

---

# SaaS Security for Confirmit Horizons

**Vandy Hamidi**  
Chief Information Security Officer

January 2021 – Confirmit Horizons

- **This document describes the Confirmit Horizons SaaS 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>

The information and facts contained in this document are provided in good faith and to the best of the knowledge of the author at the time of publication. Confirmit makes no representations and gives no warranties of whatever nature in respect to this document.

---

# Content

- 1. Horizons Software: Security and Availability**
2. SaaS Data Center: Rackspace
3. Third Party Attestations / Auditing
4. Privacy Laws Compliance

# The Conconfirm Horizons Software

- **From its inception in 1997, the architecture and code of the Conconfirm 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.**
- **Combined with our 3-tier proactive 24/7 monitoring, this provides our SaaS clients with the highest levels of security, performance and availability in the industry.**

# Security in Conformat Horizons Authoring

- **By default, only the Conformat 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 Conformat's Horizons SaaS 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 Conformat 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 Conformat employees.
  - Conformat 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 Conconfirm 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.
- **Conconfirm 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.**
- **Rackspace DDOS prevention enabled**

- 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 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.
- Confirmit Horizons SaaS data is encrypted at rest using full SAN encryption(EMC D@RE)

# Additional Security Features

- **Enforcement of HTTPS encryption for all authoring / reporting / survey activity for all users.**
  - Only modern and secure TLS 1.2 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 (“Opportunistic TLS”) by default if the receiving servers support it. STARTTLS may 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.
  - We support DKIM for customer email domains.
- **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.**

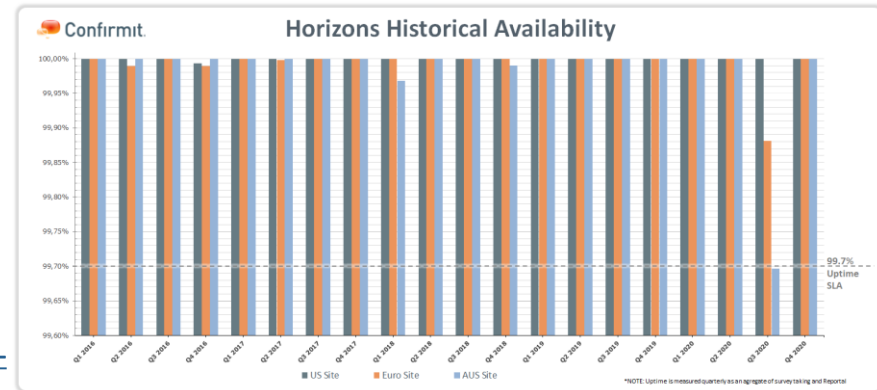
\* Subject to licensing of relevant Confirmit add-on feature

# Confirmit Horizons SaaS Environment

## Uptime and Statistics



- 66 million *completed* questionnaires in 2020 across US, Europe, Australia and Canada environments.
- Average server response time per questionnaire page: <90 milliseconds.
- A total of 3.59bn questionnaire pages processed in 2019.
  - 9.7 million questionnaire pages are processed every weekday on average.
- Our largest SaaS clients run 3 to 4 million completed questionnaires per year.
- Uptime in 2020:
  - 100% on US site
  - 99.97% on Euro site
  - 99.924% on Australia site
- Quarterly uptime stats for data collection publicly available from:  
<https://www.confirmit.com/Products/Confirmit-Horizons/#security-and-scalability>



- 
1. Horizons Software: Security and Availability
  - 2. SaaS Data Center: Rackspace**
  3. Third Party Attestations / Auditing
  4. Privacy Laws Compliance

# Hosting with Rackspace

- **Confirmit Horizons SaaS environment hosted with world-leading managed hosting provider Rackspace.**
  - We have partnering with Rackspace for our SaaS server hosting since 2004. We have a strong relationship with high management visibility.
  - Current agreements in place throughout April 2022.
- **Rackspace:**
  - Recognized world-leading provider of managed hosting services, highly secure and ticking all compliance boxes:
    - <https://www.rackspace.com/certifications>
  - Holds several awards and certifications, including:
    - SOC 1, SOC 2, and SOC 3 (<https://www.rackspace.com/compliance/soc>)
    - ISO 27001:2013 certified (<https://www.rackspace.com/compliance/iso>)
    - 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

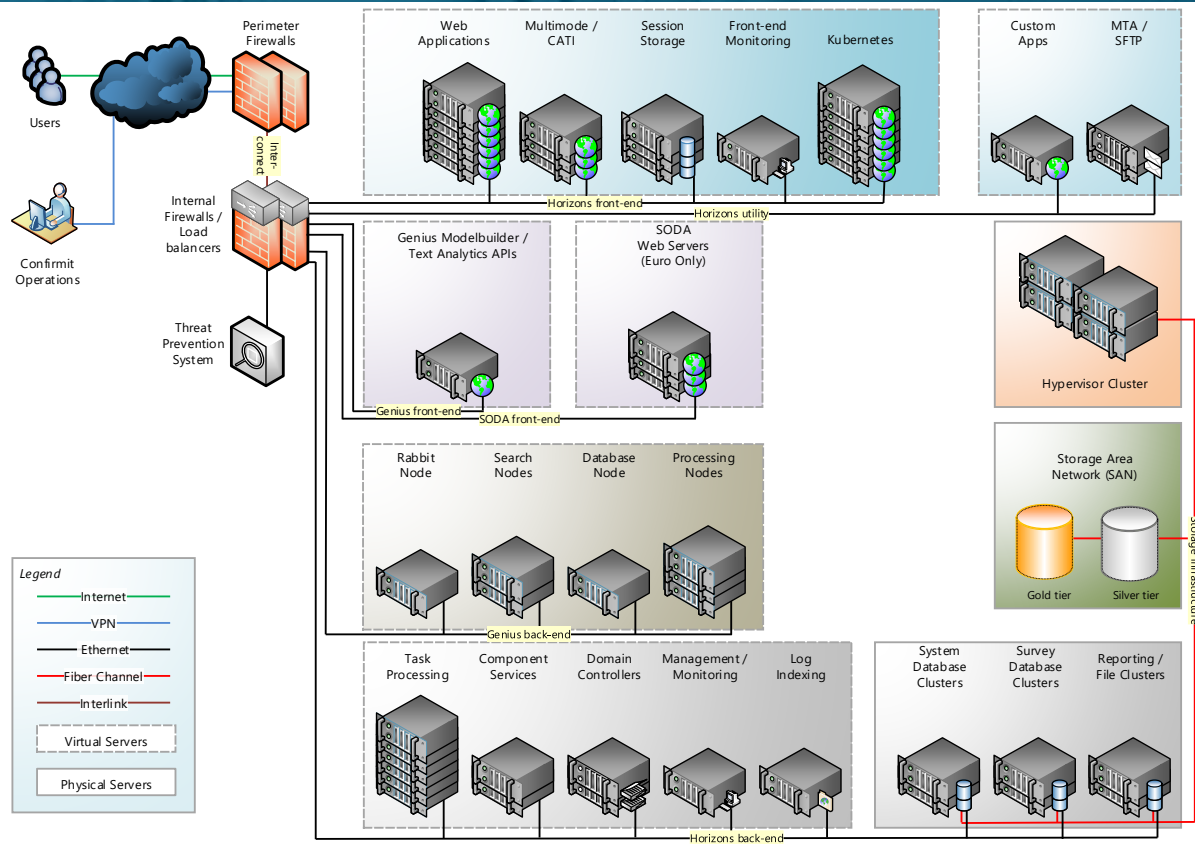


# Confirmit Horizons SaaS: Not a 'cloud' service

- **Confirmit provides its software as a web application that is available worldwide, over the Internet, accessible through a standard web browser.**
  - ◆ Unlike cloud:
    - We know exactly where your data is located
      - > Choose between UK, US or Australia
    - The servers hosting the data ***do not host or process any data for other Rackspace customers but Confirmit***
    - Database services run on ***dedicated servers***
    - We have a ***dedicated, redundant, multi-tier network security infrastructure*** protecting our equipment
    - 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)

# Conformit Horizons SaaS Architecture

## Network Overview



- **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 Unity Series)\*.**

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

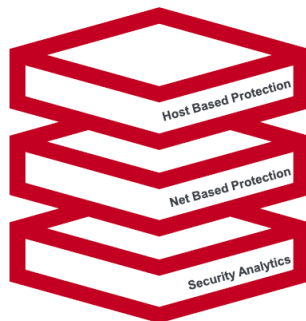
- **All network infrastructure devices are configured in high availability mode, providing a fault-tolerant network for 100% guaranteed network uptime from the hosting provider.**
- **Network segregation, with dual vendor firewalls, with internal segmentation.**
- **Load balancers with SSL acceleration is utilized to ensure high availability and performance.**
- **Daily backups. Weekly full back-ups and sent for off-site storage for 12 months\*. 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.**

# Hosting Environment Security: Rackspace Managed Security

- Rackspace Managed Security services are utilized for the Horizons SaaS infrastructure.
  - <https://www.rackspace.com/managed-security-services>
- 24x7x365 Security Operations Center (CSOC) staffed by GCIA- and GCIH-certified security analysts who are actively hunting for threats
- CrowdStrike host protection (<https://www.crowdstrike.com/>), capable of prevention and detection of threats.
- SIEM capabilities for anomaly detection on the infrastructure and alerting to the CSOC
- Rapid-response remediation – The CSOC is authorized to perform pre-approved actions and remediation 24 hours a day w/o needing to reach out to us.

## THE CSOC 'TRIPLE STACK'

- Host Based Protection
  - CrowdStrike partnership
  - Kernel-level agent
  - Combines IOC and IOA detection
- Net Based Protection
  - Visibility where agents can't go
  - Inbound and outbound C&C traffic
- Security Analytics
  - Advanced SIEM capability
  - Augmented by behavioural analytic capability
  - Enabling not replacing analyst expertise



## CYBER HUNTING

- What is Cyber Hunting?
  - Proactive analysis of data
  - Generic and targeted (focused) hunting
- Why do we Hunt?
  - Catch what is missed by tools
- How does Hunting improve security posture?
  - Earlier detection in the Attacker Life Cycle
  - Fills gaps in tool visibility



- 
1. Horizons Software: Security and Availability
  2. SaaS Data Center: Rackspace
  3. **Third Party Attestations / Auditing**
  4. Privacy Laws Compliance

# 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 and ongoing detection and reporting
- ✓ **Frequent** weekly scanning for rapid identification and remediation
- ✓ **Inclusive:**
  - Thoroughly tests the 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.



McAfee Professional Services  
Advanced Cyber Threat Services  
Technical Report Executive Summary  
Prepared for Confirmit  


# 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<sup>✦</sup> LLP who are:

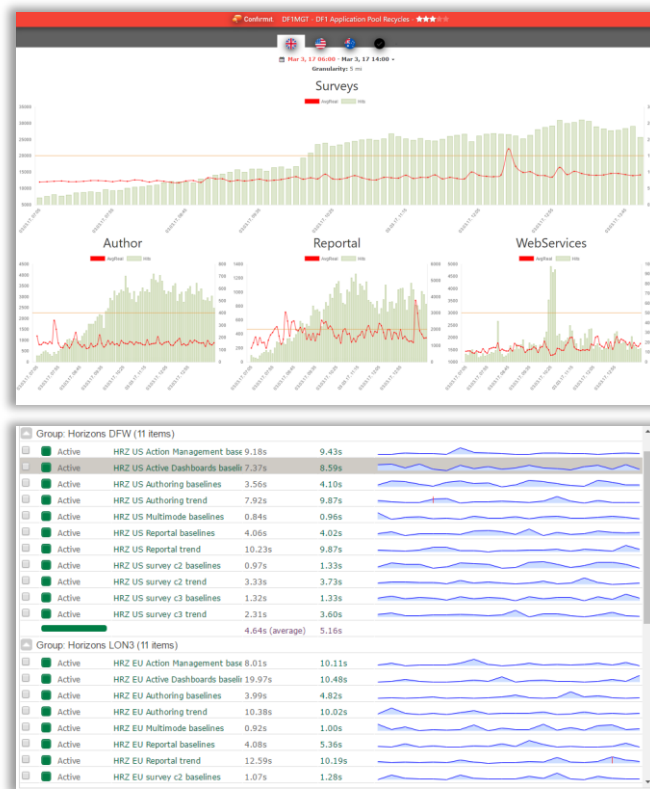
- ☑ Ranked among the 100 largest CPA firms in the U.S.A. by Accounting Today
- ☑ Dedicated Controls Assurance practice with extensive SOC 2 experience
- ☑ Recent PCAOB inspection report revealed absolutely zero deficiencies in sampled audits

## Dates of attainment:

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

# Three-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).
- **Rackspace monitors 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.
- **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.



- 
1. Horizons Software: Security and Availability
  2. SaaS Data Center: Rackspace
  3. Third Party Attestations / Auditing
  4. **Privacy Laws Compliance**

- Confirmit is GDPR compliant, both in respect to our ***Horizons Software***, and in respect to how our ***company*** operates



- See our GDPR Memo for full overview, including mapping of GDPR requirements versus the relevant features in the Horizons SaaS, ref. Appendix 2
  - <https://www.confirmit.com/Legal-Notices/>
- We offer to enter into our GDPR compliant *Data Processing Agreement* and / or *EU Standard Contractual Clauses*

# CCPA-compliant

- Confirmit is compliant with the California Consumer Privacy Act, both in respect to our *Horizons Software*, and in respect to how our *company* operates



- See our CCPA Memo for full overview, including mapping of CCPA requirements versus the relevant features in the Horizons SaaS, ref. Appendix 2
  - <https://www.confirmit.com/Legal-Notices/>
- If your company requires vendors to enter into a certification letter for CCPA compliance, we have this ready for you to countersign here:
  - <https://www.confirmit.com/Legal-Notices/>

# Privacy Laws Compliant Company

- We have in place:
  - GDPR Article 32: “...**appropriate technical and organisational measures to ensure a level of security appropriate to the risk**”



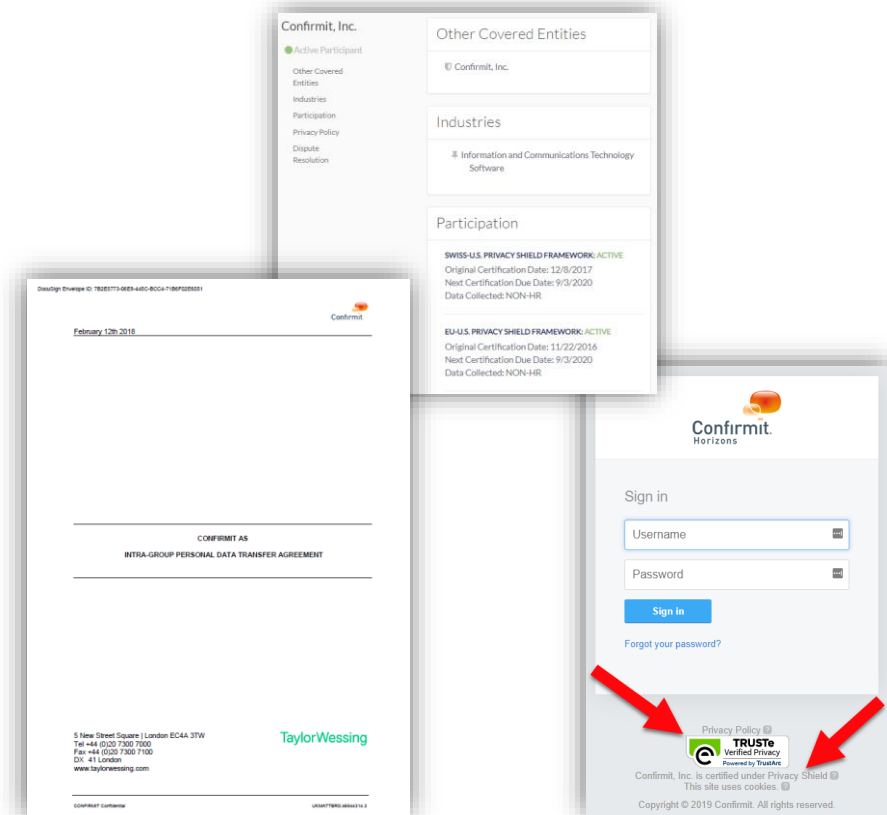
VERACODE



McAfee Professional Services  
Advanced Cyber Threat Services  
Technical Report Executive Summary  
Prepared for Confirmit  
McAfee

# Privacy and Data Transfers

- We have:
  - Verified Privacy via TRUSTe / TrustArc  
Includes “*TRUSTe Feedback and Resolution System*”
  - Intra-Group Data Transfer Agreement based on the ***EU Standard Contractual Clauses*** – Model Clauses
  - GDPR and Privacy Shield\* compliant agreements in place with sub-contractors handling personal data
  - EU/US & Swiss Privacy Shield\* certification via the US Dep Of Commerce



\* Confirmit does not rely upon the Privacy Shield Framework, but still complies

# Thank You

---

