII data for conversation or Gen-AI use cases, this disclaimer can be used to instruct users not to enter personal or sensitive information unless required for the intended functionality.
- For added protection, the product supports redaction of stored conversation data.
- Regular-expression-based redaction is available as a configurable feature to automatically detect and replace PII data elements with generic placeholders.
- Client-side input redaction can also be performed on the web interface before data is stored.

Additionally, users can exercise their Right to Erasure, enabling them to request the deletion of their personal data from the system when applicable. The data being captured, which is deemed for deletion under this, would be:

a. Email ID
b. Username
c. Query entered
d. Bot's response to the queries by the user

- This information would be erased as per the user's preference, and no back-traceable PII exists. To perform this, AEX provides Right to Delete as a console which can be admin tracked and provides it as a bot use case where the admin can enable the use case and the user can trigger if needed.
- The data erasure request will be completed within seven working days from the date of submission, depending on the organization's policies.

5.4 Chat Data

- Chat data constitutes most data that is being processed or stored in AEX for every conversation happening between the bot and the user.

- Each query or question asked by the user contributes to data that contains multiple variables and text that corresponds to a chat.
- A collection of chats altogether will form a conversation. A conversation can include both user queries and the response from AEX.

5.4.1 User:

- The chat data from the user comprises mostly the user query in the form of plain text. The user can type their query as part of the Chatbot interface, and the text will be captured and sent to AEX core, as mentioned in the network diagram.
- Even though AEX supports voice in Chrome, the data that will be processed or stored will be text, as the voice will be converted into text by using text-to-speech.
- User queries generally should not have any sensitive or critical data as part of it. AEX, while being designed for the use cases, will not collect any sensitive information, but users may type anything as a query that might include sensitive information.
- This information is not extracted, processed, or stored but is kept for historical logs and training purposes only.

5.4.2 Chat Bot:

- Chatbot data comprises responses to the user for every query or response provided by the user.
- The user query is mostly text, but chatbot response can be of many formats, including articles in HTML, Images, PDF, Video, Link, Forms, etc.
- The response from the chatbot can be a direct solution to the query posted by the user or a question to collect further information. The response can also be data from integrations with multiple applications to gather related data.

5.5 Data Access

5.5.1 User Management Console:

- Access to data in the AEX application is highly limited to only customer-side personnel. Dashboards and Portals with data will be controlled by role-based access and can only be accessed by valid users. The users with such access will be checked regularly for actions and access-related approvals to maintain such access.
- Services that hold data cannot be accessed by anyone except the Application Management Team with platform access. This level of access is only available to Administrators of the Application team and the Application Manager.
    - To obtain access to the data-rich dashboards, the user needs to be approved by the project team and justified for having such access. This access will be checked every 3 months to see if the user is active and is still a part of the organization or not.

- In case a specific user's access is revoked, the same will be notified to the user and if required, to the project team with the reason.
- If a specific user's access needs to be removed, then the same can be communicated to the team to remove the access to the dashboards.

5.5.2 SSO using SAML 2.0:

– Customer authentication and access to the AEX application can also be integrated using SAML 2.0 for secure, federated identity management.

– This allows users to log in using their enterprise credentials, ensuring a seamless and secure single sign-on (SSO) experience, while also enabling centralized control and compliance with organizational access policies.

6 Information Life Cycle and Data Management

6.1 Data Retention (for HCL BigFix SaaS)

- As part of AEX, all data that is being captured or processed has a retention period after which the data will be scraped or purged securely.
- The default retention period involves archival after 1 year or a period in compliance with customer security policy.
- Post 1 year, the data will be archived for 3 months, which can be restored in case requested by customers. The data retention period can be customized as per the customer's requirement.

6.2 Data Return and Destruction (for HCL BigFix SaaS)

- After the 15-month total retention period, the data will be purged and can no longer be accessed. In case the data in question is required, then it should be informed before the 15 months so that facilities to provide the same can be made.
- The data retention period can be customized as per the customer's requirement.

6.3 Data Backup and Resiliency (for HCL BigFix SaaS)

- 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 the restoration of data from snapshots.
- Application logs are retained for up to 30 days, and access logs are retained for up to 1 year. Additional backup and restore capacity and services are available upon request and for an additional charge.
- At the termination or expiration of the Agreement and/or this Service, HCL will not be required to remove copies of Customer data from its backups until such time as the backup copies are scheduled to be deleted in the normal course of business.

Table 2 - Data Backup and Resiliency

Component	Frequency	Duration
Cloudant	Weekly	30 Days
Vector DB	Daily	35 Days
Redis	Daily	30 Days
Postgres	Daily	30 Days

Other high availability stores like object storage services are point in time backup as they contain non-critical assets only and work with the CDN of Cloudflare.

7 Information Security Governance and Risk Management

7.1 Security frameworks

- HCL BigFix AEX maintains appropriate technical and organizational measures designed to protect the data collected from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, and access.
- BigFix AEX is built on secure cloud architecture hosted on IBM Cloud or Customer owned Infrastructure (on-premises). Security controls follow industry's best practices for encryption, authentication, and access management.
- Customers retain flexibility in selecting their preferred cloud region and hybrid configurations, ensuring alignment with their own security and compliance requirements.

7.2 Global Load Balancer Security (for HCL BigFix SaaS)

- To enhance the application's security posture, we use Cloudflare as a protective layer that also behaves as a layer 7 firewall. Additionally, Cloudflare provides DDoS protection, mitigating volumetric and application-layer distributed denial-of-service attacks to ensure availability and performance even under attack conditions.
- It also includes a robust Web Application Firewall (WAF) that helps detect and block malicious traffic, such as SQL injection, cross-site scripting (XSS), and other OWASP Top 10 threats, before they reach the application.
- This setup helps safeguard the application from external threats while maintaining reliable access for legitimate users. WAF Rules are continuously checked and updated with the help of Cloudflare to ensure the latest discovered vulnerabilities are being identified and protected against.
- In on-premises deployments, equivalent perimeter security controls are implemented and managed by the customer.

7.3 Infrastructure and Physical Security (for HCL BigFix SaaS)

AEX leverages the robust physical and environmental security controls of its cloud partners, including IBM Cloud for Application hosting and Microsoft Azure, Google Cloud, and AWS for LLM models.

- **Network and Perimeter Security:** The AEX network is designed to protect against external threats and ensure secure communication.
- **Perimeter Defense**: We utilize Cloudflare as a protective layer at the network edge. This provides:
  - **Web Application Firewall (WAF)**: To detect and block common web attacks like SQL injection and Cross-Site Scripting (XSS).
  - **DDoS Mitigation**: 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 IBM 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**: IBM Cloud manages infrastructure-level data security, compliance, and physical safeguards. More details can be found in IBM Cloud's Data Security Overview.
- **Monitoring**: The Entire platform is under 24*7 observation with a Security Information and Event Management (SIEM) using Devo as the tool, maintained by HCL SW.
- The platform also includes heartbeat monitoring as well.
- **For On-Premises deployments,** physical and environmental security controls are the responsibility of the customer's data center and infrastructure providers.

7.4 Application Security

AEX incorporates multiple layers of security at the application level to control access and protect against threats.

- Authentication and Authorization (For both Saas & On-Premises):
  - **Single Sign-On (SSO)**: User authentication is managed via SSO, integrating with enterprise Identity Providers (e.g., ADFS, Azure AD, Okta, PingFederate) over SAML 2.0 through the IBM App ID service. AEX does not store or handle user credentials.
  - **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, either through API keys (e.g., Azure OpenAI) or OAuth 2.0 (e.g., IBM Watson).
  - **Session Management**: Idle user sessions are automatically terminated after 15 minutes of inactivity to mitigate the risk of unauthorized access from unattended sessions.
- **Data Security**: In Transit and At Rest (For both Saas & On-Premises)
  - **Data in Transit**: All communication between users, services, and external systems is encrypted using **Transport Layer Security (TLS) 1.2/1.3**, ensuring confidentiality and integrity of data over the network. Internal microservice communication is also secured via mutual TLS (mTLS) where applicable.
  - **Data at Rest**: All data stored within the platform, including logs, configurations, and user-related data, is encrypted at rest using **AES-256 encryption standards.**
    - In **SaaS deployments**, encryption at rest is supported by the underlying cloud provider infrastructure, with encryption keys managed through the provider's Key Management Services (KMS).
    - In **on-premises deployments**, encryption at rest is enforced through disk- and storage-level encryption for databases and object storage, with secrets and encryption materials managed using customer-controlled vault and key management solutions (e.g., OpenBao Vault).

7.5 Human Resources Security

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

7.6 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.

7.7 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.
- In On-Premises deployments, customers retain responsibility for infrastructure-level and operational risks

7.8 AI Risk Management

- HCLSoftware has defined processes and procedures for managing and accessing information systems and operational security risks.
- HCL BigFix AEX 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 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 BigFix systems and customer data.

8 Secure Development Life Cycle (SDLC)

8.1 Secure Development

– HCLSoftware adheres to stringent development processes to protect the code we develop and provide secure products to our customers.

Figure 2 - Secure Development

8.1.1 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 One Trust 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.

8.1.2 Design

– **Threat Modelling**: 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.

8.1.3 Development

– IDE-Level Code Linting
– Open-Source Code Composition and Vulnerability Analysis
– Static and Dynamic Application security testing
– Code Quality and Code Smell Analysis
– Penetration Testing: Internal penetration testing is done for every release, and external testing is conducted annually to find vulnerabilities that attackers could exploit.

8.1.4 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 BigFix AEX 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.

9 GEN AI Data Security & Responsible AI Controls

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

9.1 User Data Protection

- Encryption in Transit and at Rest: All data exchanged within the AEX platform is encrypted in transit using TLS 1.2 / TLS 1.3 (HTTPS). For on-premises deployments, data at rest is protected through disk-level and storage-layer encryption, including:
  - Database storage (MongoDB, PostgreSQL with pgvector) using OS-level disk encryption
  - Object storage (MinIO) protected via encrypted NFS volumes and Kubernetes PVCs
  - Secrets and credentials stored securely in OpenBao Vault using AES-256 encryption
- Zero Retention **of Sensitive Inputs**: User prompts or responses classified as sensitive are not retained unless explicitly required and approved by the customer.

9.2 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**: User authentication is managed via SSO, integrating with Customer provided enterprise Identity Providers (e.g., ADFS, Azure AD, Okta, PingFederate) over SAML 2.0.
- **Audit Logs**: All access and activity logs are captured and monitored for suspicious behaviour.

9.3 API & Model Access Security

- **API Key Management**: API keys are securely generated, rotated, and stored in encrypted vaults (e.g., for SaaS using IBM Key protect, Open Vault in on-premises deployments).
- **Scoped Access**: APIs are protected with least-privileged permissions and rate-limiting to avoid abuse or overuse.

9.4 Content Filtering & Prompt Validation

- **Real-Time Content Filtering**: Built-in content moderation checks for toxic, harmful, or restricted content using prompt-based guardrails and policy checks 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.

9.5 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.
  - Follows a comprehensive security testing framework covering threat modelling, SAST, DAST, Mend, Sonar, and Prisma.
  - Includes penetration testing by HCLSW Security team aligned with OWASP Top 10 for Web and GenAI risks for every release and external team annually.
  - **Secure Deployment & Operations**: Hardened configurations, automated CI/CD security checks, strict Dev/Test/Prod separation, least-privilege access controls, and defined incident response processes.
  - **Secure-by-Design Development:** Security is embedded across the SDLC through threat modeling (e.g., STRIDE), secure coding practices, strong input validation and output encoding, encryption of data at rest and in transit, centralized secrets management, and secure code reviews.

9.6 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.

9.7 Compliance and Certifications

The HCL BigFix AEX platform (SaaS) has the following compliance certification/attestation available:

- ISO 27001
- SOC 2 Type II
- CERT – IN

The HCL BigFix AEX platform (On-premises) has the following compliance certification/attestation as part of the roadmap:

- ISO 27034

10 Conclusion

Our valued clients can rest assured that we keep security foremost in our minds as we develop, test, and deliver effective and secure solutions to our customers. For more information, please contact us.

11 Support

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

HCLSoftware

hcltechsw.com