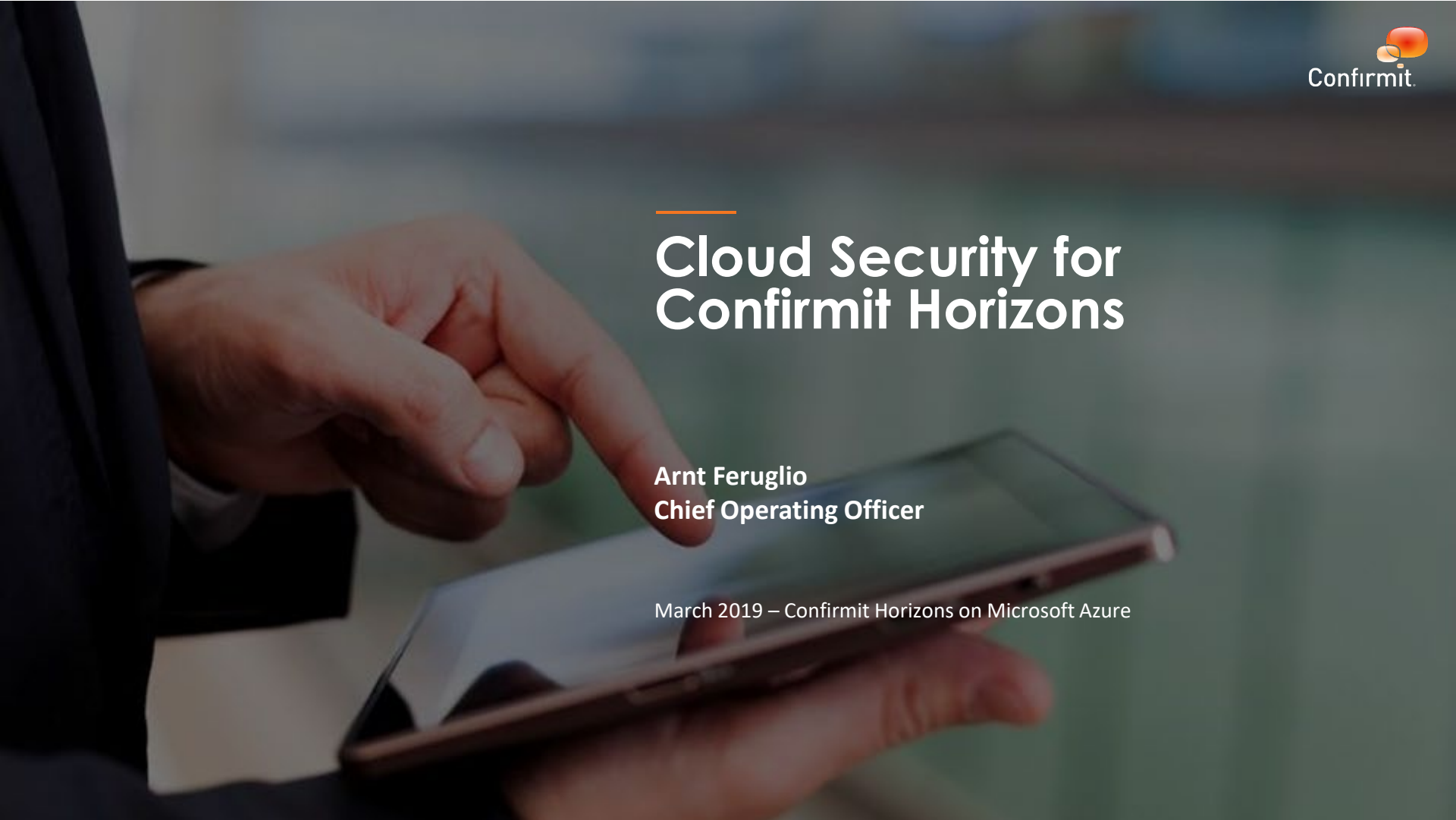


Confirmit

Cloud Security for Confirmit Horizons

Arnt Feruglio
Chief Operating Officer

March 2019 – 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 with a limited feature set 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:**
  - HTTPS (TLS) enforced for all transmission of credentials, and full session HTTPS is mandatory for all applications.
  - All user accounts are named, personal (not shared) accounts linked to an individual email address, and have an expiration date set in line with contract 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 cloud 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 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. 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 certificates from reputable vendors, providing additional safety for visitors.
- All survey databases using Azure databases will be encrypted

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

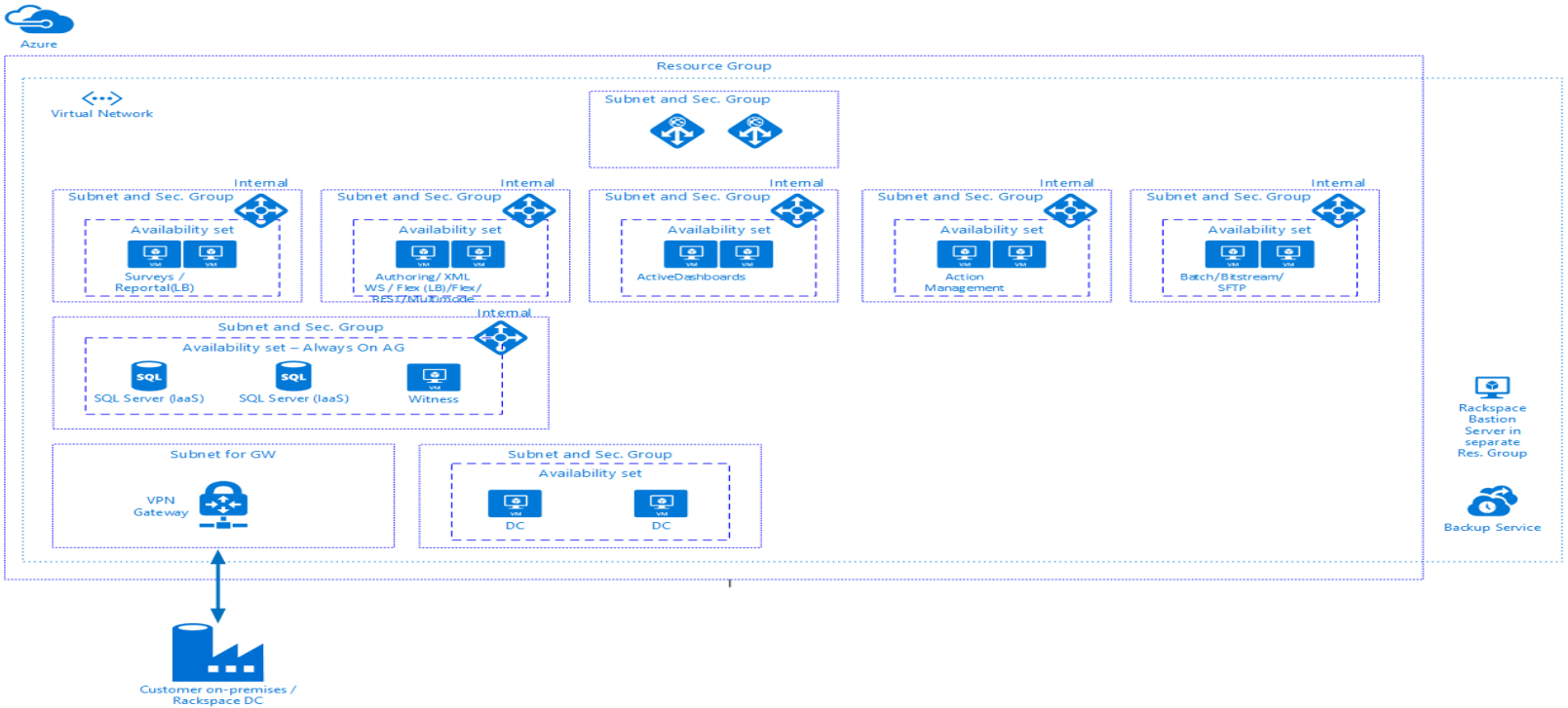
- **The Confirmit Horizons cloud platform is hosted with Microsoft Azure**
- **State-of-the-art physical building security at Microsoft Azure data centers:**
  - On-site security personnel monitor the data center buildings 24/7.
  - Live CCTV surveillance of the entire data center building is monitored 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

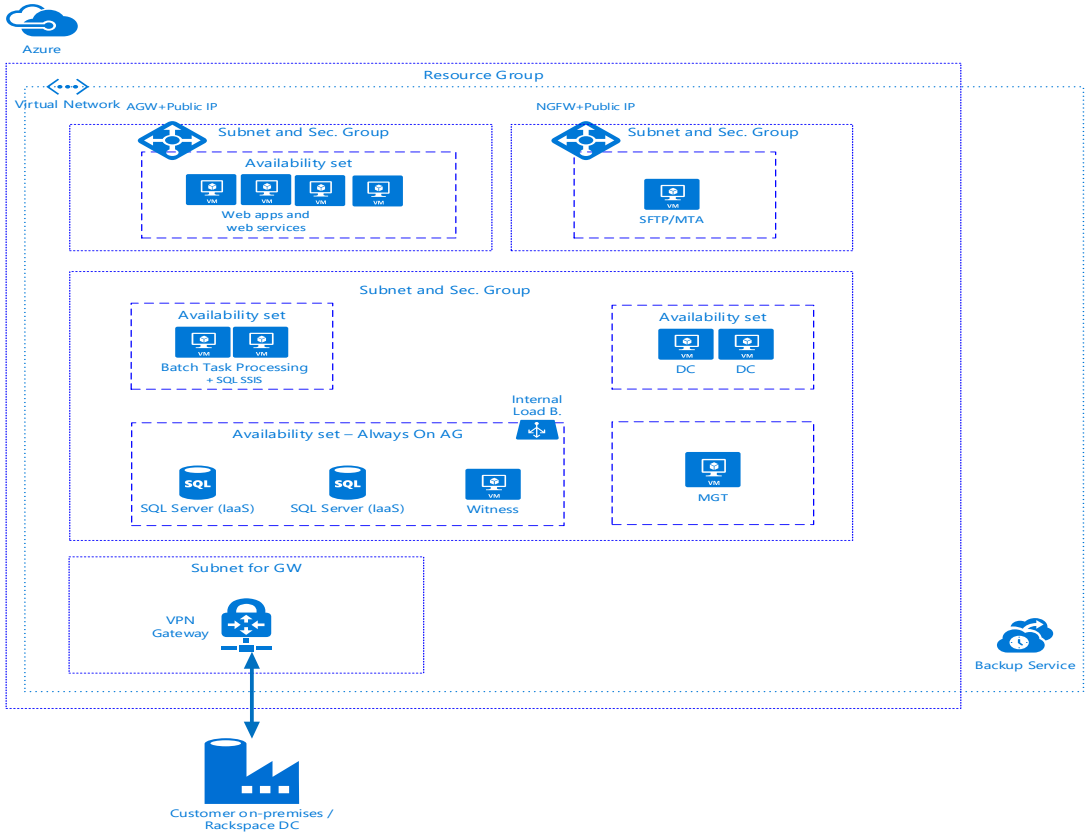
Confirmit

- **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/

Confirmit Horizons Canada East Cloud Architecture



Confirmit Horizons Hong Kong Cloud 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

Confirmit

- ☑ **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 2018):

VERACODE

APPLICATION SECURITY REPORT

ConfirmIt

Dec 03, 2018

Confirmit Horizons

Manual Analysis

Analysis Type: Penetration Test
Analysis Date: November 28, 2018
Scan Name: Confirmit Horizons 24.0.370

Summary of the final findings, after mitigations:

Flaw Severity	Flaw Count
Very High	0
High	0
Medium	0
Low	4
Very Low	0
Informational	2

Network Security / Penetration Testing

- ☑ **Frequent:** Confirmit run weekly automated Nessus network penetration and system vulnerability scans of the cloud Platform.
- ☑ **Thorough:** The scans include all external facing IPs of the hosting infrastructure, no exceptions.
- ☑ **Verified:** Relevant findings will be remediated and retested to confirm fixes.

From the summer of 2019 we will include the Canada and Hong Kong Cloud sites in our yearly third party testing as follows:

- ☑ **Independent:** Confirmit will commission a third-party security specialist (planned to be McAfee) to run thorough external vulnerability test of the Horizons Cloud infrastructure.
- ☑ **Transparent:** Reports will be made available to all clients upon request

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 1 and SOC 2 Type II – Completed Q2 - 2018, report available under NDA
  - Next SOC 2 Type II report available in Q2 2019 for the period of April 1, 2018 to March 31, 2019

Thank You

Arnt Feruglio | COO

Confirmit

