Confirmit

Cloud Security for Confirmit Horizons

Vandy Hamidi
Chief Information Security Officer

January 2021 – Confirmit Horizons on Microsoft Azure

About this document

- **This document describes the Confirmit Horizons cloud environments, and the security mechanisms we have in place to protect your data.**
- **This document is “Unclassified” and can be shared freely.**
  - Updated version of this document will be made available for download quarterly from https://extranet.confirmit.com/library/security.aspx#tab1

Content

1. **Horizons Software: Security and Availability**
2. Cloud Data Center: Microsoft Azure
3. Third Party Attestations / Auditing

The Confirmit Horizons Software

- From its inception in 1997, the architecture and code of the Confirmit Horizons software has been designed for web deployment.

- The architecture and code of the Confirmit Horizons software has over time been enhanced for Microsoft Azure cloud deployment, making a live site a reality in 2018.

- 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 tiered proactive 24/7 monitoring, this provides our cloud clients with the high security, performance and availability.

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 cloud environment include:**
  - 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.
  - Passwords are checked towards known breached password database upon change
  - 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 two-factor authentication to their account. Two-factor access is enforced for Confirmit employees.
  - Confirmit Horizons automatically locks application access for Authoring users after a period of inactivity (60 minutes), after which users must re-enter their password to unlock the application.
  - System detects logins from new or unknown location and notifies user via email

Security in Confirmit Horizons End-User Connections

- **HTTPS (TLS) enforced for all end-user connections.**
  - This applies to connections to surveys, authoring activities, panel portals and reports.
  - Strict Transport Security on all connections forces client browsers to only send HTTPS requests.

- **Confirmit Horizons automatically locks application access for Reportal users after a period of inactivity (60 minutes), after which users must re-enter their password to unlock the application.**
- **Panel portals may be configured with custom password policies to protect panelist data.**
- **Default brute-force prevention on all login forms.**
- **Azure DDOS prevention enabled**

Security of Data

- The database servers that store respondent and response data utilize the Microsoft Azure SQL database service 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 through network controls and secure VPN tunnels with dual factor authentication (2FA). 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 certificates from reputable vendors, providing additional safety for visitors.
- All client data is stored using strong 256bit encryption.

Additional Security Features

- **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.

1. Horizons Software: Security and Availability

2. Cloud Data Center: Microsoft Azure

3. Third Party Attestations / Auditing

Microsoft Azure

Confirmit

- **The Confirmit Horizons cloud platform is hosted with Microsoft Azure**
- **State-of-the-art physical building security at Microsoft Azure data centers:**
  - 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 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.
- **Azure data centers are highly secure. Please refer to**
  - https://www.microsoft.com/en-us/trustcenter/security/azure-security
  - https://azure.microsoft.com/en-us/blog/azure-layered-approach-to-physical-security/

Microsoft Azure

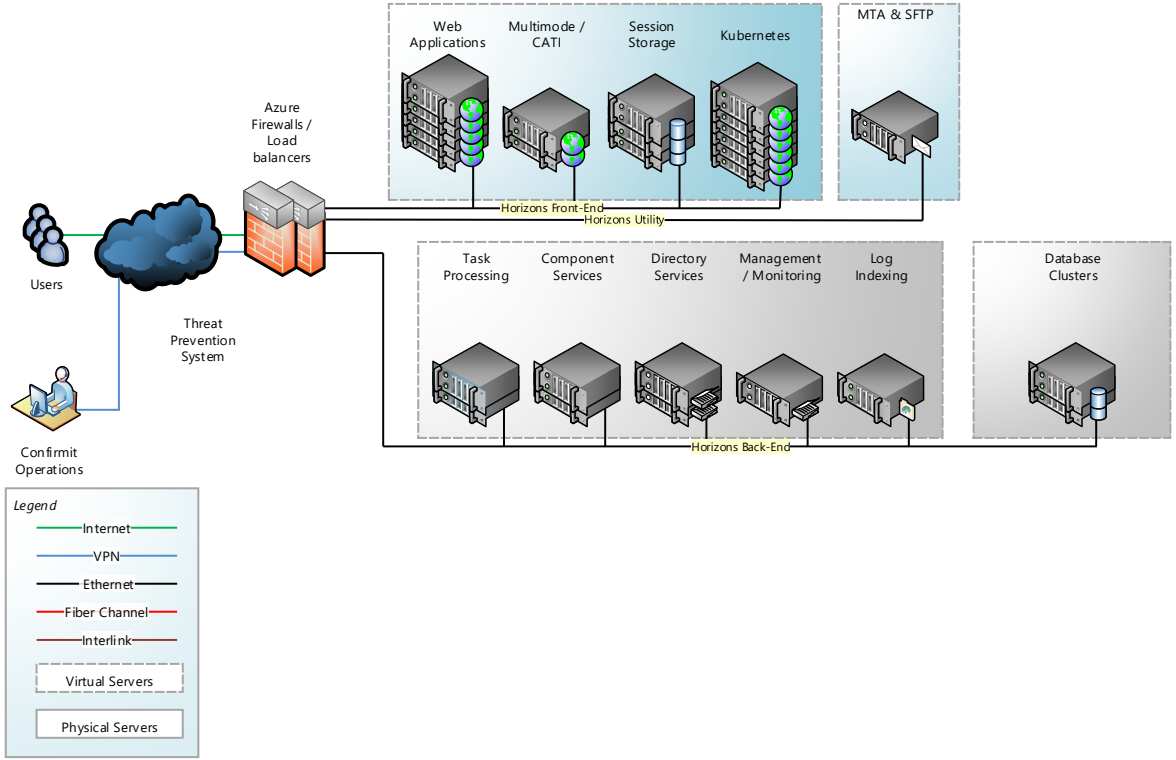
Confirmit

- **Compliance:**
  - ISO 27001:2013 certified
  - SOC 2 Type II audited (SSAE 18) for Security, Confidentiality, Availability, Privacy and Process Integrity
  - PCI-DSS compliant
  - HIPAA Business Associate
  - Details regarding these certifications and security can be found at:
    - https://azure.microsoft.com/en-us/overview/trusted-cloud/

ISO/IEC

HIPAA

Confirmit Horizons Azure Architecture



1. Horizons Software: Security and Availability

2. Cloud Datacenter: Microsoft Azure

3. Third Party Attestations / Auditing

Weekly static code-scanning of the Horizons software

- ☑ **Integrated** into our Software Development Life Cycle
- ☑ **Reputable:** Partnered with industry leader, VERACODE:

  https://www.veracode.com/products/static-analysis-sast/static-code-analysis
- ☑ **Automated** scans ensure systematic detection and reporting
- ☑ **Frequent** weekly scanning for rapid identification and remediation
- ☑ **Inclusive:**

  Thorough tests based on OWASP Top 10

  Includes 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 Horizons 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 rating after retest.**
  - Results from the latest test (December 2020):

VERACODE

APPLICATION SECURITY REPORT

ConfirmIt

Confirmit Horizons

Manual Analysis

FINDINGS BY SEVERITY

	Manual Penetration Testing (MPT)
Very High	0
High	0
Medium	0
Low	0
Very Low	0
Informational	1

Network Security / Penetration Testing

- ☑ **Frequent:** Confirmit run weekly automated network penetration and system vulnerability scans of the SaaS Platform.
- ☑ **Thorough:** The scans include all external facing IPs of the hosting infrastructure, no exceptions.
- ☑ **Independent:** Confirmit also commission third-party security specialists to run a thorough external vulnerability test of the Confirmit SaaS infrastructure. Tests are performed at least annually.
- ☑ **Reputable**: We partner with McAfee, a division of Intel Security, for the third-party annual tests. We employ Tenable's highly-rated Nessus Scanner for the weekly tests.
- ☑ **Verified:** Relevant findings are remediated and retested to confirm fixes.
- ☑ **Transparent:** Reports are made available to all clients upon request.
- ☑ **Effective:** We have always been awarded the highest grade ("A").

In the latest report (October 2020), McAfee stated that:

"[...] a number of positive security aspects were readily apparent during the assessment:

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

Table 4: Report Card after Retest

Service	High	Medium	Low	Security	Grade
External Network Penetration Testing	0	0	3	Highly Secure	A

Table 5: McAfee Grading Criteria

Grade	Security	Criteria Description
A	Highly Secure	Attention to security exists and policies are implemented effectively and consistently. **No high and medium risk vulnerabilities.**
B	Moderately Secure	Attention to security exists 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 exists but there are issues with the completeness of the organization's security policy or the organization's ability to execute its security objectives consistently for all assets tested. This is reflected by the presence of **high-risk vulnerabilities** being identified that could be exploited.
D	Insecure	Attention to security requires improvement. Significant gaps in security policy exist and/or execution issues prevent the organization from securing its critical assets from attack. A large number of high-risk vulnerabilities were identified during the assessment.

Confirmit Horizons is (SOC) 2 Type II audited

What is System and Organization Controls (SOC) 2?

- ☑ Third-party assurance of controls and control effectiveness
- ☑ Performed by independent accredited auditing firm
- ☑ Internationally recognized standard (SSAE 18 / AT 101)
- ☑ In-depth review of Security, Confidentiality and Availability

We have engaged armanino LLP who are:

- ☑ Ranked among the 100 largest CPA firms in the U.S.A. by Accounting Today
- ☑ Dedicated Controls Assurance practice with extensive SOC 2 experience
- ☑ Recent PCAOB inspection report revealed absolutely zero deficiencies in sampled audits

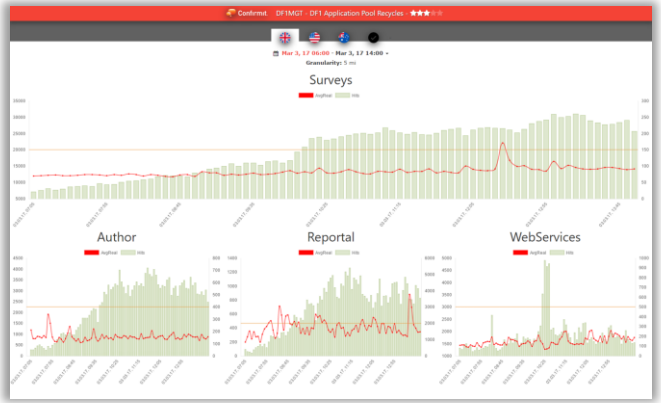
Dates of attainment:

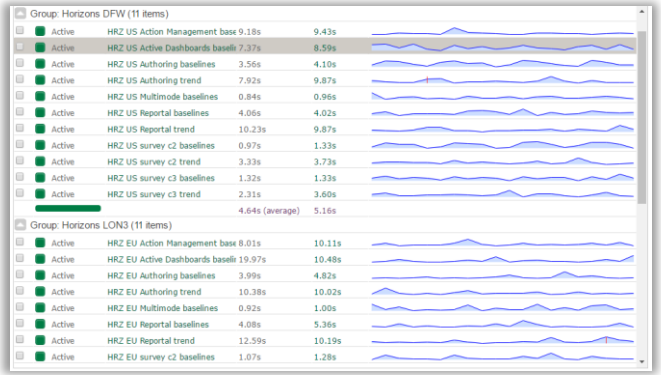
- ☑ SOC 2 Type II – Completed Q2 - 2020, report available under NDA
  - Next SOC 2 Type II report available end of Q1 2020 for the period of April 1, 2020 to March 31, 2021

Two-tier 24/7/365 monitoring

- **Confirmit monitors the availability and performance of the Horizons SaaS 24/7 by means of its proprietary NOC dashboard.**
  - The NOC polls critical application statistics with high frequency. E-mail, SMS alarms, and automated calls are triggered if irregularities are detected.
  - The NOC dashboard integrates with PRTG (third party tool) and shows alerts and performance statistic in a common interface.
  - Confirmit also monitors application service and access logs using Kibana dashboards (backed by Elasticsearch / Logstash clusters).

- **Site24x7 (https://www.site24x7.com/) performs external monitoring of availability and response times on SaaS sites for live applications:**
  - Data Collection, CATI, Report, Authoring, Active Dashboards and Action Management.
  - Polling is performed from a global monitoring network.





Thank You

Confirmit

