HighQ Hosting & Security Technical Whitepaper

VERSION 3.1.2

February 2021

Michael Hall

CONFIDENTIAL

Subject to NDA

HighQ Part of Thomson Reuters

the answer company™ THOMSON REUTERS®

Contents

Introduction to HighQ Security

Business is becoming globalized. Companies deal with clients all over the world and have offices in multiple locations. People need to share large, sensitive documents with one another instantly. They need to communicate in the open with colleagues in different offices. They need to work with external collaborators seamlessly and securely.

MAKING THE CLOUD WORK FOR YOU

Tools that enable efficient and secure remote collaboration and communication are in demand across most industries. Cloud collaboration provides these tools. This technology enables globally dispersed colleagues to work together within the same system. Colleagues anywhere in the world can work on the same documents, share files and communicate with one another through a cloud collaboration platform, unimpeded by physical location.

Working in the cloud enables collaboration between internal and external parties without any concerns about security, compatibility and excessive administration involved with using two or more systems. Companies can communicate with customers, suppliers or business partners through a cloud collaboration platform just as easily as they could if they were internal to the company.

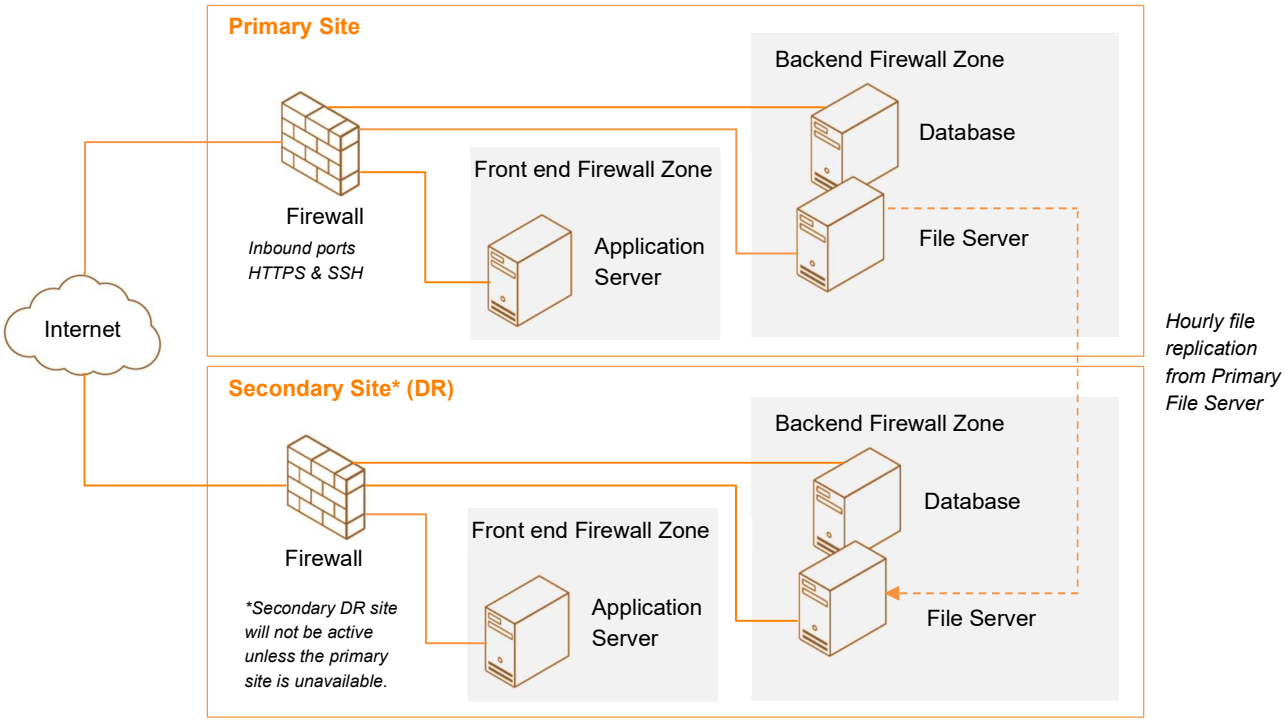
INDUSTRY LEADING SECURITY

Any cloud platform will store your organisation's content and potentially your clients' content too. You can't take any risks when it comes to guaranteeing the security of a chosen provider.

By selecting the HighQ platform, you have chosen a cloud provider that is fully audited and accredited to meet information security standards. HighQ is ISO27001 certified, which ensures the controls and processes are in place to protect your data. It's important to note that the vendors themselves must be accredited, not just their data center. We have robust security measures including advanced encryption, data back-up and a fully redundant infrastructure to guarantee uptime. We also offer single-tenancy hosting, single jurisdiction hosting and perform independent penetration tests on the platform.

SECURITY ARCHITECTURE OVERVIEW

The HighQ platform provides a variety of tools and features that you can use to keep your information safe from unauthorized use. This includes credentials for access control, HTTPS endpoints for encrypted data transmission, the creation of separate IAM user accounts and user activity logging for security monitoring. This paper outlines our approach to security and compliance for the HighQ products and will focuses on security including details on organizational and technical controls regarding how HighQ protects your data and details on compliance and how you can meet regulatory requirements.



Thomson Reuters Security Culture

Thomson Reuters and HighQ have always had security at the core of everything we do. This ethos of secure working fits will as part of Thomson Reuters inclusive security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and in company-wide events to raise awareness.

EMPLOYEE BACKGROUND CHECKS

Before they join, Thomson Reuters will verify an individual's education and previous employment, and perform internal and external reference checks. Where local law or statutory regulations allow, Thomson Reuters will also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position and geographical location.

SECURITY TRAINING FOR ALL EMPLOYEES

All Thomson Reuters employees undergo security training as part of the onboarding process and receive ongoing security training throughout their careers. New employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure, and complete a mandatory security and data protection course. Depending on their job role, additional training on specific aspects of security may be required. Our software engineers also attend technical presentations on security-related topics such as OWASP and secure coding practices.

OUR SECURITY TEAM

Thomson Reuters has a large global Information Security Risk Management (ISRM) team of 165 employees. This team is tasked with maintaining the company's defence systems, developing security review processes, building security infrastructure and implementing Thomson Reuters security policies. The dedicated security team actively scans for security threats using commercial and custom tools, penetration tests, audits and compliance reviews.

The ISRM team review security plans for all networks, systems and services. They provide project-specific consulting services to our product and engineering teams. They monitor for suspicious activity on our networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments.

OUR PRIVACY TEAM

Privacy and confidentiality are critical considerations in everything we do at Thomson Reuters. We monitor data privacy laws and proposed legislation, to ensure that our products continue to provide high investigative value while maintaining compliance with applicable laws. The Privacy Office operates separately from product development and ISRM and are responsible for ensuring the ‘privacy by design’ methodology is followed during the development of our products. They help release products that reflect strong privacy standards: transparent collection of user data and providing users and administrators with meaningful privacy configuration options, while continuing to be good stewards of any information stored on our platform.

AUDIT AND COMPLIANCE SPECIALISTS

Thomson Reuters has a dedicated internal audit team within ISRM that reviews compliance with security laws and regulations around the world. The internal audit team assesses what controls, processes, and systems are needed to meet regulatory and compliance standards. This team facilitates and supports independent audits and assessments by third parties.

Data Center Security

HighQ's data centers are state of the art, utilising innovative architectural and engineering approaches.

HOSTING PROVIDERS

All our hosting providers meet a minimum of Uptime Institute Tier 3 requirements and have many years' experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the HighQ platform and infrastructure. HighQ data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass multi-level authentication to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

STAFF ACCESS

HighQ only provides data center access and information to employees who have a legitimate business need for such privileges, and as such only a tiny fraction of our employees will ever set foot inside one of our data centers. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of HighQ. All physical access to data centers by HighQ employees is logged and audited routinely.

SINGLE JURISDICTION HOSTING

Each client instance of the application is installed in one jurisdiction only and client data stored in that instance never leaves the jurisdiction for backup, disaster recovery or any other purposes except for when your users of the system download content over the internet, therefore data sovereignty is maintained at all times.

RESILIENCE

The high-performance network architecture is built to be resilient and scalable. Bandwidth is provided across multiple diverse links, which do not depend on any single backbone, ensuring that there is full connectivity redundancy, even in the event of one of the providers failing. All our data centers meet Uptime Institute Tier 3 standards.

Communications

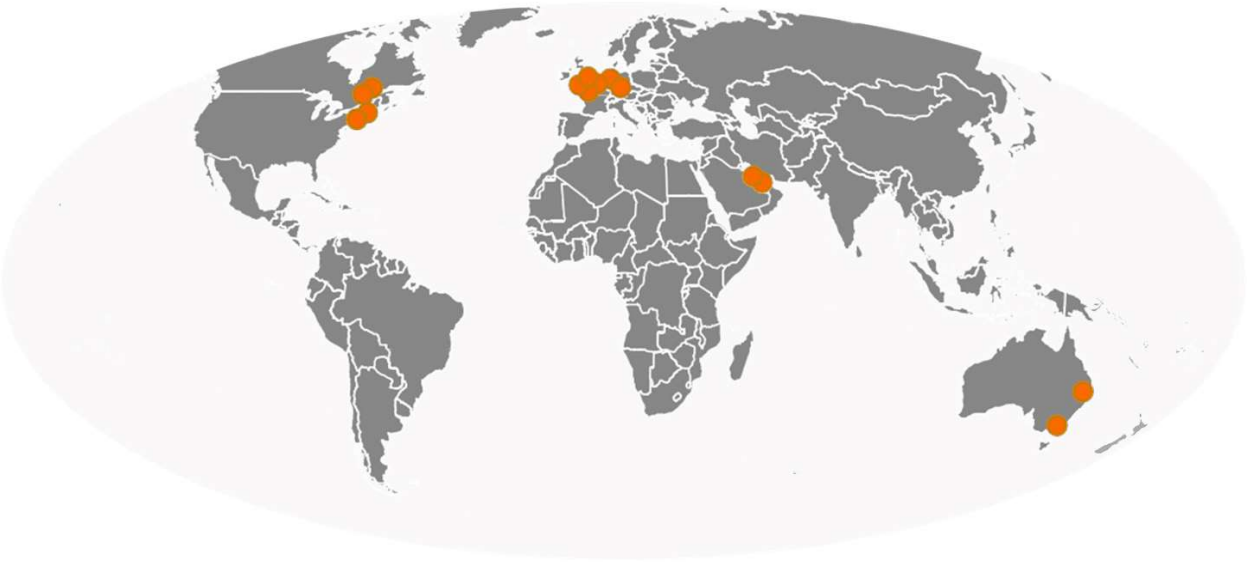
- Multiple fibre providers
- Multiple internet service providers
- Multiple internet exchanges
- Diverse independent telco risers from public highway to data floor

Power and Air Conditioning

- Generator back-up @N+1
- Air conditioning system @N+1
- Close control downflow AC conditioning units @N+1
- UPS conditioned clean power @N+1
- Diverse mains power supplies with diesel generator back-up @N+1

Security

- Smoke detection system
- State-of-the-art fire compression system
- CCTV throughout the building
- 24-hour video recording



- Sophisticated alarm systems
- PAC security card access system
- Visual verification on all persons entering the data floors
- Leak detection

SINGLE TENANCY

HighQ offers all clients a dedicated single-tenancy instance where all data is logically separated. Data resides on shared hardware.

HOSTING LOCATIONS

Thomson Reuters offers HighQ customers a choice of jurisdictions in which to host their data. All HighQ data center clusters are separated by significant geographical distance to ensure continued provision of service in the event of a disaster.

United Kingdom

In the UK, the primary and the secondary sites are both hosted in secure, industry leading data centers provided by Sungard.

- Sungard AS, Heathrow Corporate Park, Green Lane, Hounslow TW4 6ER
- Sungard AS, Global Switch House, 3 Nutmeg Ln, Poplar, London E14 2AX

UAE

In the UAE, the primary and secondary sites are both hosted in secure, data centers provided by eHosting DataFort in Dubai.

- EHDF Data Center, Building # 5, Dubai Internet City, Sheikh Zayed Road, Dubai, UAE
- DOZ Security, c/o eHosting Data Fort, Ground Floor, Bldg 6, Dubai Outsource City, Dubai, UAE

Offshore

HighQ also provide an offshore option hosted by JT Data Centers in Jersey and Guernsey.

- The Forum, Grenville Street, St Helier, JE4 8PB
- L'Avenue Le Bas, Rue Des Pres Trading Estate, St Saviour, JE2 7QN

Canada

In Canada, both facilities are hosted in state-of-the art Sungard high availability facilities in Ontario.

- Sungard AS, Argentia Rd, Mississauga, ON L5N 3K3, Canada
- Sungard AS, Gough Rd, Markham, ON L3R 4B6, Canada

SUPPORT LOCATIONS

Support can be provided from three locations: UK, Australia and USA. This allows us to provide support to clients during business hours, as well as 24 hours a day.

We recognise that some clients would prefer support from only one location to ensure data cannot be viewed outside of a particular jurisdiction. If this is requested, we have processes in place to ensure our support team can only offer you support from that nominated location.

USA

In the US, the primary site and the secondary site are both hosted in secure, industry leading data centers provided by Sungard in New Jersey and Philadelphia.

- Sungard AS, Spring Garden St, Philadelphia, PA 19130, United States
- Sungard AS, Commerce Blvd #3017, Carlstadt, NJ 07072, United StatesGermany

Germany

In Germany, the primary site in Dusseldorf and secondary site in Munich are both hosted in secure data centers provided by Equinix.

- Seidlstraße, 80335 München, Germany
- Albertstraße, 40233 Düsseldorf, Germany

APAC

In Australia, the primary site in Sydney and secondary site in Melbourne are both hosted in secure data centers provided by NextDC.

- Eden Park Dr, Macquarie Park NSW 2113, Australia
- DC2: Lorimer St, Port Melbourne VIC 3207, Australia

Operational Security

Far from being an afterthought or the focus of occasional initiatives, security is an integral part of our daily operations.

VULNERABILITY MANAGEMENT

Thomson Reuters SOC operates a vulnerability management process that actively scans for security threats across the HighQ platform using a combination of commercially available industry-leading tools, external CREST accredited penetration tests, quality assurance processes, Blackduck and Acunetix scans, code reviews, internal and external Qualys vulnerability scans and external audits by LRQA registered assessors. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Thomson Reuters also maintains relationships and interfaces with members of the security research community.

MALWARE PREVENTION

Thomson Reuters takes the threat from malware to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware. Our malware strategy begins with infection prevention by using automated Sophos scanners to scan all files at point of upload before they are placed in the file store. Any infected file is discarded immediately This applies to files uploaded directly through the platform or sent using the platforms in-built messaging systems. All storage, servers and databases are then continuously and actively scanned by Symantec SEP antivirus and Crowdstrike EDR engines for malware and indicators of compromise in HighQ to help identify malware that may be missed by antivirus signatures. The virus signature files are updated automatically, and our system administrators also can manually upgrade anti-virus software as soon as important updates are available. Any update made to the virus software (e.g. signature file) is validated and tested before being applied. All logs from our malware protection services are logged and monitored by the Thomson Reuters SOC.

MONITORING

Thomson Reuters security monitoring program is focused on information gathered from internal network traffic and user activity across the HighQ platform. This activity is ingested into our central SIEM. This is correlated against external and targeted intelligence from Anomali Threatstream and FireEye and our own analysts' knowledge and expertise of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behaviour, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing.

Our monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within HighQ are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. Monitoring and alerting is performed using Logic Monitor, SPLUNK and Pingdom. An on-call schedule is used so personnel are always available to respond to operational issues.

NETWORK SECURITY

The HighQ network provides significant protection against traditional network security issues.

Firewalls

The HighQ network is separate from our corporate network and is protected by multiple firewall zones. Only authorized services and protocols that meet our security requirements may traverse it; anything else is automatically dropped. Our Industry-standard firewalls are configured to deny all any-to-any rules and access control lists (ACLs) are used to enforce network segregation. Connections from users are restricted to port 443 https.

IDS and IPS

HighQ uses both host-based and network-based IDS and IPS systems to actively detect and prevent network intrusion.

Distributed Denial of Service (DDoS) Attacks

Endpoints are hosted on large, Internet-scale, world-class infrastructure. Industry leading DDoS mitigation techniques are used including RedSpam prevention and mitigation services. Additionally, HighQ's networks are multi-homed across a number of providers to achieve Internet access diversity.

Man in the Middle (MITM) Attacks

The HighQ platform is available via TLS 1.2 protected endpoints which provide server authentication.

IP Spoofing

HighQ instances cannot send spoofed network traffic. The HighQ-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

Port Scanning

Unauthorized port scans by HighQ customers are a violation of the terms agreed in contract. Violations are taken seriously, and every reported violation is investigated. Customers can report suspected abuse via their dedicated Customer Success Manager. When unauthorized port scanning is detected by HighQ, it is stopped and blocked.

Packet sniffing by other tenants

It is not possible for a virtual instance to receive or “sniff” traffic that is intended for a different virtual instance. The hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other’s traffic. Attacks such as ARP cache poisoning do not work within the HighQ platform. While HighQ does provide ample protection against one customer inadvertently or maliciously attempting to view another’s data, as a standard practice we also encrypt all network traffic to and from the application.

SERVER HARDENING

The operating system installed on the servers is Windows Server 2019. Default accounts have been changed and/or disabled. All demonstration folders and data have been removed.

USER DATABASE

User records are stored in a protected environment and kept up to date. The user database is not used for any marketing, research or any purpose other than the intended document sharing and log files.

SERVICE FAILURE NOTIFICATION

In the event of an application failure, users are notified of the service interruption on the front page providing contact details in case of urgent matters.

PATCH APPLICATION

All hardware and software involved in the provision of the application are patched to the latest level within an acceptable time frame. Patches are tested prior to implementation to ensure that the patch has been effective, that no new vulnerabilities have been introduced and that interconnecting systems can still interact as required. Automatic updates/patches are disabled.

INCIDENT MANAGEMENT

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Thomson Reuters security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800-61r2). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools and following ACPO guidelines. If an incident involves customer data, a client success manager will inform the customer and support investigative efforts via our support team.

HARDWARE TRACKING AND DISPOSAL

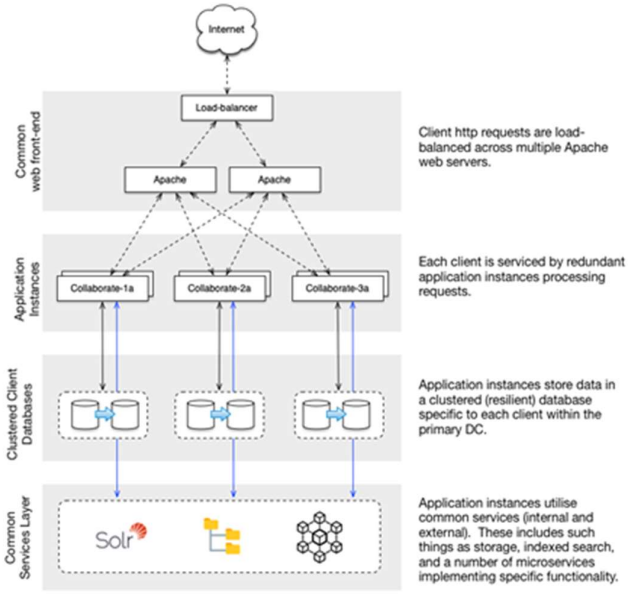
Thomson Reuters meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via barcodes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. HighQ hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is performed by a certified partner organisation who are accredited to BS EN 15713:2009.

Resilience

With an RPO and RTO of 2 hours, and an RTC of just a few minutes, our infrastructure is designed to withstand all levels of failure from basic component failure to site failure.

Component Failure

The HighQ service is accessed through redundant multi-vendor internet links into the HighQ Private Cloud. Redundant firewalls are installed in each DC location in a clustered configuration to mitigate hardware failure. Web requests are load-balanced across multiple Apache web-servers servicing requests. Each server is configured to withstand power failure (redundant power supplies) and disk failure (RAID configuration). Multiple application instances are in place for each client in an active-active configuration (sessions are replicated across application instances). Each customer database is running in a resilient cluster with each node deployed on separate physical hosts. Redundant copies of all shared supporting services are also load-balanced. All applications and services are running on Hyper-V clustered hosts which allow workloads to be recovered in real-time if there is a host failure.



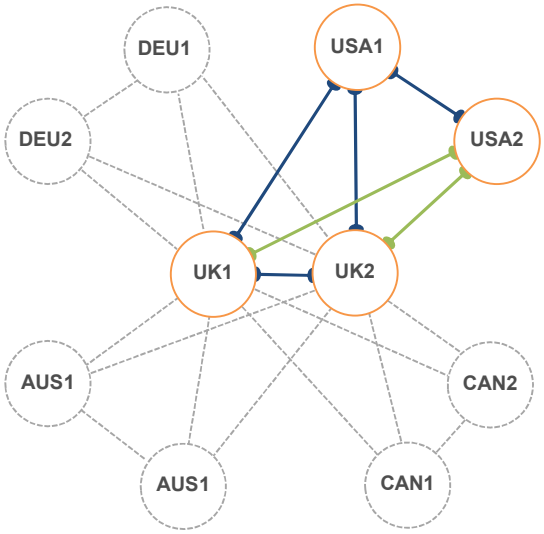
HighQ operate a 24/7 monitoring service and in the event of a component failure, the HighQ technical team are immediately alerted via email. The in-built redundancies described above ensure that the system remains fully operational. HighQ engineers will replace the failed component within 24 hours.

Software Failure

All servers are monitored 24/7 and any software failure in the operating system or application servers will immediately trigger an alert which is then prioritised and fixed. In the unlikely event that there is a coding issue, our software engineers will then create and deploy a fix.

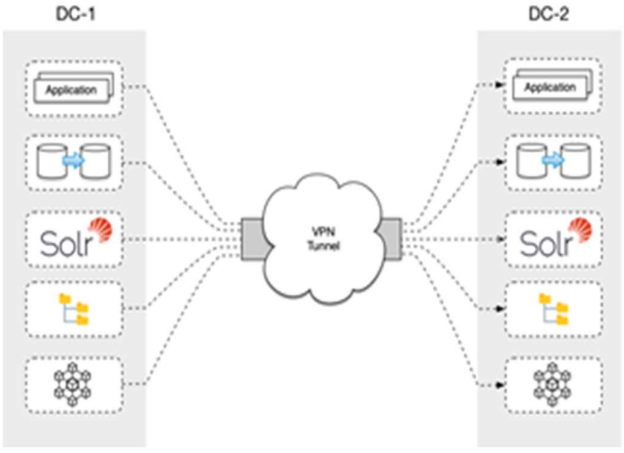
Inter-Data Center Resilience

HighQ data centers are interconnected through resilient VPN connections using a hub and spoke configuration (by region).



Hardware Failure/Site Failure

Across each region, the Data Center 'pairs' are used to provide fail-over (DR) capability. If a Data Center becomes unavailable for any reason, client services can be re-established on the secondary site without loss of data. This is achieved by actively synchronising services and data across the VPN link. In the event of a full-service failure, all data and services are available on the secondary site. DNS configuration is required via the application management layer to switch services for clients to the alternate site.



In the event of a more serious failure (entire site), we will move immediately to the DR site. This may take up to 1 hour in total to ensure complete global DNS propagation.

Data Management

Throughout its lifecycle, you can rest assured that you remain in complete control of your data whilst benefitting from the high level of security offered by the HighQ platform.

CONTROLLING YOUR DATA

Clients have complete control over what data is uploaded. HighQ do not have visibility of your data and do now know what types of data exist on your instance. HighQ act as a data processor, clients are the data controller.

DATA BACKUP

The databases are automatically backed-up (full back-up) every night. The database backups are kept on a rolling 30-day basis. The purpose of this back-up is to ensure that previous versions of the database can be restored in the event of the database becoming corrupted (it is possible that the DR database may also become corrupt through replication although very unlikely) so a separate back-up is required.

Database replication between the primary and DR site is performed over an encrypted VLAN in real time.

File based data is replicated hourly and filesystem snapshots are made daily and retained for 30 days.

SEGREGATION OF DATA

The platform enforces strict data segregation. HighQ deploys and manages application instances specific to each customer. Because of this, it is possible to manage resources for these instances based on the actual client usage, and the logical separation of the application and database allows an additional level of security.

An overarching management application allows for overall configuration and control of the client instances. The application instances each have their own resilient database configuration storing customer data, but also share some common services.

HIGHQ STAFF ACCESS TO YOUR DATA

No HighQ staff have access to your data as your data remains encrypted while it resides on the HighQ network and servers. This means that our admins cannot view your unencrypted files. Where HighQ manages your encryption key our segregation of duties principle and privileged account management system means that no admin can access both the encryption key management system and the file storage.

SUPPORT TEAM ACCESS TO YOUR DATA

The only time a HighQ employee may see your data is where you provide explicit written consent to our support staff, and you provide them with an account to log in, in order for them to assist you should you need some technical help. All access by our support staff is fully logged and clients have full access to these logs. You can revoke the support account whenever you wish to.

DATA PRIVACY REGISTRATION

HighQ is registered with the UK Information Commissioners Office.

DATA BREACH NOTIFICATION

Clients are informed in line with contractual obligations and GDPR or the data privacy law in the country in which your data is hosted. Clients are notified over established communications channels of their choosing.

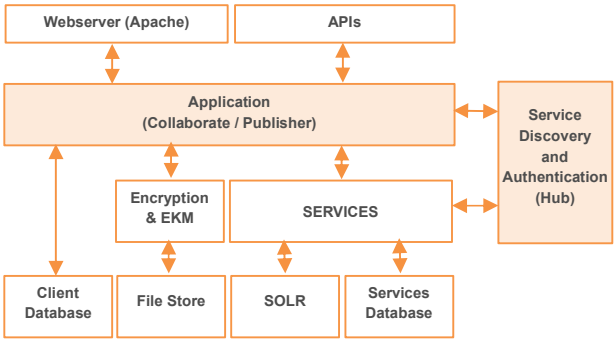
DATA DESTRUCTION

At end of contract your data will be returned to you in a manner and format of your choosing. Your data will then be securely erased from the HighQ servers. Your data will remain in backups for a further 30 days before being overwritten.

Application Architecture

Each application instance is accessed through an Apache web layer. The application and supporting services are written in Java running under Tomcat.

Our applications are built as single deployable entities, supported by separate self-contained micro-services.

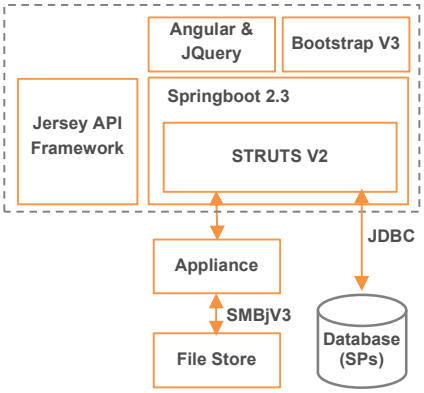


The core application is configured to access specific services through a common service broker known as Hub. This also provides authentication and SSO functionality and allows configuration changes to be applied across groups of deployed application instances.

Access to the underlying file-store is controlled through a service which provides encryption and key management. As files are uploaded, the encryption and EKM appliance will encrypt the files to make them inaccessible except through the application interface. This also automatically manages resilient data copies, keeping these in synchronization. Indexed search is provided as a common service using SOLR.

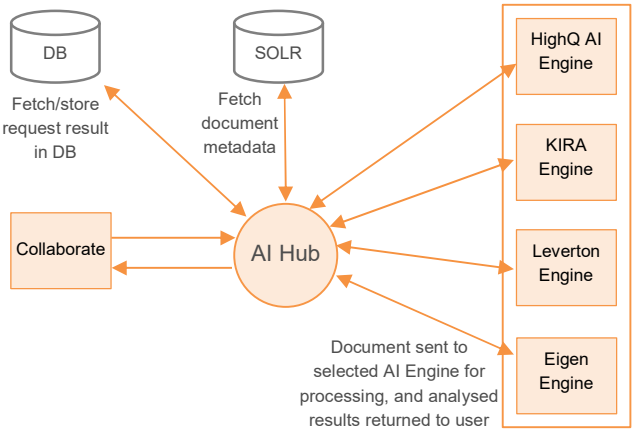
APPLICATION FRAMEWORK

The core Collaborate and Publisher applications are written in Java using Struts 2.5 running under Springboot 2.3. The UI is built using Angular, JQuery & BootStrap 3.3, and Jersey is used to expose external RESTful APIs for client integration. The application communicates with its underlying database cluster via JDBC, but standard SQL statements are prevented. To prevent SQL Injection, all actions are wrapped in Stored Procedures at the database level. The database technology used is Microsoft SQL Server.



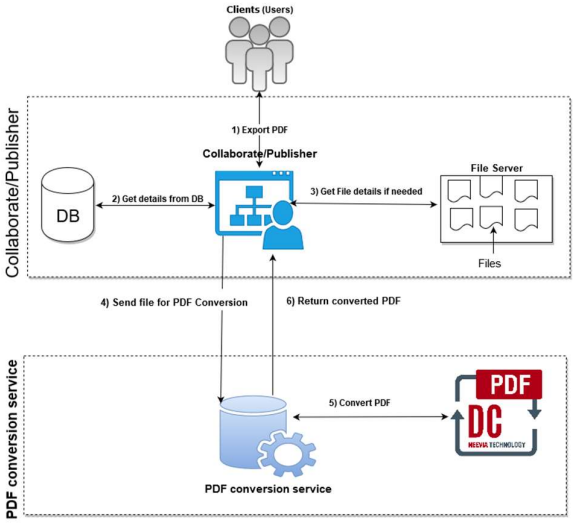
AI HUB

AI Hub is used to manage document meta-data extraction. It acts as a broker for both internal and external document analysis services. Collaborate will periodically submit documents for processing to AI Hub and the microservice will pass the documents to each configured analysis service. As soon as results are available, it will then store these results in SOLR and within Collaborate iSheet metadata. The iSheet data can be used to visualize the results.



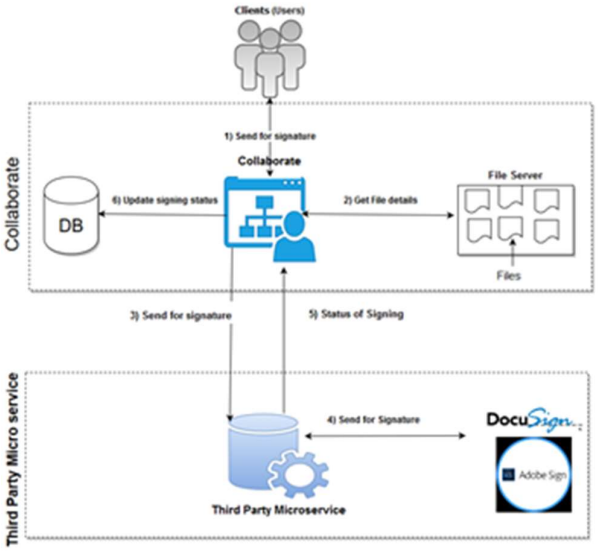
PDF SERVER

HighQ Collaborate and Publisher offer export to PDF and OCR conversion through a PDF micro-service. The PDF server uses the Neevia PDF Conversion Tool to convert original file to PDF, Apache Tika library for Text Extraction, and ABBYY for OCR processing.



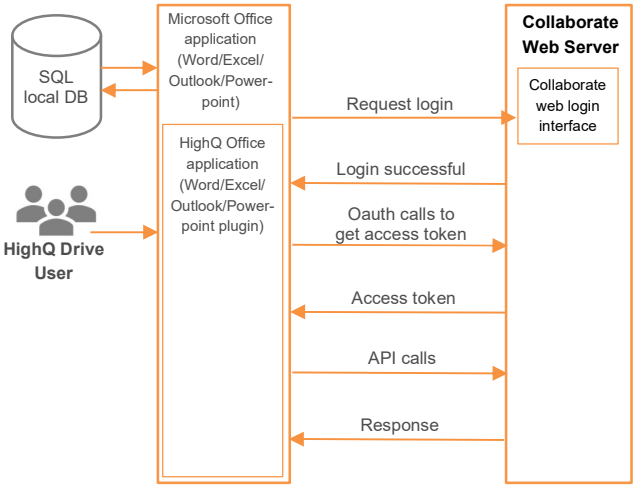
E-SIGNING

HighQ collaborate offers document E-signing capabilities under files management. Currently, it supports DocuSign® and Adobe Sign service providers as part of third party signing micro service. HighQ's e-signature integration empowers you to complete approvals, agreements and transactions faster by making it simple to select one or more files and send them to multiple recipients for signing. As you're sending them, you can indicate exactly where the documents need to be signed for greater clarity.



OFFICE ONLINE & OFFICE ADD-IN

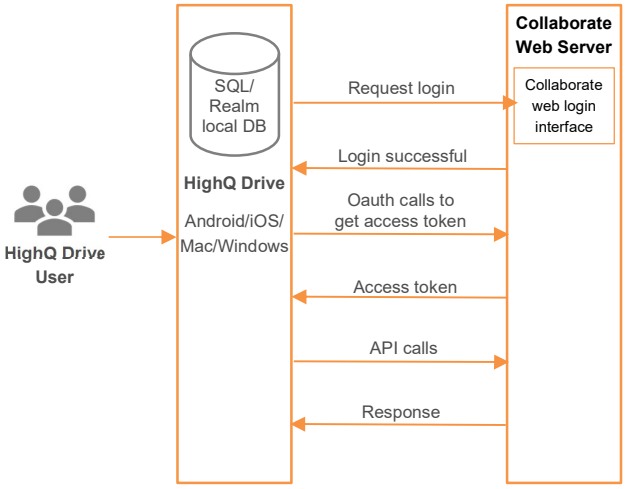
The Office Online microservice gives a user an ability to edit and view office documents such as Word, Excel and Powerpoint using Microsoft office 365 online. This means even though user does not install Microsoft Office installed in their personal computer, a document can be viewed or edited. As soon as user has updated the document a version gets saved in file repository in collaborate against same document.



HighQ Office Add-in application is available for Microsoft® Word, Microsoft® Excel, Microsoft® Power point and Microsoft® Outlook. A user can e-mail attachments, MyFile, or Teamsite file directly through the add-in plugin. It also allows documents to be uploaded and sent via an embedded link in email (for documents which are larger in size).

HIGHQ DRIVE

The HighQ drive application is available in Android, iOS, Mac and Windows Desktop platforms. The client application synchronizes all MyFile and teamsite files to the local machine. If any changes are made to the local version, then a new version will automatically be uploaded to Collaborate. The application is available to download from the profile dropdown on the Collaborate site.



THIRD PARTY SERVICES

HighQ makes use of a number of secure and trusted third party services to provide additional functionality within our products.

Adeptol

Adeptol offers the industry's leading document viewing technology which can be embedded in any webpage or application or integrated with any process or system. Adeptol is a Server Based Document Viewer uses AJAX and HTML5 technology to create fast rendering of documents on the fly and includes a unique set of capabilities to render, enrich and dynamically deliver content. Adeptol is also the one of the first companies in the world to offer a Software-as-a-Service (SaaS) based document viewing solution.

SOLR

Solr is highly reliable, scalable and fault tolerant, providing distributed indexing, replication and load-balanced querying, automated failover and recovery, centralized configuration and more. Solr is a search server built on top of Apache Lucene, an open source, Java-based, information retrieval library. Designed to drive powerful document retrieval

applications, Solr powers the search and navigation features of many of the world's largest internet sites.

Wowza

Wowza Streaming Engine is a unified streaming media server software developed by Wowza Media Systems. The server is used for streaming of live and on-demand video, audio, and rich Internet applications over IP networks to desktop, laptop, and tablet computers, mobile devices, IPTV set-top boxes, internet-connected TV sets, game consoles, and other network-connected devices. The server is a Java application deployable on most operating systems.

Keycloak

Keycloak is an open source Identity and Access Management solution aimed at modern applications and services. It makes it easy to secure applications and services with little to no code. We have used Single-sign-on feature of Keycloak. Users authenticate with individual applications so do not need to deal with login forms in another applications. Once logged-in to Keycloak, users don't have to login again to access a different application. This also applies to logout. Keycloak provides single-sign out, which means users only have to logout once to be logged-out of all applications that use Keycloak.

Neevia

Neevia Document Converter Pro is a software product that dynamically converts Microsoft Office 2003/2007/2010/2013/2016/2019/365, WordPerfect, HTML, AutoCAD DWG/DWF, EML, MSG, PostScript and many other document types to PDF, PDF/A, PostScript, JPEG, TIFF, PNG, PCX, BMP. It operates in both a batch mode via directory or email scanning and in direct mode via a COM (ActiveX) component. Document Converter can be configured to recognize text - this is known as OCR - for the converting Image and PDF files and comes with support for printing the input files directly to a physical printer instead of converting them to PDF or Image. With clustering and multi-threading support Neevia Document Converter Pro offers a reliable and stable conversion process. The goal of Neevia Document Converter Pro is to help your company create one PDF/Image standard that can be integrated into your workflow with ease and affordability.

AUTHENTICATION BETWEEN MICROSERVICES

All small services have an authentication mechanism. OAuth is implemented and HighQ Hub works as a trust store to authenticate the services.

To authenticate services which are not exposed to end-users, HighQ uses a JSON web token (JWT). JWT contains a payload which is encrypted and contains user details and realm along with authorization details.

Product Security

HighQ Collaborate has multiple layers of security to give peace of mind to your users that their data is safe.

AUTHENTICATION

All users require a userID and password to access the system. Each user's userID is their registered email address. Passwords are never sent to users in an email. The email contains a link that allows the user to set their password.

The user can select their password subject to the following restrictions:

- Must be at least 8 characters in length
- Must contain at least one integer and one CAPS
- Cannot be the userID
- Cannot be blank

Users are required to change their password the first time they log in to the extranet and can change their password at any time after that (considering the rules above) via the 'Forgotten my Password' link

Password history is retained for 5 iterations and prevents re-use of the same password in this period. Passwords will expire 90 days after they were last changed.

Passwords are never stored or visible to HighQ employees. They are salted using a unique string and SHA-256 hashed.

2-Factor Authentication

Further restrictions can be enabled via 2-factor authentication using the Oauth2 protocol and a code generator such as Google Authenticator.

New Users

New users are sent an email containing a link to create their password before they log in for the first time. This link expires within 24 hours.

Site-level passwords

Individual sites within the HighQ Collaborate application can be protected with a site password.

File sharing passwords

Files shared with external contacts using the Collaborate mail feature can be protected with a password.

User Access Control

Access control privileges assigned to users are validated every page hit / script execution and are consistent across the site. Where 'shortcuts' are enabled, authentication is still required, and suitable access control applied.

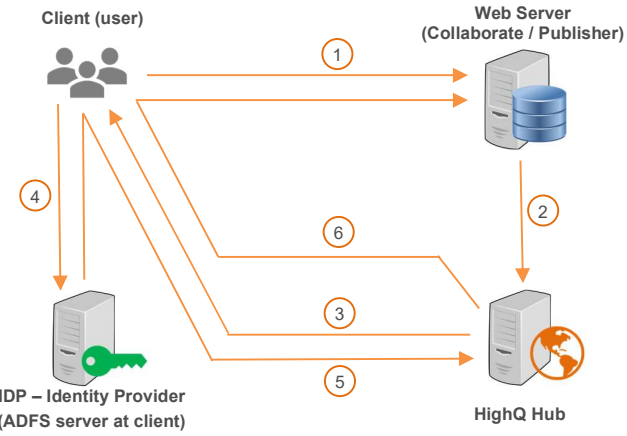
User Lockout

After 3 failed authentication attempts, the user account is locked, and an email is sent to the user (as per their registered email address) to reactivate the account and reset their password. Passwords are never sent to users in an email. The email contains a link that allows the user to set their password.

SINGLE SIGN-ON

HighQ offers the ability for any organisation to set up single sign-on (SSO) between their network and HighQ's cloud-based applications. This enables a user to seamlessly log into any HighQ application where they have an account without having to enter a separate username and password.

SSO is achieved by integrating a customer Microsoft Active Directory Federation Services 2.0 (ADFS 2.0) server OR any SAML 2.0 supported IDP with HighQ Hub via the SAML 2.0 protocol. HighQ Hub is a dedicated single sign-on application that integrates with all HighQ.



1. User submits a request to the application URL (the HighQ Collaborate instance address).
2. User request is redirected to HighQ Hub for SSO lookup.
3. HighQ Hub checks SAML assertion token to establish if there is a valid session. If it is not found it redirects to the login page for IDP.
4. User enters credentials to authenticate.
5. If user successfully authenticates, they are redirected to HighQ Hub with a valid SAML token.
6. HighQ Hub reads the SAML token, verifies if it's signed by a valid IDP Server and generates a special login URL. It then redirects the user's browser to Collaborate. Collaborate authenticates the user with the URL generated by HighQ Hub.

HighQ can accept SSO requests from many different providers. Please speak to your Customer Success Manager or Sales Consultant for more information.

SESSION MANAGEMENT

Sessions are tracked by encrypted session IDs. Session IDs are of an appropriate length and complexity to prevent a client being able to hijack another session by altering their session ID. Application firewall and the application itself have built in XSS and CSRF protection to mitigate against any session hijacking attempts

Logout

Users are directed to logout at the end of every session. No data is held on the client PC and logging out or closing the browser will invalidate the current session. Thus any subsequent connection from the PC requires reauthentication (ensuring that any other user of that PC cannot access the application).

Session Timeouts

Connected user sessions to the application require re-authentication after a period of 30 minutes of standing idle. This timeout period can be altered at client request.

SECURE COMMUNICATIONS

All communications between the browser and the application are encrypted, including logon (user authentication). Encryption is provided as a default of 256-bit AES TLS 1.2 and is cross browser compliant.

File Upload

All file uploads to the server are over a default of 256-bit AES TLS 1.2. Deprecated ciphers are not supported.

File Download

All file downloads from the server are over a default of 256-bit AES TLS 1.2. Deprecated ciphers are not supported.

ERROR MESSAGES

All error messages are controlled and give away minimal information if displayed. Examples include:

- Failed login does not define whether the userID or password was incorrect.
- All links are maintained through our development/build process. Any missing pages display a pre-defined “catch all” error page and do not give away any architectural information.

Incorrectly formatted input is validated both on client side before submission and server-side before processing.

FOOTPRINT

No sensitive data is ever stored on the client PC. The sole item of data kept on the client PC is a unique session identifier (consisting of two highly random, non-predictable numbers). This data is stored in the form of a session cookie and therefore is removed when the browser session ends.

IP WHITELISTING

IP address restrictions can be enabled by site administrators using the X-Forwarded protocol.

CKEDITOR

HighQ offers clients a feature to create code and run JavaScript within a site using the CKEditor feature. When this feature is enabled, JavaScript code can be embedded within the HTML source and will execute when a site page is loaded. All parsing and execution of the HTML and JavaScript source code are carried out on the client endpoint; no execution of CKEditor code embedded within a site happens on HighQ Servers. HighQ sites cannot run embedded Java Applets; functionality is limited to JavaScript code, which may be called from an external source.

Should a malicious actor gain access to the CKEditor feature and for example, deploy code designed to undertake session hijacking, then protections on the HighQ Servers will detect and prevent unauthorised access. The HighQ Platform is protected by multiple layers of security, which includes a WAF, multi-zone firewall, Cisco Firepower IDS/IPS, Crowdstrike EDR and SEP antivirus. HighQ also performs extensive logging and monitoring to detect and block intrusion attempts and IOC's.

A client's endpoint and browser will need to be protected by the client's own security systems to ensure any code executed within a browser is scanned and prevented from any malicious or unauthorised actions on the client device.

COOKIES

A cookie is a simple text file that is stored on your computer by a website’s server and only that server will be able to retrieve or read the contents of that cookie. Most websites you visit will use cookies in order to improve your user experience by enabling that website to ‘remember’ you, either for the duration of your visit (using a ‘session cookie’) or for repeat visits (using a ‘persistent cookie’).

Cookies do lots of different jobs, like letting you navigate between pages efficiently, storing your preferences, and generally improving your experience of a website. Cookies make the interaction between you and the website faster and easier. If a website doesn’t use cookies, it will think you are a new visitor every time you move to a new page on the site – for example, when you enter your login details and move to another page it won’t recognise you and it won’t be able to keep you logged in.

We do not use any data stored or contained in cookies for any other purpose other than as described below.

HighQ uses the following cookies:

JSESSIONID

JSESSIONID is a cookie generated by Servlet container like Tomcat and used for session management for J2EE web application for HTTP protocol.

The cookie is only used during an active session and is deleted when the browser is closed.

DWR Session

This cookie is needed for CSRF protection for AJAX

DWR library

This is used by HighQ Collaborate to perform asynchronous Javascript and XML (AJAX) calls to improve user experience and reduce page loading times.

Dwrsessionid

This cookie is used to protect against potential cross site request forgery (CSRF) attacks during such AJAX calls.

The cookie is only used during an active session and is deleted when the browser is closed.

Remember Me

Within all of our products there is a “Remember me” function. If a user selects this checkbox, a cookie will be saved on the user’s computer and this will allow the user to login automatically on subsequent visits to the site. The EU Directive does not affect the use of this cookie as it is an “opt-in” feature i.e. the user must select the “Remember me” checkbox for the cookie to be installed.

The cookie is only used for automatic login – it does not collect any user data.

FileOpen

HighQ Collaborate allows sites to be created with “PDF Security”. This is a Digital Rights Management tool that allows restrictions to be applied to PDF documents and ensures that access can be tightly controlled, even if the document is saved to the user’s computer.

In order to open a PDF document, the user is required to download the FileOpen plugin – this communicates with the server each time an encrypted document is opened. When a user downloads the first document and authenticates using the FileOpen plugin, a cookie is saved on their machine. This cookie stores the user’s login details (in an encrypted format) and ensures that authentication is not required each time an encrypted document is opened. If the cookie was not installed, the user would need to enter their login details (email address and password) for every document that was opened. We regard this cookie as an essential part of the system as not having it would render the system almost unusable.

The cookie only stores the encrypted version of users’ authentication details and is not used to collect any other information.

Analytics cookies

If requested by our clients there may be analytics cookies enabled. These cookies gather anonymous analytical information about the users of the system to help HighQ better understand the usage patterns of the application. We typically use Google Analytics for this purpose.

Identification cookie

This cookie is only used in HighQ Publisher. When a user logs in for the first time via an auto-login link and registers their account information, an identification cookie is saved to their computer. This cookie does not contain the user’s password, only an encrypted version of the user’s email address. This is used to identify the user when an auto-login link is used the next time they access the system from the same computer.

ACTIVE CODE

There are two optional components to the service which require Active Code:

- Download required for the site is the ‘FileOpen’ plugin. This is only required for sites that contain encrypted PDF documents. The FileOpen plugin has been approved by Adobe and is the most popular PDF encryption tool, currently used by the majority of leading data room providers including Intralinks and iRooms. Please note that this plugin will not be required for sites that do not use PDF encryption.
- An upload manager Java applet is also an option which can be enabled if client requests which allows for drag and drop functionality for file uploads as well as the ability to upload extremely large files

APPLICATION SECURITY

Bounds Checking & Parameter Evaluation

All input fields available within the site check the inputted data before processing it. This checking occurs on the server side as well as client side.

Common File Queries

All manufacturer supplied demonstration and sample files are removed from the site host before being published to the internet.

Any other files or file types associated with any application that can be misused are obfuscated or removed.

Link Structure

All links are maintained through our development/build process. Within the application’s coding, care has been taken to ensure that any unnecessary links have been removed (not commented out) from the site.

Additionally, all comments are visible in source only and not displayed client-side.

Source Code

The HTML source code provides no unnecessary information revealing important information about the application architecture, the coding routines, the personal details of the author or any vulnerability that the application may be exposed to.

Path Truncation
Users cannot request a site directory page. There is a default file located within each directory and directory listings are disabled in the web server configuration files.

Cross Site Scripting
The application is hardened against cross site scripting vulnerabilities. This is implemented via both application firewall and within the application itself.

SQL Injection
The application is hardened against SQL injection vulnerabilities. This is implemented via both application firewall and within the application itself.

Application Administration
Any administration of the application (i.e. add/remove users; change user privileges etc) is subject to close control and monitoring. All administrator actions are logged by the system (as well as all actions by all users).

Site Terms and Conditions
All users must accept the Terms and Conditions before being granted access to the site. If the Terms and Conditions are not accepted, the user will be denied access to the site.

Compatibility
All HighQ applications are compatible with IE 7 (and above) and the latest two versions of Safari, Chrome and Firefox. Fully responsive design for IOS delivered by Apple iTunes Store.

Also, the data held by the application host is in a format transferable i.e. returned to the client or passed to another ASP. Documents are held in their native format.

Architecture Controls
Server configuration has been well thought through and documented. Care is taken to ensure that unnecessary services are stopped and disabled; default passwords are replaced with strong passwords; default accounts are removed and/or renamed; log files are protected; patches are applied in a timely fashion. Automatic updates are disabled.

PENETRATION TESTING
Penetration tests are performed at every major release of the HighQ software, currently twice per year but at least annually, by a third-party CREST accredited firm. The scope of the penetration tests covers both the application and the hosting platform. We also carry out our own internal penetration tests conducted by the Thomson Reuters internal team throughout the year. Monthly vulnerability scans are also conducted against internal and externally facing infrastructure using Qualys.

SECURELY MIGRATING YOUR DATA INTO HIGHQ
If you are using a different application and wish to move your data and documents to HighQ, this can be done within the application itself via a bulk upload, or by using a SQL connection. Additionally, a bespoke migration tool using HighQ's API's can be developed for data or document migration.

Simple validation for successful migration can be made by comparison of HighQ audit reports and exports.

Connectors and Plugins

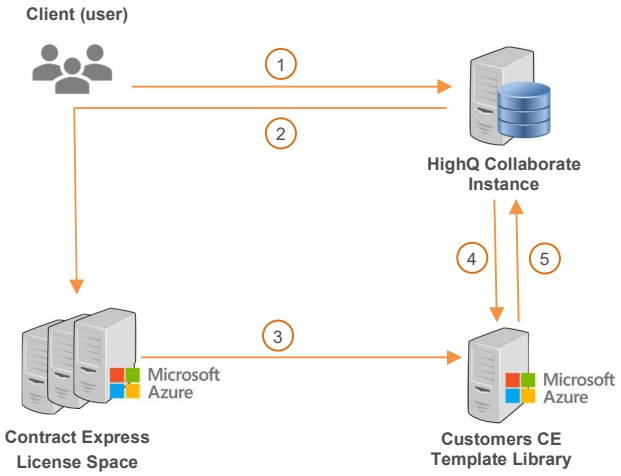
HighQ can securely connect with other Thomson Reuters products and many third-party services.

CONTRACT EXPRESS

Thomson Reuters Contract Express is the plain language automation software used legal professionals to rapidly draft documents.

Your dedicated HighQ Collaborate instance is hosted in your nominated HighQ data center, in your chosen region, where your data and documents, including those generated by the Contract Express engine, are stored.

Customers who purchase the new Doc Auto module will also have a Contract Express template library hosted on Microsoft Azure in the same region as their HighQ Collaborate instance.



1. User authenticates to HighQ using their normal credentials (SSO or HighQ Collaborate) and requests a CE template.
2. Using HighQ as the IDP, the template request is sent to the Contract Express license space in Microsoft Azure.
3. When validated, the CE document is generated within the CE instance in MS Azure using the CE document assembly engines.
4. The questionnaire data used to populate the document is temporarily held in the CE instance while the user enters the questionnaire data in HighQ Collaborate.
5. The generated document is automatically saved back to HighQ Collaborate and the questionnaire data is deleted from the Contract Express library.

The Microsoft Azure Contract Express library is held in a multi-tenant cloud instance, with each customer's template library logically separated into a private license space.

- A license space contains an individual customer's templates and associated configuration files (profiles, usernames, email address, locales and external data connections) and is also used to manage template permissions.
- A license space cannot be connected to more than one HighQ instance and a HighQ instance cannot be connected to more than one license space.
- It is only possible to access the connected Contract Express template library via Collaborate or the Contract Express Author tool, using Collaborate credentials.

The Contract Express instance also hosts the questionnaire and document assembly engines that are used to generate documents from Contract Express templates using data entered into a questionnaire by a Collaborate user.

Questionnaire data is temporarily saved in the connected license space while a user has the questionnaire open in Collaborate, however that data is not retained in Contract Express and is deleted when the questionnaire is closed.

Throughout the lifecycle of the contract document, HighQ is the primary data storage and Contract Express acts only as the template library.

SEEUNITY

HighQ and SeeUnity offer an integrated solution that enables seamless archiving, publishing and bidirectional syncing of content and metadata with applications including Microsoft SharePoint, eDoc, iManage, and NetDocuments.

The SeeUnity REST API is a generic interface that allows an application to be written once to integrate with numerous document management systems to securely synchronize and migrate data across on-premise or cloud-based solutions with HighQ.

SECLORE DRM PLUGIN

Seclore provides an advanced, secure and connected digital rights management (DRM) functionality – delivering an additional, persistent layer of protection for shared and downloaded files.

A user installs the FileSecure application on their device which implements Seclore Rights Management automatically, applying persistent, granular usage controls to sensitive documents downloaded or accessed from HighQ. Organizations can decide who can access a file, what they can do with it, for how long, and from which device. The usage controls remain with the file even after it is downloaded from the platform and shared.

Additional Security Options

HighQ can offer clients additional optional features for EKM and Hybrid Storage.

HYBRID STORAGE

Hybrid storage allows you to create a separate file store location of any site in a Collaborate instance. This is achieved by installing a HighQ Appliance server and connecting it to a chosen storage array on your private network.

This allows you greater flexibility for selecting the location for hosting your files as well as the ability to remove all physical access to your files at any time.

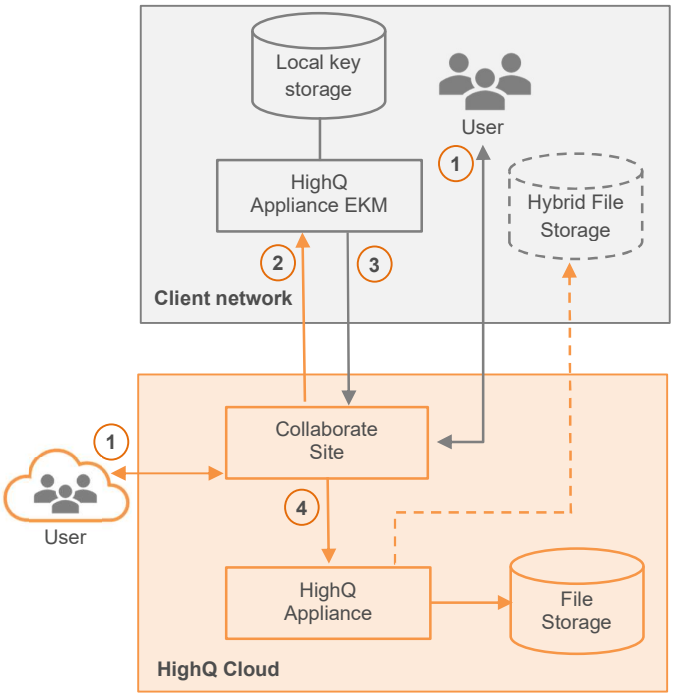
ENCRYPTION KEY MANAGEMENT (EKM)

Encryption Key Management (EKM) uses HighQ's proprietary methodology to allow clients to manage the encryption keys for files stored in HighQ Collaborate. The encryption keys are generated and stored in the HighQ Appliance, which acts as the key manager and is deployed inside your network to give you complete control.

- EKM is optional and is enabled per Collaborate instance as required
- The HighQ Appliance acts as the key manager for key generation and storage
- Keys are generated with AES 256-bit encryption
- Each instance of Collaborate can have multiple encryption key managers configured and each site can have its own configuration for EKM
- The key manager can be changed at any time and keys are migrated accordingly
- The HighQ Appliance and the instance(s) of Collaborate it's connected to communicate using the REST API and OAuth for authentication
- Each site in Collaborate has its own unique encryption key and the files in that site are encrypted using that specific key
- The key manager is only responsible for creation and storage of keys
- The file encryption and decryption is performed by the file storage manager, which can either be on the same Appliance or a different Appliance to the key manager

EKM ARCHITECTURE

1. Client user adds a file to site X. If a hybrid storage model is deployed, then the file will be stored in the client's network, otherwise the file is stored on the HighQ server in your chosen data center.
2. Collaborate sends Site ID and Instance Key to the Appliance EKM which is deployed inside the client network. The Appliance EKM generates an encryption key using Site ID and Instance Key and store it in a key store.
3. The Appliance EKM returns the encryption key to Collaborate which is located in the HighQ Data Center. Collaborate sends the source file and encryption key to HighQ Appliance for storage.
4. The Appliance uses the encryption key to encrypt the file and store it in the file store, either in the HighQ data center or the client network if a hybrid model is deployed.



Please speak to you Customer Success Manager or Sales Consultant for more information about EKM and hybrid storage.

About HighQ

Thomson Reuters HighQ provides innovative enterprise collaboration and content management solutions to the world's leading law firms, financial services companies, governments and corporations. The company's blue-chip client base includes over 50% of the global top 100 law firms and some of the largest global financial institutions. HighQ combines secure, enterprise-grade technology with an amazing user experience to transform the way businesses collaborate, communicate and share information securely in the cloud.

For more information please visit: https://legal.thomsonreuters.com/en/products/highq