InfinityQS®
Quality Re-imagined

enact®

Enact Security White Paper

Contents

Introduction

At InfinityQS, we are committed to the security of customer data. We strive to be transparent regarding the security measures taken by our third-party cloud services provider—and their compliance to industry standards and regulatory requirements in the markets in which they operate.

The use of cloud-based services is growing rapidly, with the use of software as a service (SaaS) becoming increasingly mainstream. Enact is a SaaS solution that runs on the Microsoft Azure cloud and provides a secure, fully-supported means to optimize your quality data—and operations—across the enterprise.

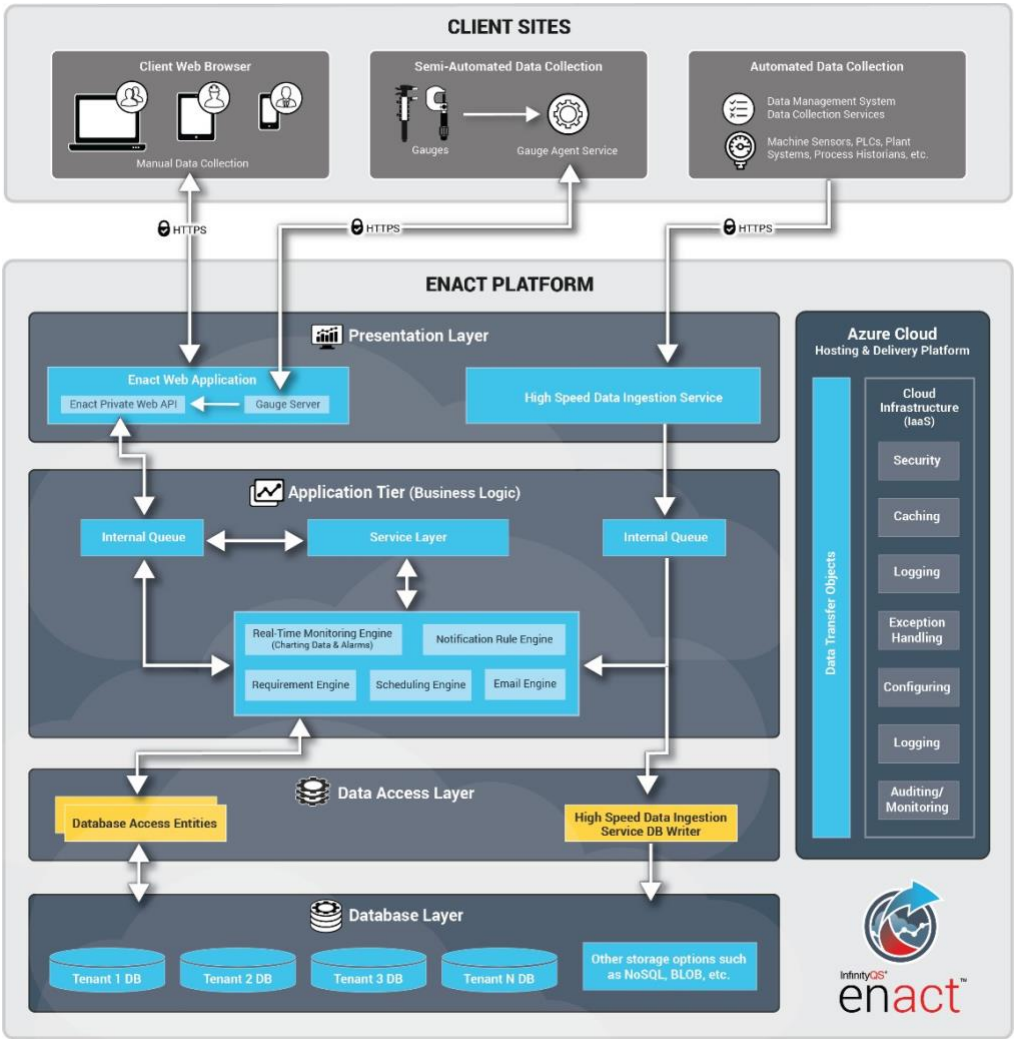
A robust networking infrastructure is included to support applications and service connectivity requirements.

Enact System Architecture

The Enact architecture uses Microsoft Azure to support cloud-based deployments, eliminating the need for local software and the IT burden required to support it. Enact is a premium multi-tenant application where all users/subscribers share the same cloud-hosted application, but each client company is provided a separate data repository or database. All Enact users have access to the latest version of the software while enjoying superior data security. Several cloud-based services are used to make the Enact application scalable, maintainable, usable, available, reliable, securable, and extensible.

Enact follows a 3-tier architecture, separating the externally facing web server from the internal application server and database server. With a tier-based architecture such as this, even if an attacker somehow compromises an externally facing web server from the outside, they still have to find ways to gain access to the internal network.

Enact follows the Open Web Application Security Project (OWASP) security guidelines, which list the most critical web application security flaws and recommended countermeasures.



Public Deployment Architecture

Application Security

The Enact web-based interface is safeguarded by user security, licenses, workstation authentication, and a customizable security policy. The following web browser applications are supported by Enact:

- Internet Explorer 11
- Edge
- Chrome (latest version)
- Safari on iOS

***Please note**: Firefox is not supported.*

Access Security

Enact can only be accessed with an active user account. Users must log in to their account using a username and password. A password can only be created for an account using a legitimate, unique email account accessible by the user. The email address must be kept current to allow for account recovery in the event of a lost password. User accounts are created and maintained by those with the appropriate privileges.

Application Security

Enact is a multi-tenant web application hosted on the Microsoft Azure public cloud. Application security is of paramount importance. Industry best practices, including “The Open Web Application Security Project (OWASP)” guidelines, were incorporated in the Enact application design.

Adherence to Security Guidelines

Using guidelines found in OWASP’s 2013 Top 10 list of cyber threats, InfinityQS addressed the following security factors during the design and development of the Enact application.

Injection Flaws

The potential threat from this flaw is that an attacker could trick the application into executing unintended commands or into changing system data. Injection flaws, particularly database injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Counter measure

The Enact application uses ORM to connect to the database, which inherently takes care of this. Also, parameter values passed to stored procedures are escaped before the DB call is made. No dynamic query is being generated in code. Dynamic stored procedures are also executed through database functions, which prevents database injection.

Broken Authentication & Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

Counter measure

The Enact application design ensures that the user only has specific privileges to access those functions that they are authorized to access, restricting access to the backend database, as well as the ability to run query commands and OS commands. For more details, please refer to the Identity Management design document.

Cross-site Scripting (XSS)

XSS flaws occur whenever an application takes user-supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Counter measure

In order to handle this, validation framework and routines are in place to validate request data and appropriate encoding for the response. Validation prevents the attack, and encoding prevents any script to execute in the browser.

Insecure Direct Object Reference

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Counter measure

The Enact application avoids exposing direct object references. All requests pass through the routing engine, which ensures the authenticity of the user. After this, the Web API controller verifies whether the user is authorized to access the referenced objects before an object is served to the client.

Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

Counter measure

The Enact application is designed to provide effective, secure separation between components. With help of build and deployment tools, the application provides a repeatable hardened process that makes it quick and robust to automate the deployment process. Using automated deployments prevents the risk of security misconfiguration while deploying the application to an existing or new environment.

Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to perpetrate credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as

encryption at-rest or in-transit, as well as special precautions when it is exchanged with the browser.

Counter measure

Enact uses SHA-256 as a standard cryptographic algorithm across the application for sensitive information. Also, passwords are stored as a one-way hashed value, which cannot be decrypted.

Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests to access functionality without proper authorization.

Counter measure

By design, the Enact application strictly follows the approach wherein all URLs and business functions are protected by an effective access control mechanism. At Web API level, the authorization mechanism is applied that allows only authorized users to access the APIs. At framework level, the application enforces mechanism(s) that deny all access by default, requiring explicit grants to specific roles for access to every function.

Cross-site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests which the vulnerable application thinks are legitimate requests from the victim.

Counter measure

Synchronizer Token Pattern is used to facilitate the CSRF prevention. It requires the generation of random "challenge" tokens that are associated with the user's current session. These challenge tokens are inserted within the HTML forms and links associated with server-side operations. When the user wishes to invoke these operations, the HTTP request contains this challenge token. It is then the responsibility of the server application to verify the existence and correctness of this token.

Using Components with Known Vulnerabilities

Components such as libraries, frameworks, and other software modules almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Counter measure

All the components are wrapped before use in the Enact application; these wrappers ensure that only the functionality that is required for the application is exposed via the wrappers, and all other functionalities are filtered by these wrappers. Also, the required functionalities are then well tested and taken care of with consideration to all such vulnerabilities.

Invalidated Redirects & Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Counter measure

As a guideline, absolute redirects and forwards are avoided in general throughout the application. Checks, including a code review process, are in place to enforce relative redirects within the application.

Multi-tier architecture

Enact follows a three-tier architecture, separating the externally-facing web server from the internal application server and database server. With a tier-based architecture such as this, even if an attacker compromises an externally-facing web server from the outside, they still must find ways to gain access and attack the internal network. This is the principle of defense-in-depth protection, a more practical approach to information security.

Authentication/Authorization

The Enact system needs authentication/authorization at the Web application level and authorization at the Web API level. To meet these requirements, a common solution is better than implementing different approaches for Web application and Web API. The system will use OpenID Connect to achieve the same. OpenID connect is an interoperable authentication protocol based on the OAuth 2.0 family. OpenID connect will authenticate the Web application and OAuth will authorize the Web API.

Code Analysis

A static code analysis tool was used to help developers identify security issues, and many other categories of potential problems—as per Microsoft's best practices for writing code. Static here means the source code is analyzed without executing it. This code analysis is integrated with the build to keep a real-time check on the issues.

Data Security

In the Enact application, only the Web APIs are exposed to the public and all Enact components like the web server, application server, and the data server are part of a virtual network (VNet). The VNet is configured with the Azure Network Security Group (NSG). NSG contains access control

rules that allow or deny traffic based on traffic direction, protocol, source address and port, and destination address and port.

Database Security

Data protection involves protecting Enact databases from unwanted actions from unauthorized users.

Only authorized users can access Enact data, based on their user role. The Enact database server is not exposed to the Internet. It can only be accessed via Enact application components within the Azure Virtual Network (VNet).

Data Transport Security

To ensure message integrity, all public facing data is encrypted flowing through Transport Layer Security (TLS). Emails sent from the Enact SMTP server are encrypted using TLS, provided that the recipient's mail server is configured to support TLS. Minimum TLS version supported is 1.2.
The protocols used within TLS are:

- HTTPS and Web Socket Security (WSS) – for all web application transactions, including gauges
- HTTPS port 443 – for Automated Data Collection

OAuth 2 and OpenID Connect: the predominate Industry Standard protocols used for Authentication and Authorization within Enact. By creating tokens that exist only during application handshake, OAuth prevents password propagation.

Data Encryption: Enact uses the SHA-256 cryptographic algorithm across the application for sensitive information. All passwords are stored as a salted one-way hashed value—which cannot be decrypted.

Client Information Security

InfinityQS maintains client data, including contact and billing information. InfinityQS is committed to properly securing the information we maintain for our clients.

Protection of Client Information

InfinityQS employs numerous methods for securing online data and client contact/billing information. Protection of client information is maintained through a variety of technology and processes, including the following:

- We employ internal access controls to ensure that the only people who see your information are those with a need to do so to perform their official duties.
- We train all personnel on our privacy and security measures and policies.
- InfinityQS personnel do not have access to your account passwords. InfinityQS will not ask you for credit card or other personal information via email. InfinityQS personnel may ask you for partial personal or credit card information in order to verify your identify if you call our Technical Support team (for example, our personnel can only see, and therefore only ask you for, four digits of your credit card information to verify your identity).
- We physically secure the areas where we hold electronic or hard copies of information we collect through a combination of 24x7 security guards, biometric scanners, secure safes, and badge/card key access.
- All online storage systems fully encrypt the data regardless of media type (e.g., disk or tape).
- We use technical controls to secure the information we collect online using techniques such as Secure Socket Layer (SSL), electronic digital certificates, encryption, firewalls, and password protections.
- We periodically test our security procedures to ensure both personnel and technical compliance.

Sharing Client Information

InfinityQS does not share any client information with other companies or entities. From time to time, InfinityQS may be required to provide personal information in response to a valid court order, subpoena, government investigation, or as otherwise required by law. We also reserve the right to report to law enforcement agencies any activities which, in good faith, we believe to be unlawful. We may release certain personal information when we believe that such release is reasonably necessary to protect the rights, property, and safety of others and ourselves.

High Availability, Disaster Recovery & Backup

Enact has been architected for durability, high availability, and maintaining a 99.5% uptime per the Enact Service Level Agreement (SLA), even in the event of hardware failure. Enact runs in geographies around the world on Microsoft's Azure cloud platform and utilizes the following design features:

- Each region is paired with another region within the same geography
- Data is always replicated within the same region, and all copies are committed before the write is acknowledged
- Each region also contains a replica of Enact infrastructure from a different region running in a primary active mode and secondary disaster recovery passive mode
- For data durability, data is automatically replicated at least three times within the primary region, and three times in the paired regions

Please see the following Microsoft Azure links for additional information:

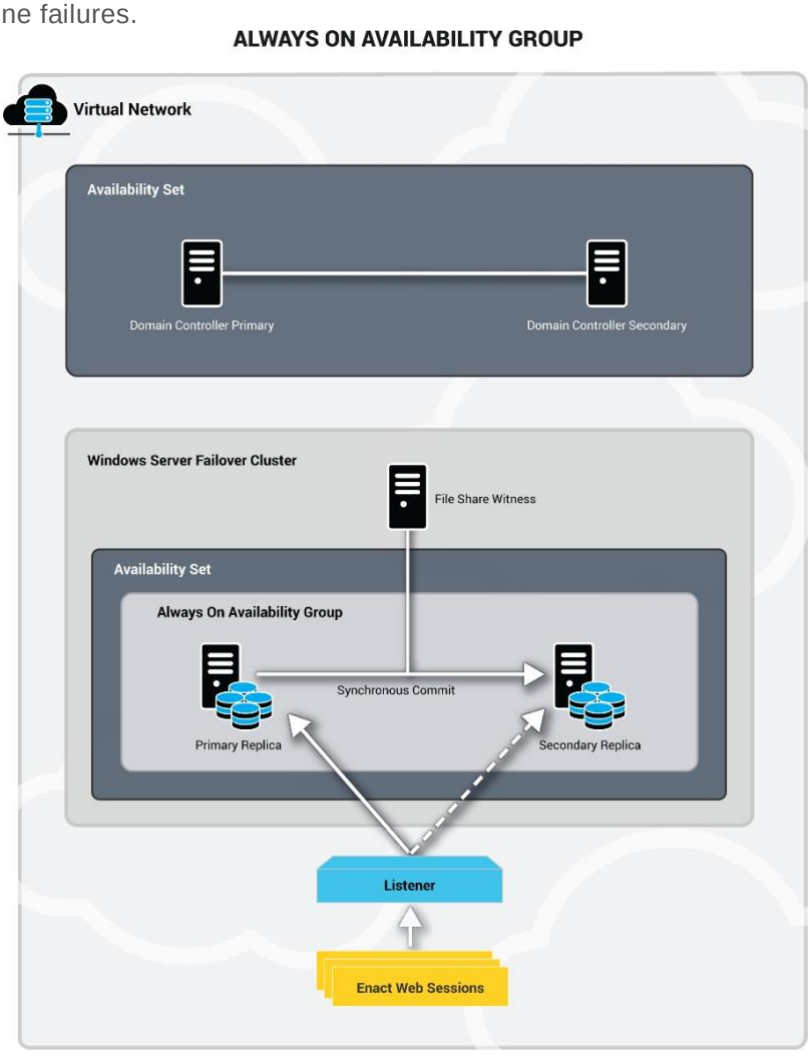
- https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions
- https://docs.microsoft.com/en-us/azure/storage/storage-redundancy#locally-redundant-storage

Geography	Paired Regions	
North America	North Central US	South Central US
	East US	West US
	East US 2	Central US
Europe	North Europe	East Europe
Asia	South East Asia	East Asia
China	East China	North China
Japan	East Japan	West Japan
Brazil	South Brazil(1)	South Central US
Australia	East Australia East	Southeast Australia
US Government	US Gov Iowa	US Gov Virginia
India	Central India	South India

Enact Regional Pairs

High Availability Processes

To mitigate the probability of a possible system failure, the strategy used focuses on system availability, scalability, and fault tolerance. Through redundancy and resilient redesign, the following features have been deployed: Availability Set, Load Balancer, and Always On Availability Groups (AOAGs). This enables the Enact cloud platform to absorb planned maintenance events and unplanned maintenance events such as network failures, disk failures, and Virtual Machine failures.



Always On Availability Groups on the Database Tier Available Set perform server failure detection and protect the operating system and the application-specific failures, such as (but not limited to):

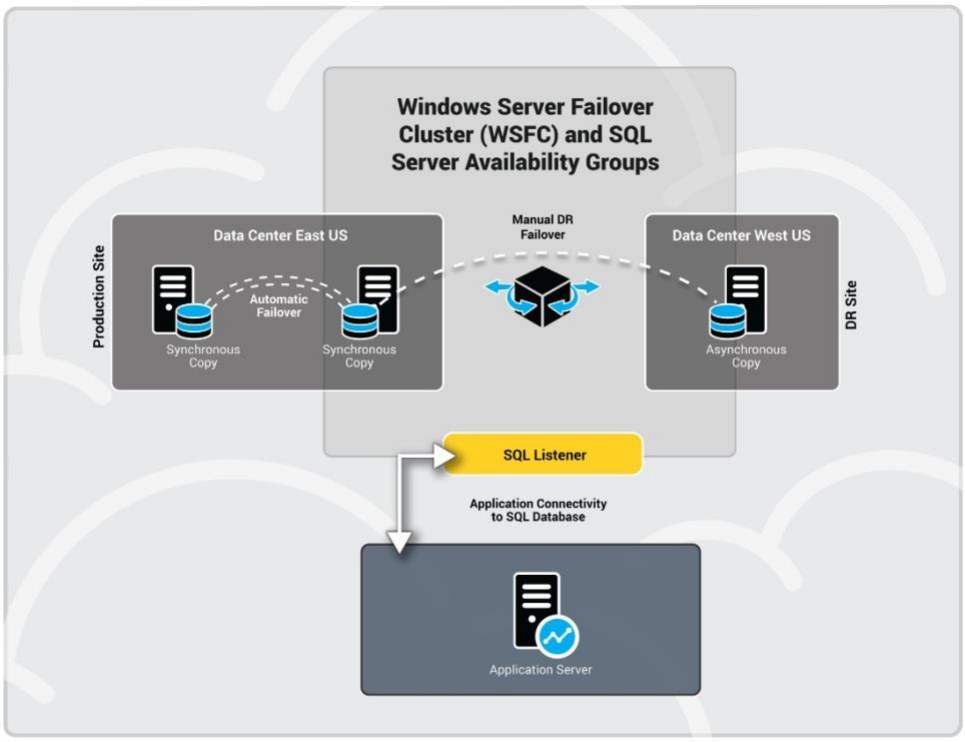
- Database server service could be down or hung
- Database failover takes approximately 10 seconds
- Automated data collection writes to a cache and data is not committed until the destination is available
- Patching database server causes downtime (e.g., due to system updates)

Disaster Recovery Processes

InfinityQS has many policies and procedures in place to support Business Continuity. Part of that plan consists of keeping documentation, software code, and other pertinent information stored and backed up by utilizing software tools across the organization such as Team Foundation Services (TFS) and SharePoint. Critical roles, procedures, and tasks are duplicated across the InfinityQS staff. IT and other technical personnel can work remotely, and many have mobile workstations that enable them to work off-site and keep the business operational.

Passive Data Center Configuration

The Web Tier Available Set and Application Tier Available Set will be deployed when disaster recovery is required. The Database Tier Available Set will always stay active for asynchronous mode replication from the Active Replica. The disaster recovery process of different application services will be both manual and automatic, depending on platform service (Infrastructure as a Service or Platform as a Service—IaaS or PaaS).



Disaster Recovery & Replication

Data Backup Processes

All tenant databases have scheduled backups: weekly full backups, daily differential backups, and hourly transaction log backups.

Enact supports the active/passive database-only approach to disaster recovery. Only the primary datacenter has Enact fully deployed, but both datacenters are synchronized across the tenant databases. If a disaster such as a power outage occurs at the primary datacenter, Azure Traffic Manager detects it and routes users to the alternate datacenter. Manual activation will begin the deployment of the application in the secondary datacenter. Operations resume when the environment becomes available.

Backup & Restore with Azure

In order to provide the highest level of confidence in critical quality data, production databases are backed up directly to a different datacenter for disaster recovery using the following strategy:

- Full backup—weekly, retention period: 16 days
- Differential backup—daily, retention period: 16 days
- Transactional backup—hourly, retention period: 16 days

This enables clients to recover their environment to a specific time with a maximum potential data loss of 30 minutes over a duration of four weeks.

***Note**: System recovery is not limited to subgroup data. System recovery includes, but is not limited to the following: collected data, master data (parts, process, features, specification limits, etc.), data collections, operation diagrams, gauge configurations, parts recipes, etc.*

Enact Application Management Procedures

Monitoring Systems

InfinityQS utilizes several network, server, and application monitoring systems to ensure system reliability and security. All these systems are tied to a centralized monitoring and alert system.

Specific rules have been configured in order to track, detect, and escalate security-based events as quickly as possible; system/software log auditing alerts are also part of this procedure. InfinityQS Operations personnel can proactively monitor all network, server, and application activities. They can also immediately respond to a wide range of incidents, including outages, warnings, and potential security threats, on a 24x7 basis. Events logs from all systems are retained for at least seven days.

Incident Response Procedures

Equally important to the technical security measures are detailed job procedures that instruct operations and support personnel on the tasks they must perform in order to ensure the security of our service and our customer's data. These procedures include periodic (daily, weekly, monthly) security maintenance procedures, as well as the detailed incident response procedures that are followed in the event of a security incident. Detailed incident management procedures have been established to cover all types of security incidents, including the following:

- Information system failures and loss of service
- Denial of service attacks
- Malicious software attacks
- Breaches of confidentiality

In addition to normal contingency plans (designed to recover systems or services as quickly as possible), these procedures also cover the following:

- Analysis and identification of the cause of the incident
- Planning and implementation of remedies to prevent recurrence, if necessary
- Collection of audit trails and similar evidence
- Communication with those affected by, or involved with, recovery from the incident
- Reporting the action to the appropriate authority

Application Update Procedures

InfinityQS Enact provides a common platform for all users. As mentioned earlier, multiple client companies use the same deployment to access Enact; however, it's important to note that each customer has their own discrete database. All system users will always be using the same version of Enact.

All system updates will be scheduled, and users appropriately informed, of the improvements prior to deployment. Following are the four types of updates:

- Critical updates
- Enhancements
- New functionality to existing modules
- New functional modules

Critical Updates

Critical updates are implemented, as needed, to ensure full system functionality and performance for all users. This update type may fix an existing "bug," fix a performance issue, or fix a display issue (e.g., new browser, browser update, etc.). These fixes are time-sensitive and will not normally afford an opportunity for client evaluation.

All critical updates will undergo a thorough testing process and will have an established procedure for rolling back to a previous version if an unforeseen issue arises.

Enhancements

Enhancements provide refinements and improvements to existing functionality. These changes are not as time-sensitive as critical updates. Examples of enhancements could include visual changes to the user interface (UI), display issues, and availability of new statistics in existing reports.

Clients will be able to review a list of enhancements contained in an update prior to the scheduled implementation date.

New Functionality

Adding new features and functionality to existing modules will occur over time. As new functionality is added to the system, users will be provided information on the new capabilities prior to deployment of the new functionality. New functionality will have little or no impact on existing functionality. For example, a new data collection or new “themes” may be available, but users have no obligation to use these new features. The ability to preview (beta) the functionality may be available on a limited basis.

New Functional Modules

New functional modules will add entirely new capabilities to the system and will extend the system beyond its core functionality. Functional modules will typically be offered for an additional fee.

Examples of possible functional modules might include the following:

- Advanced quality analytics
- Industry specific modules
- Compliance reporting

The ability to preview (beta) functional modules prior to release may be available on a limited basis.

EU Safe Harbor Principles

The Microsoft Trust Center documentation covers the EU Safe Harbor Principles:

https://www.microsoft.com/en-us/TrustCenter/Privacy/default.aspx

InfinityQS IT Organization Security

InfinityQS IT Personnel Background Verification Procedure

Personnel security begins even before employees are hired. All job descriptions include the security responsibilities that the employee will be expected to understand and meet. Potential employees undergo background investigations that may include identity, criminal, and credit checks, former employer reference checks, and education verification. Employees vying for more sensitive positions, such as datacenter operations, undergo more rigorous checks. To further ensure we have the best people in the business, we require our engineers to be trained and certified, and we have programs to help them maintain and improve their certifications levels. Our procedures help ensure that only those professionals with the best abilities, trustworthiness, and integrity are employed. Given that security is such an important facet of our business, we stress security awareness and promote a security-conscious culture at all levels within the organization.

InfinityQS IT Personnel Security Policy

InfinityQS has established a strict personnel security policy, which is reviewed and accepted by all employees as a requirement for employment. These security precautions and controls serve as both a guideline and a policy covering the access, protection, and dissemination of information for both InfinityQS internal and client data.

Azure Security

Microsoft Azure, our cloud services provider, delivers a physically safe, network-secure, and reliably available environment:

- SSAE 16 Certified
- 24/7 monitoring of physical security, including motion sensor and security breach alarms
- Redundant high-speed Internet links that connect Enact directly into the core of the global Internet backbone
- HVAC temperature control systems with separate cooling zones and state-of-the-art smoke detection
- UPS and fully redundant power with natural gas backup

Security Auditing

See Appendix A: Azure Compliance Certifications.

Monitoring & Logging

Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Antivirus & Antimalware

All software components must go through a virus scan prior to deployment. In addition, native antimalware on all VMs is provided.

Penetration Testing

Our cloud services provider conducts regular penetration testing to improve security controls and processes. They understand that security assessment is also an important part of our customers' deployment. Therefore, they have established a policy for InfinityQS to carry out authorized penetration testing.

DDoS Protection

Our cloud services provider has a defense system against Distributed Denial-of-Service (DDoS) attacks on platform services. It uses standard detection and mitigation techniques. The DDoS defense system is designed to withstand attacks generated from outside and inside the platform.