HCLSoftware

HCL BigFix AEX

v14

Release Notes



The data contained in this document shall not be duplicated, used, or disclosed as a whole or in part for any purpose. If a contract is awarded to chosen parties because of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client's or prospective client's right to use the information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in all marked sheets. HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcltechsw.com.

Copyright © 2026 HCL Technologies Limited.

Table of Contents

1 Executive Summary 5
2 Key Features 6
2.1 AEX A2A Server 6
2.2 Programmable Context Management 6
2.3 Agent Taxonomy Console 6
2.4 Workflow Resilience & Controls 7
2.5 Workflow Canvas Enhancement 7
2.6 Agent Builder 2.0 7
2.7 Function Changelog and LLM as Judge 8
2.8 Redaction Console and Chaos Playground 8
2.9 MCP Server Creation using Gateway 8
2.10 Workflow Versioning and Changelogs 9
2.11 MCP Server Health Monitoring 9
2.12 List of Supported OTB Tools 10
3 HCL BigFix AEX Architecture 11
3.1 Reference Architecture 11
3.2 Deployment Architecture 12
3.2.1 AKS 12
3.2.2 EKS DEPLOYMENT 12
3.2.3 VM-BASED DEPLOYMENT 13
4 Secure Release Checklist and Reports 13
4.1 Release Checklist 13
4.2 Packages included in HCL BigFix AEX 14
4.2.1 AEX 14
4.3 AEX Analytics 17
4.4 AEX Functions 17
4.5 AEX Utilities 18
4.5.1 Scheduler 19
4.6 Gateway Services 20
4.6.1 Gateway Client (only on EKS, AKS) 20
4.7 HCL AppScan SAST Reports (AKS, EKS, VM-Based) 21
4.7.1 SAST Report - AEX 21
4.7.2 SAST Report - Scheduler 21
4.7.3 SAST Report - AEX Analytics 22
4.7.4 SAST Report - AEX Functions 22
4.7.5 SAST Report - AEX Utilities 22
4.7.6 SAST Report - AEX Gateway Services 22
4.7.7 SAST Report - AEX Gateway Client (EKS, AKS) 22
4.8 HCL AppScan DAST Reports (AKS, EKS, VM-Based) 23
4.8.1 DAST Report - AEX Web 23
4.9 Mend Security Reports (AKS, EKS, VM-Based) 23
4.10 Security Penetration Testing Report 23
4.11 PSIRT Details 24
4.12 Load Testing Reports 24

5 Application Security Controls..... 25
6 Known Issues..... 26
7 Looking Forward..... 27
8 Blocked Packages..... 28

1 Executive Summary

HCL BigFix AEX v14 advances the platform's focus from explainability toward interoperability, resilience, and operational control, extending the agentic AI foundation with secure external connectivity, hardened workflow execution, and tighter governance over context, functions, and agent authoring.

The release extends the platform with the AEX A2A Server, introducing a defined, secure Agent-to-Agent protocol that lets external agents and third-party systems connect bidirectionally with AEX agents and moving beyond one-way API calls to enable AEX's participation in multi-vendor agent architectures. Programmable Context Management gives developers and administrators fine-grained control over conversational memory, combining truncation and summarization strategies with persistent, user-level preferences, alongside a configurable iteration execution range that replaces the previous fixed limit for safer, more predictable agent runs.

Governance deepens across the platform. The Agent Taxonomy Console brings full lifecycle management to agent classification tags, with impact preview and delete guardrails to prevent accidental breakage at scale. Function Changelog and LLM as Judge add an audit and safety layer to function development, automatically screening code on every save and logging a permanent, reviewable trail of changes and overrides. Agent Builder 2.0 is redesign of the GUI builder into a behavior-first, step-by-step canvas, further refining it into a guided authoring experience that follows the agent's chronological execution lifecycle from setup through decision-making to execution. Workflow Canvas Enhancements optimized performance for complex workflows, design-time execution testing, multi-node bulk editing, cutting iteration time for workflow designers and extending authoring access to non-technical users.

Overall, this release reinforces AEX as a platform built not just to connect and automate agentic work, but to ensure every connection, change, and execution remains auditable, recoverable, and under direct administrative control.

2 Key Features

This release includes the following list of new features & enhancements.

2.1 AEX A2A Server

AEX introduces a defined, secure Agent-to-Agent (A2A) protocol that lets external AI agents and third-party systems connect directly with AEX agents, supporting two-way collaboration rather than one-way API calls.

Key Enhancements:

- Secure external agent endpoint with all external calls authenticated and authorized
- Defined message schema covering requests, responses, events, and metadata
- Bidirectional communication - external systems can trigger actions on AEX agents, and AEX agents can push events/updates back out

Business Impact:
Enables AEX to participate in multi-vendor agent architectures alongside external agents and systems.

2.2 Programmable Context Management

Gives developers, professional service teams, and administrators fine-grained, agent-level control over how an agent manages conversational context and long-term memory - balancing continuity, relevance, and resource consumption.

Key Enhancements:

- Context handling - truncation and summarization-based strategies manage the context window as conversations grow, retaining relevant information without unchecked growth.
- Persistent, controlled memory - Long-term user preferences persist across sessions and can be naturally added, updated, or deleted through the same conversational experience used to interact with the agent, delivering consistent personalization.
- Execution safeguards - Replaces the previous fixed 16-iteration execution limit with a configurable 3–50 iteration range, preventing runaway reasoning loops, improving predictability, stability, and cost control during agent execution.

Business Impact:
Prevents unnecessary context-window bloat and token consumption, enables personalized agent experiences through persistent user preferences, and gives users precise control over agent execution depth. Thus, directly addressing context reliability, a top pain point in agentic AI products.

2.3 Agent Taxonomy Console

A dedicated admin console for full lifecycle management of agent tags - moving from tags fixed at creation time to complete CRUD control and governance at any point.

Key Enhancements:

- Hierarchical, searchable taxonomy view with usage counts per tag
- Add/edit/delete custom tags with duplicate prevention; with custom tags appear alongside the default taxonomy in Agent Builder
- Impact preview before deletion to see and link to affected agents
- Delete guardrails where tags still in use can not be deleted

Business Impact:
Gives admins ongoing, safe control over agent taxonomy at scale while preventing accidental classification breakage.

2.4 Workflow Resilience & Controls

Hardens workflow execution so failures are handled gracefully and administrators retain direct control over running activations at all times.

Key Enhancements:

- Scheduler resilience - execution state persists and auto-recovers after outages
- Continue on Error - skip failed nodes gracefully instead of halting the whole run
- Disable individual nodes without deleting them, for safe testing of alternate paths

Business Impact:
Workflows no longer silently fail or get stuck and thereby reducing downtime, support escalations, and the operational risk of runaway or broken executions.

2.5 Workflow Canvas Enhancement

A faster, more capable workflow-building experience - from canvas performance to bulk editing to API-driven workflow creation.

Key Enhancements:

- Optimized canvas performance for large, complex workflows
- Design-time execution - test workflows instantly without saving first
- Multi-node select, copy, paste, duplicate, and delete for bulk editing
- API-first workflow creation with automatic visual layout generation
- Refreshed, modernized workflow list page UI

Business Impact:
Cuts development and debugging time significantly, letting workflow designers iterate faster and reuse work across projects, directly improving time-to-value for automation teams.

2.6 Agent Builder 2.0

Redesigns the Agent Builder from a technical node graph into an intuitive, behaviour-first sequential canvas that mirrors how an agent actually thinks and acts.

Key Enhancements:

- Agent building is elevated to a guided behavior-first authoring experience where the builder naturally follows the chronological execution lifecycle of an agent.
- Canvas redesigned as a step-by-step timeline that mirrors how the agent actually thinks and acts, from setup through decision-making to execution.
- Prompts introduced as an independent, first-class node

Business Impact:
Makes agent authoring accessible to non-technical users by transparently visualizing how platform components collaborate during execution, reducing reliance on technical expertise while still serving experienced builders and expanding who across an organization can build and maintain agents.

2.7 Function Changelog and LLM as Judge

A built-in audit and safety layer for functions - every change is automatically tracked, and every piece of code is screened by an AI safety judge before it's deployed.

Key Enhancements:

- Changelog of every function change (create, update, delete, import), who changed it, and when
- AI-powered safety check on every save, flagging code as Safe, Unvalidated, or Risky with a clear reason
- Override capability for risky code, with a logged audit trail of who approved it and when
- Signature verification on import - safety status is preserved if valid, or cleared for re-validation if not
- Version snapshots of function code, letting teams checkpoint and revert to known-good states

Business Impact:
Gives teams full visibility and control over function changes, while the built-in AI safety check reduces the risk of unsafe or unauthorized code reaching production - all backed by a complete, permanent audit trail for compliance.

2.8 Redaction Console and Chaos Playground

A central console for defining, managing, and testing the rules that detect and redact sensitive data, with a Chaos Playground to see how a message is sanitized before it reaches the model.

Key Enhancements:

- Redaction Rules table showing each rule’s type, pattern, action, and on/off status
- Built-in Rule Library for importing common personal-data protections in a few clicks
- Custom rules with configurable patterns and match thresholds, editable at any time
- Chaos Playground that runs a sample message through four stages: raw input, sanitized payload, simulated LLM response, and final output

Business Impact:
Lets teams find and fix data-exposure gaps before agents go live, and confirm how sensitive data is handled at each step. This improves compliance confidence and reduces the risk of customer data reaching the model or logs.

2.9 MCP Server Creation using Gateway

A guided tool in the Gateway Client that turns an existing API into a ready-to-use MCP server in just a few steps, no manual coding required along with a built-in way to test it before putting it to work with an agent.

Key Enhancements:

- One-click MCP server generation from an API collection you already have, with no manual setup required
- A simple selection screen to choose exactly which API actions should be made available to AI agents
- An instant, ready-to-run server package delivered as a single downloadable file, complete with setup instructions
- A built-in testing tool to confirm the new server works correctly before it’s connected to a live agent

Business Impact:

Turns an existing API into an agent-ready tool in minutes instead of days of custom development. Teams can safely validate a new integration before it goes live, lowering the risk of failures once agents start relying on it.

2.10 Workflow Versioning and Changelogs

Every workflow change is recorded, and any saved version can be compared or restored, so teams can answer both “what changed and who changed it” and “can we go back.”

Key Enhancements:

- Automatic changelog of every workflow change, showing the field changed, previous and updated values, who made the change, and when
- Save named versions from the workflow canvas at any point
- Side-by-side comparison of two versions, highlighting what differs at each node
- One-click rollback to a previous version, recorded as a new version so no history is lost

Business Impact:
Teams can make workflow changes with confidence, because every change is recorded and any saved version can be restored in one step. This shortens troubleshooting and strengthens governance, since audit records show exactly what changed, who changed it, and when.

2.11 MCP Server Health Monitoring

A live dashboard that keeps watch over all connected MCP servers, so teams can see at a glance which ones are up and running and catch problems before they disrupt agent workflows.

Key Enhancements:

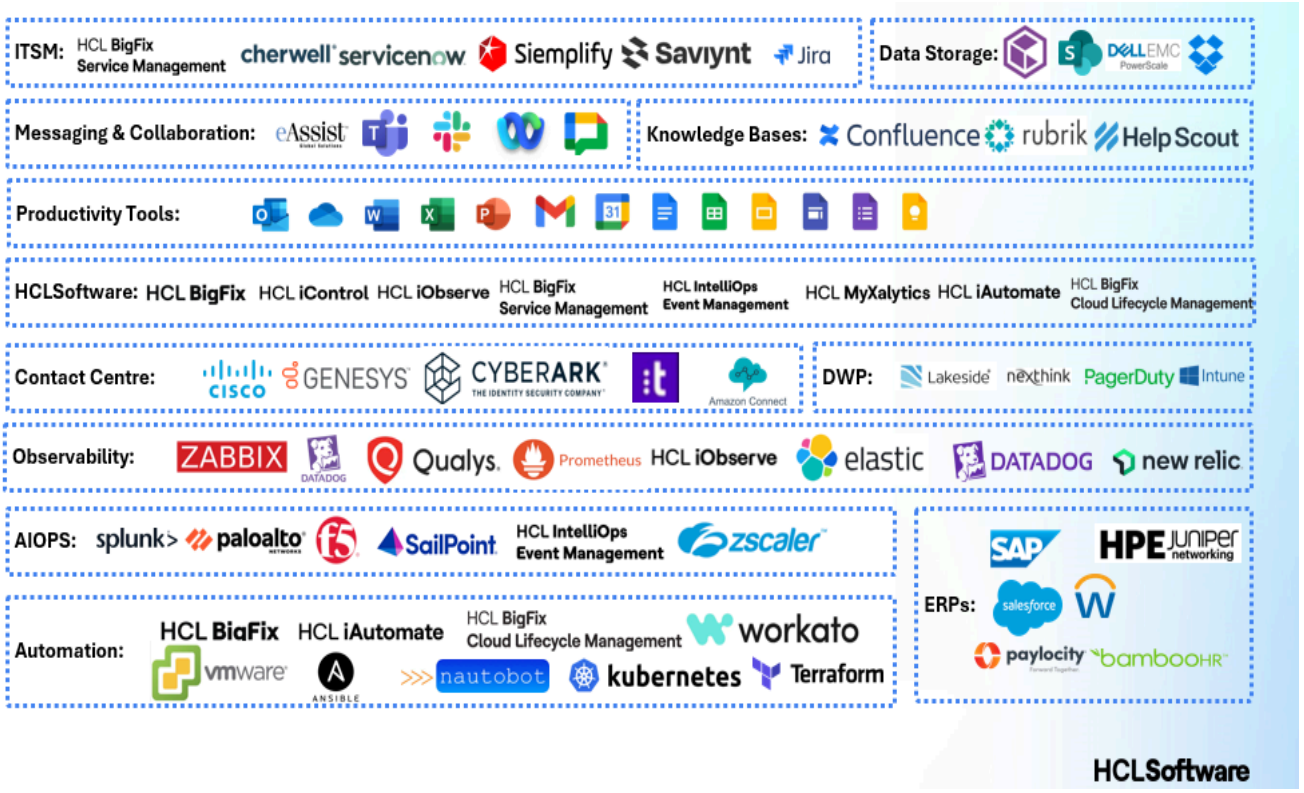
- An at-a-glance dashboard showing how many MCP servers are healthy, unhealthy, or in an unknown state, refreshing automatically every 60 seconds
- A one-click “Check Now” option to instantly re-verify any server’s status on demand
- A direct link to detailed logs for any server, for deeper troubleshooting when needed

Business Impact:
Gives teams early visibility into failing or unreachable MCP servers before they disrupt agent-driven workflows. Reduces downtime and troubleshooting time by making server health visible at a glance and checkable on demand, without digging through logs.

2.12 List of Supported OTB Tools

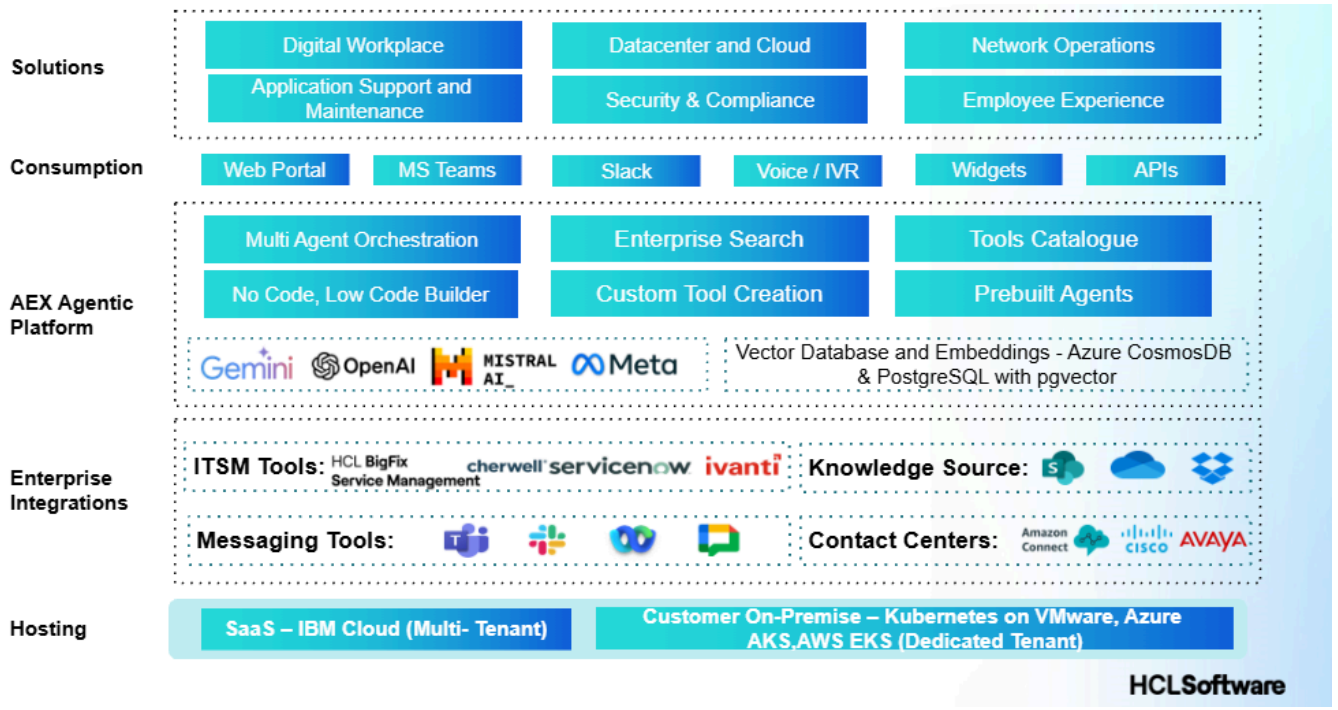
HCL BigFix AEX provides a flexible tool integration framework that enables agents and workflows to connect with enterprise systems through out-of-the-box tools, MCP-based integrations, and custom API integrations. These integrations allow AEX agents to retrieve information, execute actions, automate service requests, trigger workflows, and support cross-system orchestration across IT, HR, productivity, observability, automation, and business application ecosystems.

The tools listed below represent the supported out-of-the-box and feasible integration ecosystem for AEX.



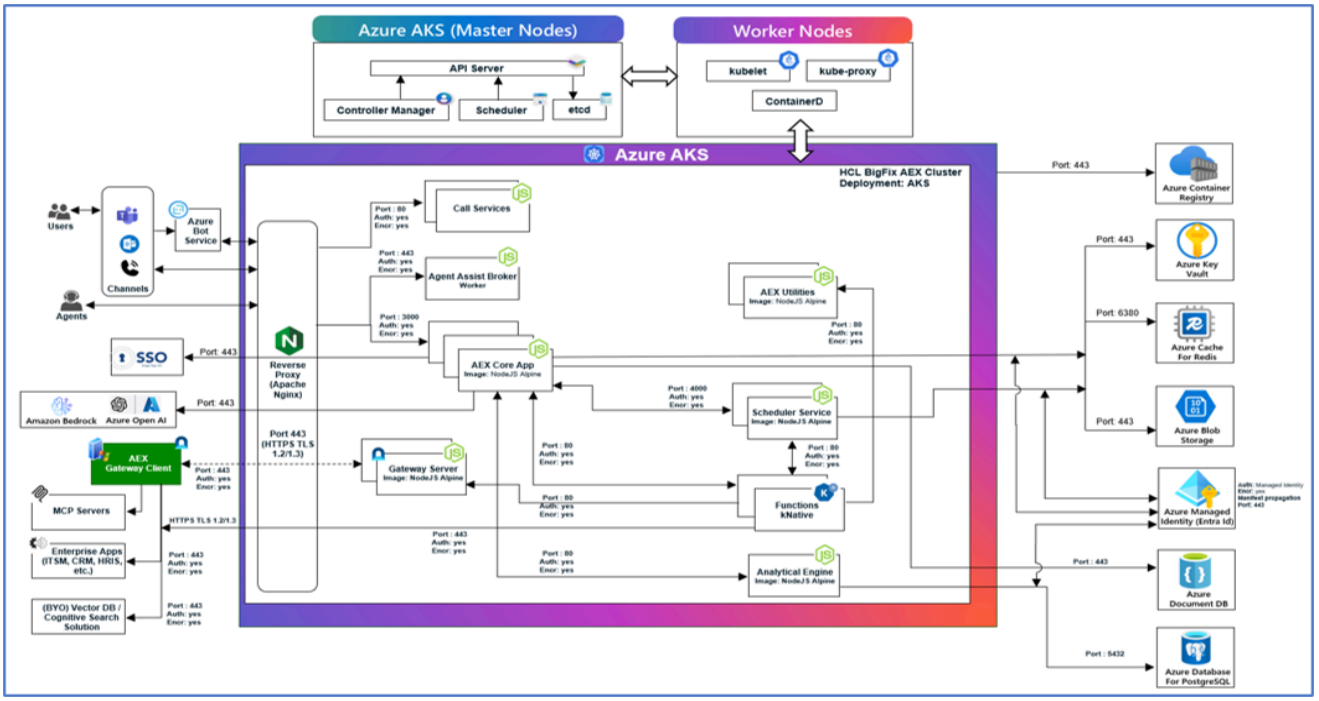
3 HCL BigFix AEX Architecture

3.1 Reference Architecture

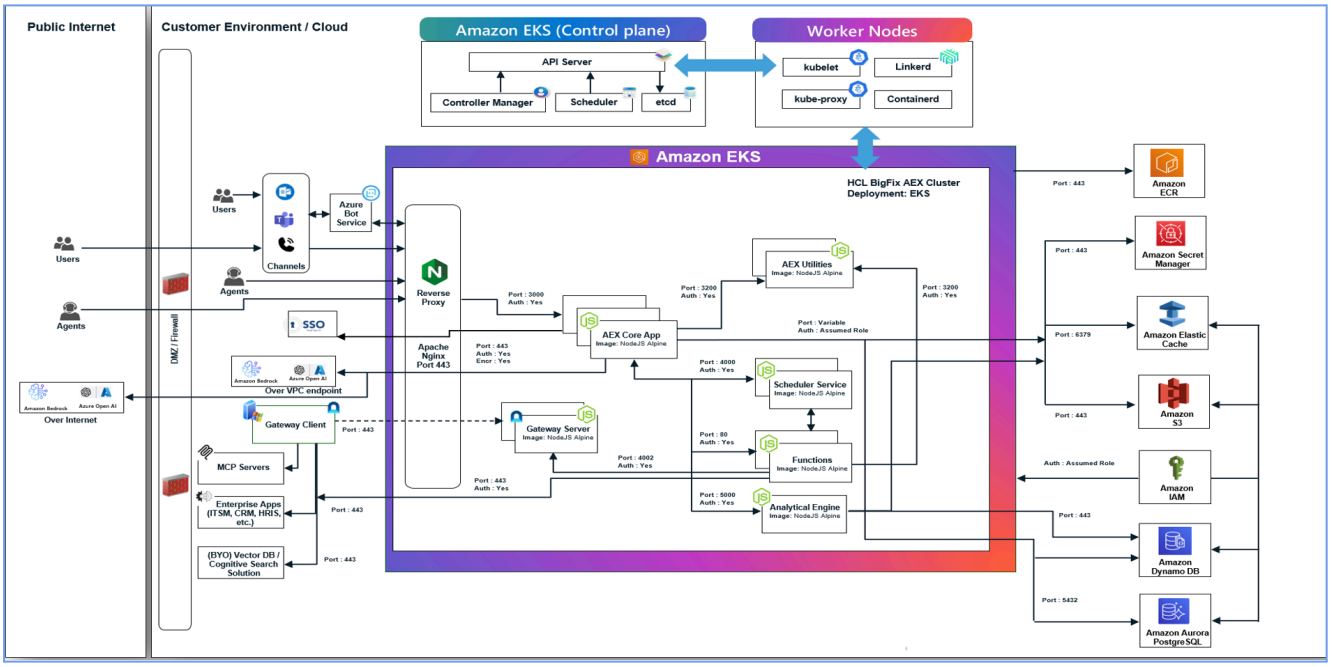


3.2 Deployment Architecture

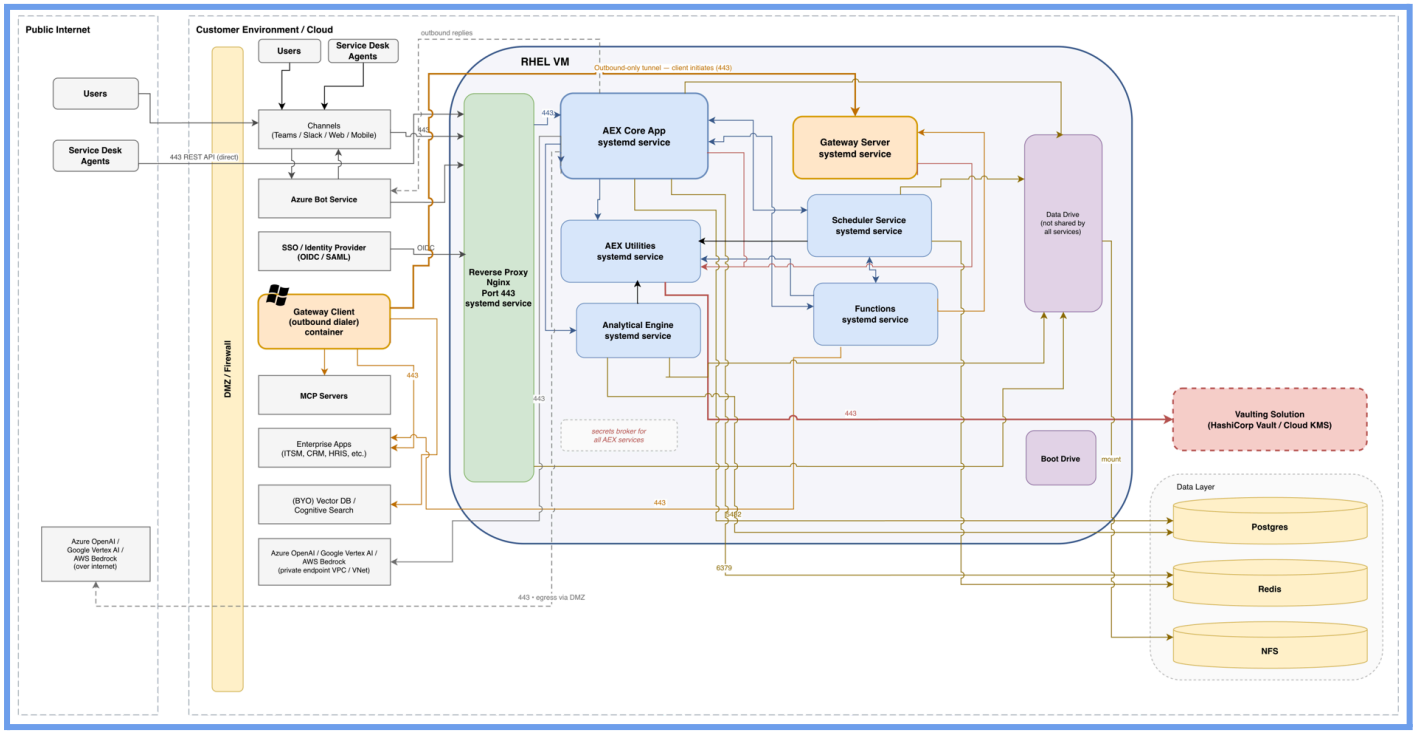
3.2.1 AKS



3.2.2 EKS DEPLOYMENT



3.2.3 VM-BASED DEPLOYMENT



4 Secure Release Checklist and Reports

4.1 Release Checklist

Release Checklist	Criteria	Status	Improvement / Comments
Feature development for current release completed and verified	Pass/Fail	Pass	
Quality objectives have been met for current release (including Functional / Load testing)	Pass/Fail	Pass	95% closure rate for defects
Export Classification with Country specific import requirements completed	Pass/Fail	Pass	
Certificate of Originality Approved	Pass/Fail	Pass	
OneTrust Product Privacy Assessment Approved	Pass/Fail	Pass	
Threat Model and Secure Design Review	Pass/Fail	Pass	
Security Testing - SAST	Pass/Fail	Pass	No Critical/High/Medium issues
Security Testing - DAST	Pass/Fail	Pass	No Critical/High/Medium issues
Security Testing - Pen Testing for OWASP Top 10 for Web and Gen AI	Pass/Fail	Pass	1 Medium & 1 Low issues
Open-Source Vulnerability scanning via Mend	Pass/Fail	Pass	4 High issues tracked under PSIRT Record

Security Hotspot, Code smell and Code quality analysis using SonarQube	Pass/Fail	Pass	A rating for all parameters
Service Description document completed with HCLSW Legal	Pass/Fail	Pass	
New Release Training delivered to PS and support team	Pass/Fail	Pass	
Pricing approvals and CRM part code creation completion	Pass/Fail	Pass	
Marketing activities completion (including GTM collaterals, Launch webinars, Sales enablement sessions etc).	Pass/Fail	Pass	
Online Product documentation and lifecycle page update	Pass/Fail	Pass	

4.2 Packages included in HCL BigFix AEX

This section lists all top level packages included in various components of HCL BigFix AEX along with their license type, version, and description. The current version of nodejs-24 used is 24.18.0-r0.

Component Name	VM Based	AKS, EKS
AEX	88	83
AEX Analytics	22	22
AEX Functions	25	25
AEX Utilities	21	21
Scheduler	24	21
Gateway Client	**NA**	23
Gateway Services	15	15
Total	195	210

4.2.1 AEX

Note: **** Present only in the VM-based package set; not in the EKS/AKS package set.***

License Name	Version	Description	License Type
@a2a-js/sdk	0.3.13	A2A JavaScript SDK / JavaScript library for Agent-to-Agent protocol-based applications	Apache 2.0
@aws-sdk/client-cost-explorer	3.1116.0	AWS Cost Explorer client for JavaScript	Apache 2.0
@aws-sdk/client-dynamodb	3.1116.0	AWS DynamoDB client for JavaScript	Apache 2.0
@aws-sdk/client-ec2	3.1002	AWS EC2 client for JavaScript	Apache 2.0
@aws-sdk/client-lambda	3.1116.0	AWS Lambda client for JavaScript	Apache 2.0
@aws-sdk/client-secrets-manager	3.1043.0	AWS Secrets Manager client for JavaScript	Apache 2.0

@aws-sdk/client-ses	3.1116.0	AWS SES (Simple Email Service) client for JavaScript	Apache 2.0
@aws-sdk/credential-providers	3.700.0	Collection of AWS credential providers for JavaScript	Apache 2.0
@aws-sdk/lib-dynamodb	3.1116.0	DynamoDB document client simplifying attribute value handling	Apache 2.0
@aws-sdk/rds-signer	3.901.0	RDS IAM authentication token signer for JavaScript	Apache 2.0
@azure/arm-compute	22.4.0	Azure Compute Management SDK	MIT
@azure/cosmos	4.5.1	Azure Cosmos DB client library	MIT
@azure/identity	4.8.0	Azure Identity authentication library	MIT
@azure/keyvault-secrets	4.10.0	Azure Key Vault Secrets client library	MIT
@google-cloud/translate	9.1.0	Google Cloud Translation API client	Apache 2.0
@ibm-cloud/cloudant	0.12.0	IBM Cloudant SDK	Apache 2.0
@ibm-functions/iam-token-manager	1.0.3	IAM token manager for IBM Cloud Functions	Apache 2.0
@microsoft/agents-activity	1.7.2	Microsoft 365 Agents SDK activity protocol serialization	MIT
@microsoft/agents-hosting	1.7.2	Microsoft 365 Agents SDK for hosting agents in JavaScript	MIT
@node-saml/passport-saml	5.1.0	SAML authentication strategy for Passport	MIT
@redis/client*	5.11.0	Core Redis client library (used internally by the redis package)	MIT
@redis/entraid	5.11.0	Microsoft Entra ID authentication support for Redis	MIT
@socket.io/redis-adapter	8.2.1	Redis adapter for scaling Socket.IO	MIT
altcha-lib	2.3.2	Library for creating and verifying ALTCHA CAPTCHA challenges	MIT
async	3.2.6	Asynchronous utility functions for Node.js	MIT
aws4	1.13.2	Signs and prepares requests using AWS Signature Version 4	MIT
axios	1.20.0	Promise-based HTTP client	MIT
bcrypt	5.1.1	Password hashing library	MIT
bcryptjs*	2.4.3	Pure JavaScript bcrypt password hashing library	BSD 3-Clause
botbuilder*	4.17.1	Microsoft Bot Framework SDK	MIT
botframework-connector*	4.23.1	Bot Framework connector client	MIT
bullmq	5.81.3	Redis-based queue for messages and jobs	MIT
busboy	1.6.0	Streaming parser for HTML form data	MIT
compression	1.8.1	Node.js compression middleware	MIT
connect-flash	0.1.1	Flash message middleware for Express	MIT
connect-redis	7.1.1	Redis session store for Express	MIT
cookie-parser	1.4.7	Cookie parsing middleware	MIT
cron-validator	1.3.1	Validates cron expressions	MIT
eld	1.0.0	Language detection utility	MIT
email-signature-detector	0.0.6	Email signature detection utility	MIT
express	4.17.3	Web application framework for Node.js	MIT

express-handlebars	9.0.1	Handlebars view engine for Express	BSD 3-Clause
express-session	1.18.2	Session middleware for Express	MIT
form-data	4.0.6	Form data creation library	MIT
generate-password	1.4.2	Password generation utility	MIT
geoip-country	4.1.50	GeoIP country lookup utility	MIT
googleapis	181.0.0	Google APIs client library for Node.js	Apache 2.0
ibm-cloud-sdk-core	5.1.0	Core SDK utilities for IBM Cloud services	Apache 2.0
ibm-cos-sdk	1.15.0	IBM Cloud Object Storage SDK	Apache 2.0
ibmcloud-appid	7.0.0	IBM Cloud App ID SDK	Apache 2.0
joi	18.2.9	Object schema validation library	BSD 3-Clause
jose	5.10.0	JSON Object Signing and Encryption library	MIT
jsonwebtoken	9.0.2	JSON Web Token implementation	MIT
ldapts	9.0.0	LDAP client for Node.js	MIT
lusca	1.6.1	Security middleware for Express	Apache 2.0
markdown-it	14.3.1	Markdown parser	MIT
mime-types	2.1.35	MIME type lookup utility	MIT
mobile-detect	1.4.3	Mobile device detection utility	MIT
module-alias	2.2.2	Module path aliasing utility	MIT
moment	2.30.1	Date and time manipulation library	MIT
mongodb	6.21.0	MongoDB driver for Node.js	Apache 2.0
morgan	1.10.1	HTTP request logger middleware	MIT
mssql	11.0.1	Microsoft SQL Server client for Node.js	MIT
multer	2.1.1	File upload middleware for Express	MIT
nocache	3.0.1	Middleware to disable client-side caching	MIT
nodemailer	10.1.1	Email sending library	MIT
passport	0.6.0	Authentication middleware for Node.js	MIT
password-validator	4.1.1	Password policy validation library	MIT
pg	8.14.1	PostgreSQL client for Node.js	MIT
pg-format	1.0.4	PostgreSQL query formatting utility	MIT
polly-tts	1.0.4	Text-to-speech utility using Amazon Polly	MIT
prom-client*	15.1.3	Prometheus metrics client for Node.js	Apache 2.0
qrcode	1.5.0	QR code generation library	MIT
qs	6.16.1	Query string parsing and stringifying library	BSD 3-Clause
re2	1.27.0	Fast, safe regular expression engine bindings (RE2)	BSD 3-Clause
recursive-readdir	2.2.3	Recursive directory reading utility	MIT
redis	5.12.1	Redis client for Node.js	MIT
slackify-html	1.0.1	HTML to Slack-compatible markdown converter	MIT
slackify-markdown	4.4.0	Markdown to Slack-compatible format converter	MIT
socket.io	4.2.0	Real-time bidirectional event communication library	MIT
socket.io-client	4.2.0	Socket.IO client library	MIT
speakeasy	2.0.0	Two-factor authentication token utility	MIT
striptags	3.2.0	HTML tag stripping utility	MIT

svg-captcha	1.4.0	SVG CAPTCHA generation library	MIT
twilio	4.21	Twilio API client library	MIT
uuid	14.0.0	UUID generation library	MIT
web-push	3.6.7	Web push notification library	MIT
write-excel-file	4.1.1	Library for writing .xlsx Excel files in Node.js or browser	MIT

4.3 AEX Analytics

Library Name	Version	Description	License Type
@aws-sdk/client-dynamodb	3.700.0	AWS DynamoDB client for JavaScript	Apache 2.0
@aws-sdk/client-s3	3.700.0	AWS S3 client for JavaScript	Apache 2.0
@aws-sdk/client-secrets-manager	3.700.0	AWS Secrets Manager client for JavaScript	Apache 2.0
@aws-sdk/credential-providers	3.700.0	Collection of AWS credential providers for JavaScript	Apache 2.0
@aws-sdk/lib-dynamodb	3.700.0	DynamoDB document client simplifying attribute value handling	Apache 2.0
@aws-sdk/rds-signer	3.700.0	RDS IAM authentication token signer for JavaScript	Apache 2.0
@azure/identity	4.13.1	Azure Identity authentication library	MIT
@azure/keyvault-secrets	4.11.2	Azure Key Vault Secrets client library	MIT
@azure/storage-blob	12.31.0	Azure Blob Storage client library	MIT
@ibm-cloud/cloudant	0.12.20	IBM Cloudant SDK	Apache 2.0
aws4	1.13.2	Signs and prepares requests using AWS Signature Version 4	MIT
compression	1.8.1	Node.js compression middleware	MIT
express	4.22.2	Web application framework for Node.js	MIT
gibberish-detective	1.1.1	Detects gibberish strings using Markov-chain analysis	MIT
ibm-cos-sdk	1.15.1	IBM Cloud Object Storage SDK	Apache 2.0
ioredis	6.0.0	Robust, performance-focused Redis client for Node.js	MIT
mongoose	8.24.0	MongoDB object data modeling (ODM) library for Node.js	MIT
node-cron	4.2.1	Job scheduling library for Node.js	ISC
pg	8.21.0	PostgreSQL client for Node.js	MIT
sequelize	6.37.8	Promise-based ORM for SQL databases	MIT
uuid	14.0.0	UUID generation library	MIT
yaml	2.8.3	JavaScript parser and stringifier for YAML	ISC

4.4 AEX Functions

Library Name	Version	Description	License Type
@ibm-cloud/cloudant	0.12.0	IBM Cloudant SDK	Apache 2.0
adaptivecards	3.0.6	Adaptive Cards UI framework	MIT
axios	1.18.1	Promise-based HTTP client	MIT

docx	9.5.1	Library for generating Word (.docx) files in JavaScript	MIT
ejs	3.1.10	Embedded JavaScript templating engine	Apache 2.0
form-data	4.0.6	Form data creation library	MIT
Hucre (replaces exceljs /xlsx)	1.1.0	Zero-dependency spreadsheet engine for reading/writing XLSX, CSV, ODS	MIT
ibm-cloud-sdk-core	5.1.0	Core SDK utilities for IBM Cloud services	Apache 2.0
ibm-watson	10.0.0	IBM Watson services SDK	Apache 2.0
jsonwebtoken	9.0.3	JSON Web Token implementation	MIT
jszip	3.10.1	Create, read and edit ZIP files in JavaScript	MIT
mammoth	1.12.0	DOCX to HTML/text conversion library	BSD 2-Clause
markdown-it	14.2.0	Markdown parser	MIT
moment	2.31.0	Date and time manipulation library	MIT
mongodb	5.6.0	MongoDB driver for Node.js	Apache 2.0
nodemailer	10.0.9	Email sending library	MIT
pdf-parse	1.1.0	PDF text extraction utility	MIT
pptxgenjs	4.0.1	Library for generating PowerPoint presentations in JavaScript	MIT
qrcode	1.5.0	QR code generation library	MIT
qs	6.11.1	Query string parsing and stringifying library	BSD 3-Clause
utf8	3.0.0	UTF-8 encoder/decoder library	MIT
uuid	14.0.0	UUID generation library	MIT

4.5 AEX Utilities

Library Name	Version	Description	License Type
@asciidoctor/core	3.0.0	AsciiDoc processing library for JavaScript	MIT
@aws-sdk/client-s3	3.750.0	AWS S3 client for JavaScript	Apache 2.0
@aws-sdk/client-secrets-manager	3.750.0	AWS Secrets Manager client for JavaScript	Apache 2.0
@azure/identity	4.5.0	Azure Identity authentication library	MIT
@azure/keyvault-secrets	4.9.0	Azure Key Vault Secrets client library	MIT
@azure/storage-blob	12.23.0	Azure Blob Storage client library	MIT
axios	1.20.0	Promise-based HTTP client	MIT
csv-parse	7.0.2	CSV parsing library implementing the Node.js stream API	MIT
express	4.18.2	Web application framework for Node.js	MIT

hucre	1.1.0	Zero-dependency spreadsheet engine for reading/writing XLSX, CSV, ODS	MIT
ibm-cos-sdk	1.15.0	IBM Cloud Object Storage SDK	Apache 2.0
jsonwebtoken	9.0.3	JSON Web Token implementation	MIT
mammoth	1.6.0	DOCX to HTML/text conversion library	BSD 2-Clause
morgan	1.10.1	HTTP request logger middleware	MIT
multer	2.1.1	File upload middleware for Express	MIT
officeparser	7.5.1	Library for parsing and extracting text from office files	MIT
pdf-parse	2.2.2	PDF text extraction utility	MIT
sendmail	1.6.1	Sends email without setting up an SMTP server	MIT
tesseract.js	6.0.0	OCR library for image text extraction	Apache 2.0
turndown	7.1.0	Converts HTML into Markdown	MIT
turndown-plugin-gfm	1.0.2	Turndown plugin adding GitHub Flavored Markdown support	MIT

4.5.1 Scheduler

Note: * ***Present only in the VM-based package set; not in the EKS/AKS package set.***

Library Name	Version	Description	License Type
@aws-sdk/client-dynamodb	3.1116.0	AWS DynamoDB client for JavaScript	Apache 2.0
@aws-sdk/client-secrets-manager	3.1116.0	AWS Secrets Manager client for JavaScript	Apache 2.0
@aws-sdk/credential-providers	3.1116.0	Collection of AWS credential providers for JavaScript	Apache 2.0
@aws-sdk/lib-dynamodb	3.1116.0	DynamoDB document client simplifying attribute value handling	Apache 2.0
@aws-sdk/rds-signer*	3.1150.0	RDS IAM authentication token signer for JavaScript	Apache 2.0
@azure/identity	4.6.0	Azure Identity authentication library	MIT
@azure/keyvault-secrets	4.10.0	Azure Key Vault Secrets client library	MIT
@ibm-cloud/cloudant	0.12.3	IBM Cloudant SDK	Apache 2.0
aws4	1.13.2	Signs and prepares requests using AWS Signature Version 4	MIT
axios	1.20.0	Promise-based HTTP client	MIT
bull	4.11.5	Redis-based queue for handling distributed jobs	MIT
fastify	5.7.4	Fast and low overhead web framework for Node.js	MIT
ibm-cloud-sdk-core	5.3.2	Core SDK utilities for IBM Cloud services	Apache 2.0
jsonwebtoken	9.0.2	JSON Web Token implementation	MIT
module-alias	2.2.2	Module path aliasing utility	MIT
mongodb	7.6.0	MongoDB driver for Node.js	Apache 2.0
nodemailer	10.1.1	Email sending library	MIT
openwhisk	3.21.4	JavaScript client library for the Apache OpenWhisk platform	Apache 2.0
pg*	8.22.0	PostgreSQL client for Node.js	MIT

pg-format*	1.0.4	PostgreSQL query formatting utility	MIT
qs	6.11.2	Query string parsing and stringifying library	BSD 3-Clause
socket.io-client	4.8.3	Socket.IO client library	MIT
twilio	6.1.1	Twilio API client library	MIT
uuid	14.0.2	UUID generation library	MIT

4.6 Gateway Services

Library Name	Version	Description	License Type
@aws-sdk/client-secrets-manager	3.700.0	AWS Secrets Manager client for JavaScript	Apache 2.0
@aws-sdk/credential-providers	3.700.0	Collection of AWS credential providers for JavaScript	Apache 2.0
@azure/identity	4.0.0	Azure Identity authentication library	MIT
@azure/keyvault-secrets	4.7.0	Azure Key Vault Secrets client library	MIT
@redis/entraid	6.2.1	Microsoft Entra ID authentication support for Redis	MIT
@socket.io/redis-adapter	8.2.1	Redis adapter for scaling Socket.IO	MIT
async	3.2.0	Asynchronous utility functions for Node.js	MIT
aws4	1.13.2	Signs and prepares requests using AWS Signature Version 4	MIT
axios	1.15.2	Promise-based HTTP client	MIT
ejs	3.1.5	Embedded JavaScript templating engine	Apache 2.0
express	4.15.2	Web application framework for Node.js	MIT
qs	6.16.1	Query string parsing and stringifying library	BSD 3-Clause
redis	4.7.0	Redis client for Node.js	MIT
socket.io	4.8.3	Real-time bidirectional event communication library	MIT
uuid	14.0.0	UUID generation library	MIT

4.6.1 Gateway Client (only on EKS, AKS)

Library Name	Version	Description	License Type
@modelcontextprotocol/sdk	1.32.1	Model Context Protocol implementation for TypeScript	MIT
@selfheal/ad-library	1.0.0 (local)	Internal self-heal Active Directory library (bundled as a local tarball, not published to npm)	Internal/Proprietary
archiver	5.3.1	A streaming interface for archive generation	MIT
axios	1.15.2	Promise based HTTP client for the browser and node.js	MIT
body-parser	1.20.0	Node.js body parsing middleware	MIT
ejs	3.1.5	Embedded JavaScript templates	Apache-2.0
ejs-electron	3.0.0	A lightweight module for ejs templating in an Electron app	MIT
electron-alert	0.1.20	SweetAlert2 for Electron applications	MIT
electron-log	5.1.1	A simple logging module for Electron applications	MIT
electron-updater	6.3.0	Cross-platform auto-updater for Electron applications	MIT

express	4.18.1	Fast, unopinionated, minimalist web framework for Node.js	MIT
form-data	4.0.0	A library to create readable multipart/form-data streams	MIT
https-proxy-agent	7.0.6	An HTTP(S) proxy http.Agent implementation for HTTPS	MIT
jquery	3.6.1	JavaScript library for DOM operations	MIT
kafkajs	2.2.4	A modern Apache Kafka client for Node.js	MIT
level	10.0.0	Universal abstract-level database for Node.js and browsers	MIT
module-alias	2.3.4	Create aliases of directories and register custom module paths	MIT
ncp	2.0.0	Asynchronous recursive file copy utility	MIT
qs	6.16.1	A querystring parsing and stringifying library	BSD-3-Clause
socket.io-client	4.8.1	Realtime application framework client	MIT
uuid	14.0.2	RFC4122 (v1, v3, v4, v5) UUIDs	MIT
winston	3.3.3	A logger for just about everything	MIT
winston-daily-rotate-file	5.0.0	A transport for winston which logs to a rotating file each day	MIT

4.7 HCL AppScan SAST Reports (AKS, EKS, VM-Based)

4.7.1 SAST Report - AEX

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

HCL AppScan SAST Results	
Critical	0
High	0
Medium	0
Low	0
Informational	0
Total	**0**

4.7.2 SAST Report - Scheduler

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

HCL AppScan SAST Results	
Critical	0
High	0
Medium	0
Low	0
Informational	0
Total	**0**

4.7.3 SAST Report - AEX Analytics

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

HCL AppScan SAST Results	
Critical	0
High	0
Medium	0
Low	0
Informational	0
Total	**0**

4.7.4 SAST Report - AEX Functions

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

HCL AppScan SAST Results	
Critical	0
High	0
Medium	0
Low	0
Informational	0
Total	**0**

4.7.5 SAST Report - AEX Utilities

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

HCL AppScan SAST Results	
Critical	0
High	0
Medium	0
Low	0
Informational	0
Total	**0**

4.7.6 SAST Report - AEX Gateway Services

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

HCL AppScan SAST Results	
Critical	0
High	0
Medium	0
Low	0
Informational	0
Total	**0**

4.7.7 SAST Report - AEX Gateway Client (EKS, AKS)

No security vulnerabilities were found in the SAST Report, as detailed in the table below.

HCL AppScan SAST Results	
Critical	0
High	0
Medium	0
Low	0
Informational	0
Total	**0**

4.8 HCL AppScan DAST Reports (AKS, EKS, VM-Based)

4.8.1 DAST Report - AEX Web

No security vulnerabilities were found in the DAST Report, as detailed in the table below.

HCL AppScan DAST Results	
Critical	0
High	0
Medium	0
Low	0
Informational	0
Total	**0**

4.9 Mend Security Reports (AKS, EKS, VM-Based)

The Mend Scan identified four high severity security issues (PRB0180261, PRB0180262, PRB0180263, PRB0180261). Security exception has been approved.

Mend Security Results	
Critical	0
High	4
Medium	0
Low	0
Informational	0
Total	**4**

4.10 Security Penetration Testing Report

For Current release HCLSW Security Team conducted Penetration Testing for all the components of HCL BigFix AEX v14 based on OWASP Top 10 guideline for Web and Gen AI.
The two vulnerabilities found during the penetration testing are being carried forward with this release (PRB0177663- Medium, PRB0177668 -Low).

External Security Penetration Testing Results	
Critical	0
High	0
Medium	01
Low	01
Informational	0
Total	**02**

4.11 PSIRT Details

As part of HCL Software Product Security Incident Response (PSIRT) process, for current release 2 PSIRT records were created for Security issues. Following is the description of PSIRT ID.

Issue id	Source	Issue Description
CVE-2026-93687 (High Severity)	Mend Scan	braces@3.0.3 package Vulnerability detected in the HCL BigFix AEX Risk is contained because ibmcloud-appid only processes trusted Enterprise AD SAML 2.0 flows, with WAF and schema-validation controls blocking any malformed input, making the exploit path unreachable. .
PRB0170901 (High Severity)	Mend Scan	http-cache-semantics package Vulnerability detected in the HCL BigFix AEX Risk is contained because ibmcloud-appid communicates only with trusted Enterprise AD endpoints and ignores client-supplied cache headers, with ingress WAF filtering and egress allow-listing providing further protection.
PRB0169924 (High Severity)	Mend Scan	sift package Vulnerability detected in the HCL BigFix AEX Code review confirmed no reachable exploit path, as the vulnerable mongoose feature is unused and no user-supplied data can reach the affected code.
PRB0180261 (High Severity)	Mend Scan	Zod package Vulnerability detected in the HCL BigFix AEX Risk is contained because Bot Framework JWT authentication validates every request before it reaches the parser, so unauthenticated callers can never reach the vulnerable code path.

4.12 Load Testing Reports

As part of the current release load testing was performed using HCL OneTest tool and HCL Playwright K6 tool. Following table provides the details around same:

Module Name	Maximum User Count Against Which Test Case Passed	Results
Login – LUMS Authentication	200 users	Average response time for all pages: 4.015s (5 users/ second ramp up)
Ticket creation using ServiceNow Tool	200 users	Average response time for all pages: 3.485s (5 users/ second ramp up)
Agent Assist Chat Interaction	40 users	Average response time for all pages: 23s (5 users/ second ramp up)
Knowledge Search	1000 users	Average response time for all pages: 38.75s (5 users/ second ramp up)

5 Application Security Controls

Control	Description
Data at rest and in transit encryption	• Data in Transit: All communication between users, services, and external systems is encrypted using HTTPS TLS 1.2/1.3. • Data at Rest: AES-256 encryption standards
Authentication & Authorization	• Single Sign-On (SSO): User authentication is managed via SSO, integrating with Customer provided enterprise Identity Providers (e.g., ADFS, Azure AD, Okta, PingFederate) 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, either through API keys (e.g., Azure OpenAI) or OAuth 2.0 (e.g., IBM Watson).
Content Filtering & Prompt Validation (using Azure, AWS and GCP native content filtering service)	• 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. • Runtime Safeguards: Input and output safeguards help enforce scope, confidentiality, and safe response behaviour during agent execution.
Security Testing	• 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.
Secure Gateway	• Integrates seamlessly within the customer's on-premise environment. • Routes all communication through a secure, encrypted tunnel. • Uses end-to-end encryption to protect internal and external interactions from interception.
Responsible AI - Risk & Incident Management	• Conducts an AI Risk Assessment for every major release. • Maintains structured processes for identifying, reporting, and resolving AI-related security incidents. • Kill Switch & Controlled Operations supports rapid disablement of misbehaving agents through kill switch / agent state controls to reduce operational risk.
Responsible AI - Human Oversight	• Incorporates human-in-the-loop workflows for sensitive or high-impact agent actions. • Provides safeguards to maintain operational safety during agent execution.
Responsible AI - PII Protection	• Follows a "purposeful, limited, and minimized" approach for handling PII. • Redaction Console provides a central, rule-based engine for detecting and redacting sensitive data with each rule has a configurable type, pattern, action, and on/off status, editable at any time. • Built-in Rule Library allows common personal-data protections to be imported in a few clicks, alongside support for fully custom rules with configurable match thresholds. • Processes only the minimal data required for operational needs.

	• Allows display of a customizable banner to notify users not to provide or prompt any sensitive/PII data when interacting with AI agents.
Responsible AI - Accuracy & Transparency	• Supports tuning of AI hyperparameters to improve accuracy and groundedness. • Promotes transparency and clarity in AI-driven workflows. • Provides visibility into agent execution flow, including conversation steps, tool calls, and outcomes.
Security Testing - AI-Assisted Function Safety Validation	• Every saved JavaScript function is automatically reviewed by an LLM for security and structural risks, such as hardcoded credentials or incomplete logic, before it is marked Safe. • Risky code triggers a warning at save time; users may proceed only via an explicit override, which is logged rather than silently permitted. • Every override is recorded with the user, timestamp, and the specific reason the code was flagged, supporting post-hoc security review.
Traceability, Auditability & Observability	• Provides execution transparency across conversation turns, tool calls, outcomes, and timelines. • Supports step-level payload inspection and auditability for governance, troubleshooting, and investigations. • Enables operational monitoring of agent behaviour and execution flow. • Maintains a full Changelog per function, recording every code change, the safety verdict, the validating model, and any override history, with a side-by-side diff of what changed. • MCP Server Health Monitoring gives continuous visibility into MCP endpoint availability (color-coded health status, auto-refreshing every 60 seconds), so failures in agent tool-calling workflows are surfaced proactively rather than discovered after the fact.
Guardrails	• Multi-Layer Guardrails architecture is applied across knowledge ingestion, runtime input/output handling, and agent execution to help enforce safe, scoped, and policy-aligned behaviour • Guardrails help restrict agents to their intended domain, reduce unsafe or unauthorized actions, and support grounded responses. • Runtime Protection via Input and output safeguards help detect unsafe prompts, protect confidential information, and prevent restricted or non-compliant responses from reaching users. • Guardrails work together with tool authorization, traceability, and approval controls to support operational governance .
Compliance Attestation	The HCL BigFix AEX platform has the following compliance certification/attestation available for SaaS: • ISO 27001 • ISO 27034 • SOC 2 Type II • SOC 3

6 Known Issues

The v14 release of HCL BigFix AEX has the following issues categorized by severity:

- Critical Severity: 0 Issues
- High Severity: 0 Issues
- Medium Severity: 5 Issues
- Low Severity: 0 Issues

Issue ID	Severity	Issue Description
23570	Low	**Gateway>** The validation message displayed by the application is unclear and not user-friendly, making it difficult for users to understand the issue and take appropriate action. **RCA**- When the MCP server returns a non-2xx response, its raw HTML error body is passed through as-is instead of being converted into a readable error message, so the user sees unformatted HTML rather than a clear description of the failure.
23567	Low	**LDAP>** When user enable show domain selector and add domain mapping and save it, then the login page UI is breaking. **RCA-** This will be taken as UI enhancement request for next fix release.
23451	Low	**Gateway->** Gateway theme preference is not maintained after relaunch and changes unexpectedly during navigation **RCA**- The saved theme is only applied to the first screen after launch; subsequent screens read from a separate in-session store that isn't updated on relaunch, so navigating away from the first screen reverts the theme to the default until it's toggled manually.
23668	Medium	**VM based Env > Workflows-** Workflows are not deleting, getting success message, post reload workflows appears back in list, working in EKS **RCA**- Soft delete logic was built for Cloudant's single-collection model, which separates documents by a doc_type field; since PostgreSQL uses a separate table per doc_type, the queries weren't routing to the correct table and the operation failed until the logic was updated to target the right table.
23484	Medium	**General Instructions>** Getting error "Failed to fetch models. Please try again." and console strucks in processing state when no genai subscription is available. **RCA-** When an active GenAI subscription is missing, the system fails to handle the empty subscription state gracefully during model list retrieval.

7 Looking Forward

Looking ahead, AEX v15 is expected to further strengthen the platform's governance, knowledge management and agent-building experience for enterprise teams. The next release is focused on giving administrators central control over models, policies and guardrails, while making it easier for builders to create agents, ground them in trusted knowledge and measure results.

Key areas of focus include:

- **LLM Gateway and Budget Controls** - A central gateway for model access across agents, tools and workflows, with routing, policy enforcement and model expiry information. Token usage tracking, budgets and breach notifications help teams keep model spend in check.
- **AEX Policies** - A centralized policy console to define and enforce governance rules across agents, tools, workflows, projects and environments, using conditions, approvals and effective dates, with audit visibility.
- **Guardrails Enhancements** - A central console within Governance to apply out-of-the-box guardrails and configure custom guardrails across multiple agents.
- **AI Observability** - Unified observability across agents, available through APIs, to support audit and trust and to speed up root-cause analysis.

- **AEX Companion** - Create agents and workflows from natural-language prompts, making creation easier and reducing dependency on subject-matter experts.
- **Skills Framework for Agents** - Create, version and assign bundled skill packages (instructions, reference documents and scripts) to specific agents, tenants or use cases, for governed and reusable capabilities.
- **Knowledge Management Studio Enhancements** - Configure end-to-end ingestion pipelines in one console, including chunking strategies, embedding models, hybrid and semantic retrieval, image OCR and vision parsing, more media formats and AEX workflow sync. Retrieval configuration and support for custom vector databases through AEX workflows help improve accuracy on complex queries.
- **Knowledge Governance and Monitoring** - Document management with a status for each document, an audit console for reviewing detected personal data before indexing, an organization-wide audit trail, an index monitor for vector database health and capacity, and a search simulation to test retrieval results.
- **Gateway Enhancements** - The Gateway console moves into AEX with operational improvements. IP allow-listing restricts access to approved ranges, and Linux support enables Linux VMs and containerized deployments.
- **Enhanced Agent Assist** - A refreshed interface for the Desk, Supervisor and Admin dashboards, multi-desk assignment with automatic desk switching, downloadable chat transcripts for audit, real-time language translation settings at supervisor and desk level, larger queues, more consistent ticket assignment, and enhanced search and export in Cognitive Analytics.
- **Analytics and Reporting** - Conversation intelligence with a configurable KPI builder, a view of tickets resolved by AEX compared with human agents, richer ITSM ticket details, and additional KPIs and reporting improvements.
- **Voice** - Voice agents can run on edge or on-premises small language models for low-latency, cost-efficient and data-resident deployments. Voice analytics covers topics, sentiment and quality assurance.
- **Chat Experience** - A new chat theme with an improved experience, pre-built adaptive-card response templates for consistent, branded responses, and a video avatar agent experience for websites.
- **Agent Marketplace** - A storefront of pre-built, out-of-the-box agents that can be pushed to the library, helping teams get to value faster.
- These upcoming capabilities are designed to strengthen AEX as a foundation for secure, governed and scalable agentic operations in enterprise environments.

Disclaimer: This roadmap is intended to outline general product direction. This roadmap is intended for information purposes only and may not be incorporated into any contract. These documents are not a commitment to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for HCL BigFix AEX product remains at the sole discretion of HCLSoftware.

8 Blocked Packages

As part of ongoing security hardening, the following Node.js built-in/core modules have been blocked from use within the product runtime.

1. os
2. child_process
3. cluster
4. process
5. fs
6. readline
7. net
8. dgram

9. dns
10. tls
11. http
12. https
13. http2
14. worker_threads
15. repl
16. vm
17. v8
18. inspector
19. module
20. import
21. async_hooks
22. perf_hooks
23. diagnostics_channel
24. trace_events
25. wasi
26. sqlite
27. domain
28. path
29. events
30. util
31. zlib
32. string_decoder
33. punycode
34. querystring
35. assert
36. constants
37. timers
38. sys

HCLSoftware