About this document

• This document describes the Confirmit Horizons SaaS environments and security mechanisms we have in place for protecting customer data.

• As per Confirmit’s information classification policy, this document is provided as “Unclassified”. Unclassified documents can be shared freely without the need to sign a non disclosure agreement.

  • Updated version of this document will be made available for download (at least) quarterly from https://extranet.confirmit.com/library/security.aspx#tab1
The Confirmit Horizons Software

• From its inception in 1997, the architecture and code of the Confirmit Horizons software has been designed for web deployment.
  - We started offering “Software as a Service” long before the SaaS term was in use.

• The code is subject to significant ongoing investment (code refactoring) to ensure the code remains up to date. This allows us to take advantage of new technologies and thereby boost security, performance, reliability, and scalability.

• The Confirmit Horizons code itself is very resilient. Combined with our 3-tier proactive 24/7 monitoring, this provides our SaaS clients with the highest security, performance and availability in the industry.
Security in Confirmit Horizons Authoring

• By default, only the Confirmit Horizons user who creates a project has access to information about the project and the related data. Additional access must be set up by the project owner.
• In addition to different levels of project permissions, access levels are determined by the user’s role membership.
• Login controls on Confirmit’s Horizons SaaS environment include:
   HTTPS (TLS) enforced for all transmission of credentials, and full session HTTPS is optional for all applications. HTTPS may also be enforced for all connections at individual user or company level. Confirmit recommends using HTTPS for all web connections to protect data in transit.
   HTTPS is always enforced for all application access for Confirmit employees.
   All user accounts are named, personal (not shared) accounts linked to an individual email address, and have an expiration date set in line with contractual expiration.
   Strong password policies are enforced for all users on the system. Passwords expire after a set number of days, and password history is enforced to prevent passwords from being re-used. Company specific settings allow for even stronger password rules for all users within a company to meet any internal policy requirements.
   Accounts are automatically locked by the system after 5 consecutive failed login attempts. A locked account must be re-opened by Confirmit Technical Support.
   Passwords are one-way hashed (PBKDF2) with a high iteration count and unique salt values for each user account. One Time Password reset links are generated for new / re-opened accounts / lost password e-mails, to prevent account passwords being displayed in clear text. Not even our Technical Support staff can view user passwords.
   Users can further improve their account security by adding Google Authenticator two-step authentication to their account. Two-step access is enforced for Confirmit employees.
   Confirmit Horizons automatically locks application access for Authoring and Reportal users after a period of inactivity (60 minutes on our SaaS environment), after which users must re-enter their password to unlock the application.
Security of Data

• The database servers that store respondent and response data are placed behind two tiers of firewalls (see network maps later in this document), and data can only be accessed through the Confirmit Horizons applications. No application users have direct database access, the servers are only accessible for database administrators.

• Remote server access is only available to our system administrators from a specific internal IP range within Confirmit’s corporate network and through a secure VPN tunnel. If outside the corporate network, dual factor authentication is required to establish a secure VPN tunnel into the corporate network (in order to access the production VPN through a hop-server), and only computers that are under Confirmit’s control are allowed to connect to the VPN.

• Confirmit Horizons surveys are stateless, sessionless and do not require any user-identifiable information to be transmitted between page submissions. Surveys use a combination of hidden form fields and system generated identifiers to identify the respondent and the correct state in the interview when moving from page to page.

• Interview pages include meta code to prevent them from being cached on the client. No information is stored on a respondent’s computer when the browser is closed. To further prevent caching, all surveys are available over HTTPS.

• We use Extended Validation certificates, providing additional safety visibility for visitors by having a green address bar for all services running on the platform.

• Confirmit Horizons supports encryption of data at rest*, based on the Transparent Data Encryption feature in SQL Server.
  • This setting can be enforced for all surveys for a specific company, or applied to individual surveys during initial survey launch.

* Subject to licensing of relevant Confirmit add-on feature
Additional Security Features

• Individual company settings allow the enforcement of HTTPS encryption for all authoring / reporting / survey activity for all users.
  • SSLv2/v3 connectivity is disabled and only secure TLS encryption ciphers are enabled. The list of supported ciphers is continuously reviewed to ensure mitigation of known vulnerabilities targeting insecure cipher suites and settings.
• Confirmit Horizons supports PGP encryption of files prior to delivery for data transfers such as data exports, report exports and respondent uploading.
  • Encryption can be enforced at a company level to prevent non-encrypted data being exported from or imported to Confirmit Horizons.
• Data file delivery via SFTP download is supported, and can be combined with PGP file encryption.
  • SFTP file transfer can also be enforced on the company level, preventing Confirmit Horizons from delivering exported data via email. SFTP connections can be authenticated by username/password, private/public certificate or a combination of both methods for maximum security.
  • Confirmit Horizons also supports uploading exported files to remote (client-controlled) servers using either FTP or SFTP connections (and similarly for pulling remote files for import into the system).
• For our own employees, all data exports from Confirmit Horizons are enforced PGP encrypted before transfer. Further, all of our employees with access to client data work on laptops encrypted with Microsoft BitLocker (AES256).
• Confirmit Horizons e-mail servers use TLS encrypted transmissions by default if the remote servers support it. TLS can also be enforced for specific target domains if required, preventing unencrypted delivery altogether.
  • Furthermore, we maintain valid DNS records for all email infrastructure, and use SPF, DKIM and DMARC technologies where applicable.
• Confirmit can assign an e-mail server with a Dedicated Mail Server IP Address* to your company, and deliver survey URLs with your company name in the URL.
• Fixed Sender Domain and Dedicated Mail Server IP Address* reduces the risk of emails being treated as spam.

* Subject to licensing of relevant Confirmit add-on feature
More Sources for Security Information

• The Confirmit Horizons software does not serve cookies to ordinary web-based respondents. To learn more about Confirmit and the “Privacy and Electronic Communications (EC Directive) Regulations 2011, go to https://www.confirmit.com/Cookie-Policy/

• The security features available are presented on our Extranet. You can point your own clients there for reassurance. Visit http://extranet.confirmit.com/library/security.aspx (this page also contains a link to download this document).
• 60.2 million *completed* questionnaires in 2016 across US, EURO and Australian environments.

• Average server response time per questionnaire page: <90 milliseconds.

• A total of 3.16 billion questionnaire pages processed in 2016.
  - 5 to 10 million questionnaire pages are processed every weekday on average.

• Our largest clients run 3 to 4 million completed questionnaires per year on the Confirmit SaaS sites.

• Uptime in 2016:
  - 99,998% on US site – *(9 minutes outage)*
  - 99,995% on EURO site – *(28 minutes outage)*
  - 100% on AUS site

• Quarterly uptime stats for data collection publicly available from: [https://www.confirmit.com/Products/Confirmit-Horizons/#security-and-scalability](https://www.confirmit.com/Products/Confirmit-Horizons/#security-and-scalability)
Hosting with Rackspace

• Confirmit Horizons SaaS environment hosted with world-leading managed hosting provider Rackspace.
  - We have been using Rackspace for our server hosting since 2004, and have current agreements in place through March 2019. We have a strong relationship with high management visibility.

• Rackspace:
  - Recognized world-leading provider of managed hosting services, highly secure and ticking all compliance boxes:
    - [https://www.rackspace.com/certifications](https://www.rackspace.com/certifications)
  - Holds several awards and certifications, including:
    - SSAE 16 Type II SOC 1 (formerly SAS 70 Type II), SOC 2 (Security and availability only), and SOC 3
    - ISO 27001:2013 certified.
    - Microsoft Gold Certified.

• We are on Intensive Hosting with Rackspace, i.e. not “co-location” or standard, reactive “Managed hosting”. This means (i) Highest available SLAs; (ii) Dedicated service delivery team with SLM and technical specialists dedicated to our account; (iii) Aggressive hardware replacement guarantees
Confirmit Horizons SaaS: Not a ‘cloud’ service

• Confirmit provides its software as a web application that is available worldwide, over the Internet, accessible through a standard web browser.

• Does this make Confirmit Horizons SaaS a cloud service? – Not really, and here’s why:
  
  • Companies offering services from the cloud will often use a hosting solution where the server infrastructure is provided by the cloud provider as either Infrastructure as a Service (IaaS) or Platform as a Service (PaaS), such as Amazon’s EC2, Microsoft Azure or Rackspace Cloud. With cloud infrastructure/platform providers, the underlying infrastructure resources is usually shared between all the provider’s customers. Data is also comingled between customers, and there is usually no dedicated security infrastructure that provides additional security for the data hosted on these services.
  
  • Confirmit delivers Software as a Service from a traditional server platform hosted with Rackspace, in a known data center location, and on server hardware that are fully dedicated to Confirmit.
  
  • Although Rackspace also offers cloud services through its Rackspace Cloud offering, Confirmit does not utilize any of these services for its SaaS offerings.
  
  • The Confirmit SaaS service provides end users with the same ease of access as a cloud service, but there are some important differences:
    o *We know exactly where your data is located*
    o The servers hosting the data do not host or process any data for other Rackspace customers but Confirmit (even the VMware hypervisors are dedicated to running our virtual infrastructure)
    o Database services are separated from virtual infrastructure and run on dedicated servers
    o We have a dedicated, redundant, multi-tier network security infrastructure protecting our equipment
    o All our data is stored on dedicated SAN arrays and is not co-mingled with other Rackspace customers’ data (our Australia based environment being an exception, until further notice)
Confirmit Horizons EURO SaaS Architecture

Network Overview
Hosting Environment Security

• State-of-the-art physical building security at Rackspace:
  • On-site security personnel monitor the data center buildings 24/7.
  • Live CCTV surveillance of the entire data center building is monitored 24/7. Biometric hand scanners are used to restrict access to the Rackspace data center.
  • Multiple levels of security are employed to ensure that only Data Center Operations Engineers are physically allowed near the hosted routers, switches, and servers.

• All critical systems in the DC are N+1 redundant to provide uninterrupted availability (Power Distribution Units, UPS systems, NIC teams, database clusters, virtualization hypervisors, virtual servers, SAN fiber connections, storage groups, switches, load balancers and firewalls). Weekly tests are conducted on all HVAC, UPS, fire suppression, and generator systems.

• Standard hardware and software supplied by industry leading vendors used for all parts of the delivery chain.

• Clustered database servers, load balanced application servers for high availability.

• Dedicated SAN arrays (EMC VNX2 5x00 series)*.

*For the Confirmit Horizons Australia SaaS Environment, storage is provisioned from Rackspace shared SAN infrastructure.
Hosting Environment Security

• All network infrastructure devices are configured in high availability mode, providing a fault-tolerant network for 100% guaranteed network uptime from the hosting provider.

• Network segregation*, with Cisco ASA as perimeter firewalls, Juniper SRX for internal segmentation.
  *For the Confirmit Horizons Australia SaaS Environment, F5 Big-IP devices are used as perimeter firewalls, while Cisco ASA is used for internal segmentation.

• F5 Big-IP load balancers with SSL acceleration is utilized to ensure high availability and performance.

• HTTPS (TLS) encryption enforced for all authentication requests and available for all web facing servers

• Encryption of data available during transit and at rest; SFTP file transfer, PGP file encryption, TLS-encrypted email when supported on recipient end, data encryption at rest through SQL Server Enterprise Transparent Data Encryption

• AlertLogic Threat Manager (IDS / IPS), monitored 24/7 by AlertLogic SOC and updated regularly with new traffic detection patterns.

• Daily backups. Weekly full back-ups and sent for off-site storage for 12 months* with Iron Mountain. Backups are encrypted twice (AES-256 encrypted both by our backup software, and again when backing up to tape media).
  *Off-site backups available for 12 weeks for the Confirmit Horizons Australia SaaS Environment.

• Complete SaaS environment documentation available under NDA.
Data Privacy – Compliance Accomplished

• Our US data center provider (Rackspace, Inc.), as well as our US entity (Confirmit, Inc.), both acting as data importers of personal data originating from the European Economic Area, operate in accordance with Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This is achieved via Data Transfer / Processing Agreements including EU Model Clauses.

• Additionally, both Confirmit and Rackspace are Privacy Shield certified. The EU(EEA)-US Privacy Shield is a replacement for Safe Harbor (which stopped having effect in October 2015). The Privacy Shield model is managed by the International Trade Administration (part of the US Department of Commerce). The Privacy Shield certified listing is available [here](#).

• Further, we offer an Horizons SaaS in Australia, so to help companies meet requirements for localization of data in that region under the Australian Privacy Act.
Ongoing Static Application Code Vulnerability Testing

Confirmit perform static code-scanning of the Horizons software:

- **Integrated** into our Software Development Life Cycle
- **Reputable**: Partnered with industry leader, VERACODE
  Thoroughly tests the OWASP Top 10
- **Automated** scans ensures flaws are systematically detected and reported
- **Frequent** scanning rapidly identifies vulnerabilities for remediation
- **Inclusive** testing of third-party libraries (in addition to Confirmit’s own software)
Ethical Hacking / Application Vulnerability Assessments

• Confirmit commission independent third party security specialists to run application testing of Confirmit Horizons software. The tests are run annually.
  - Application testing: We grant a user a valid password and User ID to the Software, and see if they can “hack” any part of the system, i.e. gain illegitimate access to data, elevate permissions, compromise the software, etc.

• Any relevant findings are promptly corrected and retesting is carried out to verify fixes.

• Transparency: Report is made available to clients upon request.

• We have been always awarded the highest grade (“A”).
  - Results from the latest test (November 2016):

<table>
<thead>
<tr>
<th>Service</th>
<th>High</th>
<th>Medium</th>
<th>Security</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional Authoring</td>
<td>0</td>
<td>0</td>
<td>Highly Secure</td>
<td>A</td>
</tr>
<tr>
<td>Survey Designer</td>
<td>0</td>
<td>0</td>
<td>Highly Secure</td>
<td>A</td>
</tr>
<tr>
<td>Discover Analytics</td>
<td>0</td>
<td>0</td>
<td>Highly Secure</td>
<td>A</td>
</tr>
<tr>
<td>Active Dashboard</td>
<td>0</td>
<td>0</td>
<td>Highly Secure</td>
<td>A</td>
</tr>
<tr>
<td>Action Management</td>
<td>0</td>
<td>0</td>
<td>Highly Secure</td>
<td>A</td>
</tr>
<tr>
<td>Report Viewer</td>
<td>0</td>
<td>0</td>
<td>Highly Secure</td>
<td>A</td>
</tr>
<tr>
<td>Password Protected Survey</td>
<td>0</td>
<td>0</td>
<td>Highly Secure</td>
<td>A</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>0</td>
<td>0</td>
<td>Highly Secure</td>
<td>A</td>
</tr>
</tbody>
</table>

Table 3: Foundstone Grading Criteria

- **A** Highly Secure: Attention to security assets and policies are implemented effectively and consistently. No high and medium risk vulnerabilities.
- **B** Moderately Secure: Attention to security assets but there are issues with the completeness of the organization’s security policy or the organization’s ability to execute its security objectives consistently. This is reflected in the identified vulnerabilities, with no high risk issues found.
- **C** Marginally Secure: Attention to security assets but there are issues with the completeness of the organization’s security policy or the organization’s ability to execute its security objectives consistently. This is reflected by the presence of high risk vulnerabilities being identified that could be exploited.
- **D** Insecure: Attention to security assets requires improvement. Significant gaps in security policy exist and/or execution issues prevent the organization from securing its critical assets from attacks. A large number of high risk vulnerabilities were identified during the assessment.
Network Security / Penetration Testing

• Confirmit commission independent third party security specialists to run external vulnerability testing of the environment hosting the Confirmit software. Tests are performed at least annually.
  • Network Security / Penetration testing: Try to gain access to the SaaS environment without knowing any valid credentials, probing for unnecessary/unsecured running services, verifying best practices for service hardening.

• Any relevant findings are promptly corrected and retesting is carried out to verify fixes.
• Transparency: Report is made available to clients upon request.
• We have always been awarded the highest grade (“A”).
  • Results from the latest test (July 2016):

In the results [...], Foundstone determined that:

• “The hosts that Foundstone located on the network contained no high risk and few medium risk vulnerabilities, indicating that host deployment and maintenance were performed in a timely and controlled fashion for those key Internet accessible resources.”

• “It appears that close control is maintained on the Internet accessible hosts, allowing rapid response to issues reported during the assessment, as most issues identified during testing were resolved immediately.”

<table>
<thead>
<tr>
<th>Table 4: Report Card After Retest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>External Network Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5: Foundstone Grading Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grade</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>A</td>
</tr>
<tr>
<td>B</td>
</tr>
<tr>
<td>C</td>
</tr>
<tr>
<td>D</td>
</tr>
</tbody>
</table>
Three-tier 24/7/365 monitoring

• Confirmit monitors the hosting environment and the Confirmit application 24/7 by means of its proprietary NOC monitor.
  - The NOC polls critical application statistics with high frequency. E-mail, SMS alarms, and automated calls are triggered if irregularities are detected.
  - Confirmit also monitors application logs through dashboards using an ELK cluster.

• Rackspace monitors the SaaS 24/7 by means of 3 applications: Microsoft (SCOM), SiteScope, and RackWatch (Rackspace proprietary application).
  - Rackspace will call Confirmit engineers if severe issues persist for more than 15 minutes.

• Neustar WPM (https://home.wpm.neustar.biz/) performs external monitoring of availability and response times on US, EURO and AUS sites for live applications:
  - Data Collection, CATI, Reportal, Authoring, Active Dashboards and Action Management.
Polling is performed from a global monitoring network.
Thank You

Arnt Feruglio | COO