TECHNICAL WHITE PAPER

# HP Intelligent Transformation security

## CONTENTS

## OVERVIEW

HP Intelligent Transformation enables organizations to create sustainable, often game-changing innovations based on a complete view of the people, systems, and processes within their organization.

This software uses powerful visualization and engaging techniques to draw out the needs of users and brings into focus where to act and why. As a team utilizes the application, it builds out personas across a service or business and creates detailed blueprints and value maps, which highlight issues, duplication, inefficiency, and bias. The software also helps the delivery team develop actionable options from HP's portfolio to move to digitized workflows.

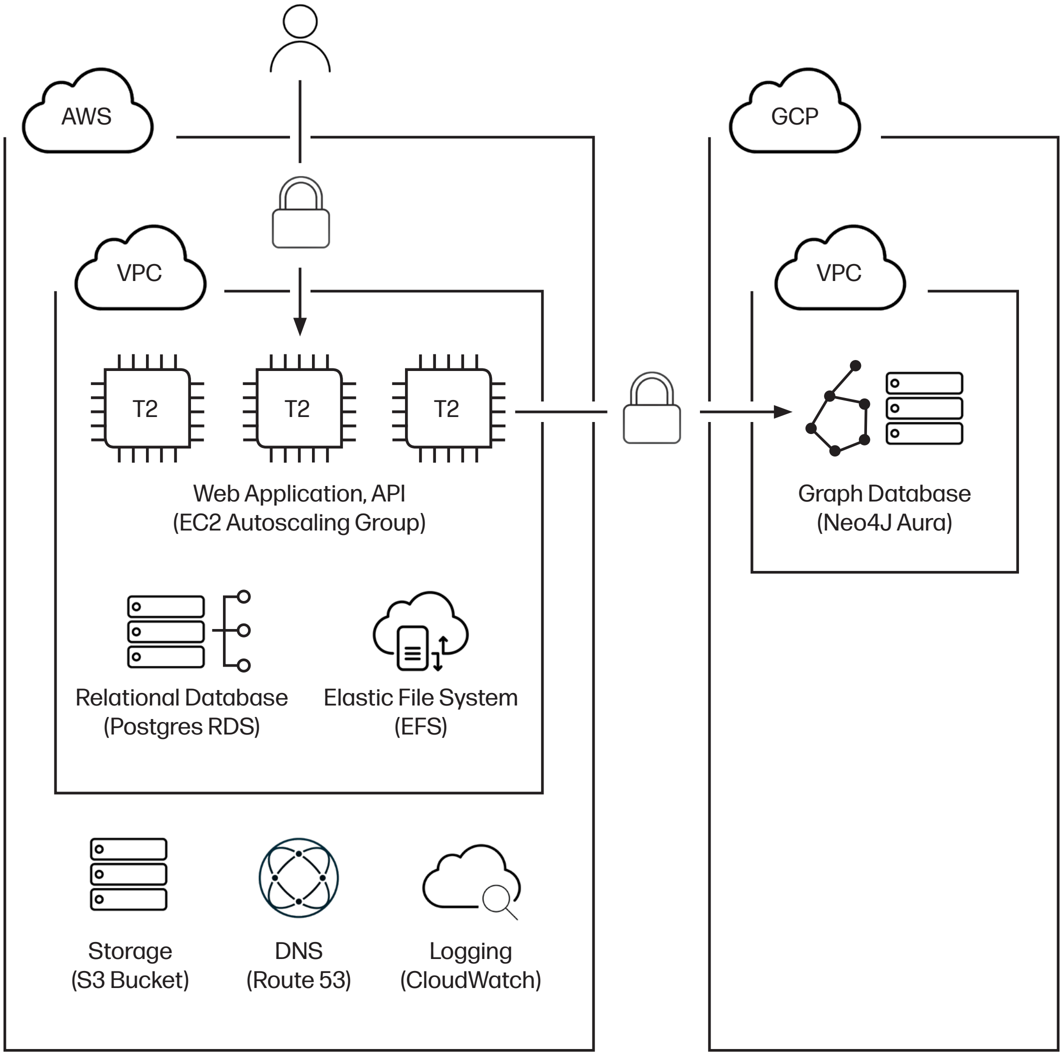
## SERVICE

HP Intelligent Transformation is a multi-tenant SaaS application hosted on Amazon Web Services (AWS).[1] It consists of a modern React single-page web application (SPA) communicating through an authenticated GraphQL API running on a NodeJS server.

The application currently utilizes two database systems—PostgreSQL and Neo4J.[2] PostgreSQL is hosted and managed within Amazon RDS. The Neo4J[2] graph database is hosted and managed by Neo4J[2] Aura within the Google Cloud Platform™.

All network traffic ingress is handled by Nginx servers running within our AWS[1] instance, which are used to route traffic to the system.

Asset/file storage is on Amazon EFS, managed by Amazon.



HP Intelligent Transformation system diagram

## SECURE COMMUNICATION

HP Intelligent Transformation software utilizes Amazon's Elastic Beanstalk deployment architecture. Each component in the software stack is in an isolated Docker container deployed using Amazon Elastic Compute (EC2) instances. EC2 instances maintain current patching against evolving security threats. EC2 instances are also deployed with malware detection sensors.

All communication to the service is secured using transport layer security (TLS) version 1.2. TLS 1.2 uses 2048-bit level encryption and certificate validation to establish a secure channel. Older versions of TLS 1.1 and 1.0 are not supported.

The back-end application is a NodeJS web server running within a Docker container, with minimal priority and only exposing port 80 accessible by the Nginx network ingress. All major application components are separated into their own respective Docker containers to ensure isolation and only exposing the necessary ports to function.

HP Intelligent Transformation currently supports username/password authentication. Authentication is done using JWT-based authentication with an 8-hour time-based revocation. User passwords are stored hashed in the database using the bcrypt algorithm with random salt.

Single sign-on integrations with identity providers such as Microsoft® Azure AD, Google™ Identity, or HP-ID will be supported in the future.

No system passwords or secrets are stored directly within the web application source code or build bundles. All system passwords are injected securely via environment variables into their respective Docker containers.

Access to systems is limited to specific individuals and we require multi-factor authentication for system access. We utilize Amazon IAM roles for access and permissions and enforce a least privilege permission model. Administrative users and access keys are reviewed on a schedule and rotated to ensure security.

All code is minimized and obfuscated as part of our CI/CD application build process.

Third-party penetration testing is performed regularly as part of our System and Organization Controls (SOC) 2 compliance certification. The penetration tests performed are a gray box assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those catalogued in the Open Web Application Security Project (OWASP).[3] The assessment also includes a review of security controls and requirements listed in the OWASP[3] Application Security Verification Standard (ASVS).

We use cookies to make the application usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

## CLIENT PLATFORMS

The service is accessed using a desktop or mobile web browser. HP Intelligent Transformation will support the last three recent versions of Google Chrome™, Firefox, Microsoft Edge®, and Apple® Safari® web browsers.

## DATA STORAGE

The PostgreSQL database is hosted on Amazon RDS, which manages access permissions and secure backups. PostgreSQL is part of a secure virtual private cloud (VPC) that is only accessible by the HP Intelligent Transformation application. Database credentials are injected via secure environment variables into the application's Docker container. Database backups are encrypted at rest in a private AWS[1] S3 bucket. Note: The Postgres database will be decommissioned in the future.

The Neo4J[2] database is hosted on Neo4J[2] Aura within the Google Cloud Platform. Aura manages access permissions and secure encrypted database backups. All communication between the GraphQL API and the Neo4J[2] graph database service in GCP is secured using transport layer security version TLS 1.2.

File storage is managed through Amazon EFS mounts to the application Docker containers. The EFS mount is encrypted and only accessible to the HP Intelligent Transformation application via a secure Amazon VPC. File management is isolated by tenant.

## PORT REQUIREMENTS

The only access to the application is via the network ingress on the load balancers, which only expose port 443 for secure HTTPS communication using SSL certificates.

## DATA COLLECTION AND PERSONALLY IDENTIFIABLE INFORMATION (PII)

HP Intelligent Transformation requires users to provide the following information in order to use the service:

- First name
- Last name
- Email address
- Password

We automatically collect the following telemetry data for system monitoring and debugging purposes:

- IP address
- Operating system and version
- Browser version

As part of the application's function, generalized questions are asked about the user's relationship to a specific product or service. No questions are asked that request personally identifiable information.

The web application assumes a low security browser environment. No sensitive personally identifiable information (PII) is stored on the browser client.

## SCALABILITY AND RELIABILITY

HP Intelligent Transformation is designed as a scalable architecture with a deployment model capable of responding to increased traffic and usage spikes. Leveraging Amazon's elastic compute capabilities, we can automatically and proactively deploy additional resources to meet rising demand.

Neo4J[2] database instances can be scaled from 1 GB memory/1 CPU/2 GB storage to 384 GB memory/24 CPU/256 GB Storage. Databases can be resized at any time with zero downtime.

## PASSWORD REQUIREMENTS AND STORAGE

User access credentials include a unique email address (with validated owner control) and a minimum 8-character password, adhering to a 64-bit level of entropy (STRONG level).

SSO integration with identity providers such as Microsoft Azure AD, Google Identity, or HP-ID are planned. Password requirements will be managed by the individual identity provider under those circumstances.

## LOGS

System logs are kept on usage, function, and access. The logs are reviewed as necessary when determined by issue reports, service management, and/or automated service monitors.

## PRIVACY POLICY

To learn more about the HP privacy policy, visit hp.com/us/en/privacy/privacy.html.

## CUSTOMER INFORMATION ACCESS

Access to PII and/or customer information is limited to HP Intelligent Transformation product team members, comprised of HP and HP's development partner. Access is limited on a need-to-know basis.

[1] For more information, see aws.amazon.com/security.

[2] For more information, see neo4j.com/cloud/security.

[3] For more information, see owasp.org/www-project-top-ten/.

© Copyright 2022 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Apple and Safari are registered trademarks of Apple Inc. Google, Google Cloud Platform, and Google Chrome are trademarks of Google Inc. Microsoft and Microsoft Edge are U.S. registered trademarks of the Microsoft group of companies.

4AA8-1838ENW, July 2022