Security & Architecture Whitepaper

Invenias X

Contents

1 Introduction

Invenias X is the next generation of the world's leading executive search platform and is delivered on Microsoft Azure (PaaS).

Microsoft Azure is a fully managed cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers. Microsoft Azure provides software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) and supports many different programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems. Microsoft Azure delivers significant benefits and options around functionality, performance, availability and security.

The Invenias X platform is coded to utilize a pure a PaaS architecture. The new platform delivers new desktop, web and mobile apps centered around a single API and provides a secure solid foundation for fast innovation and business growth.

2 Hosting Partners

2.1 Microsoft Azure

Microsoft is the selected hosting partner for the Invenias global platform. Invenias utilizes the Microsoft cloud and leverages its PaaS capabilities to build a dynamic, secure and scalable platform.

Microsoft is a global leader in providing cloud computing capabilities in over 50 regions. Each region has a set of data centers deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. Microsoft Azure safeguards data in facilities that are protected by industry-leading physical security systems and are compliant with a comprehensive portfolio of standards and regulations.

2.2 Microsoft Data Center Compliance

Global Centric

- CIS Benchmark
- CSA-STAR-Attestation
- CSA-Star-Certification
- CSA-STAR-Self-Assessment
- DFARS
- ISO 20000-1:2011
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 9001
- SOC 1, 2 and 3
- WCAG 2.0

Industry Centric

- 23 NYCRR Part 500
- APRA (Australia)
- CDSA
- CFTC 1.31
- DPP (UK)
- FACT (UK)
- FCA (UK)
- FFIEC
- FINRA 4511

- FISC (Japan)
- GLBA
- GxP
- HIPAA/HITECH
- HITRUST
- MARS-E
- MAS + ABS (Singapore)
- MPAA
- NEN-7510 (Netherlands)
- NHS IG Toolkit (UK)
- OSFI (Canada)
- PCI DSS
- SEC 17a-4
- Shared Assessments
- SOX

2.3 Resilience & Availability

All Microsoft Azure components that Invenias use have resilience and redundancy built in as part of the PaaS infrastructure offering from Microsoft. Invenias have also used design and architecture best practice considerations in the implementation of the Invenias platform to provide further resilience and availability. Customers can opt to globally replicate the data held within their Azure SQL database to further enhance resilience and availability.

3 Platform Architecture

The Invenias Platform architecture leverages Microsoft Azure PaaS. It's a pure PaaS architecture which includes infrastructure resilience, availability and security along with rich feature and component utilization.

3.1 What is PaaS? (definition)

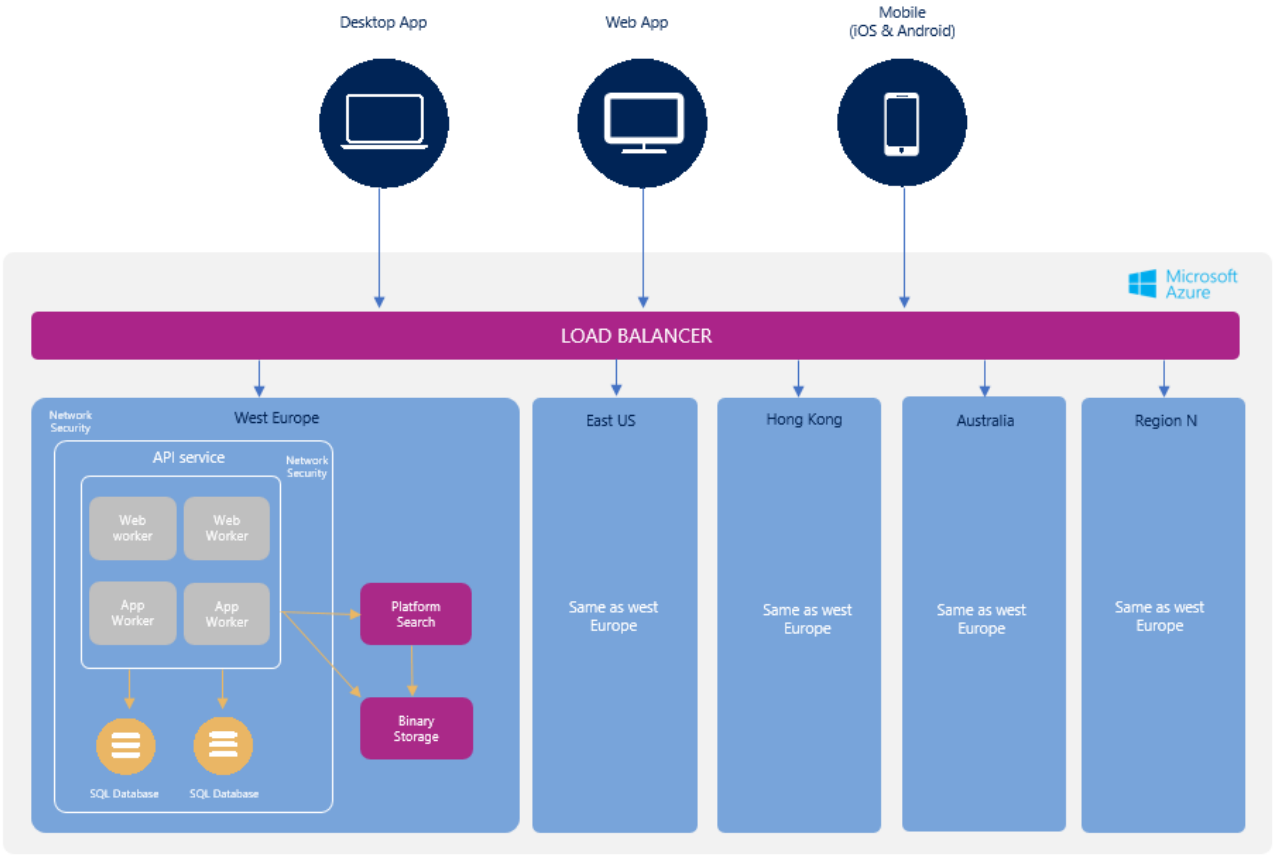
Platform as a service (PaaS) is a complete development and deployment environment in the cloud that enables the building and deployment of cloud-enabled applications and entire platforms.

PaaS enables companies to focus on developing dynamic, secure applications at scale without the need to spend valuable resources on running and managing physical or virtualized infrastructure.

Microsoft Azure PaaS is an ever-growing set of component services with built in resilience and availability designed to support the complete web application and platform life cycle - now and in the future.

3.2 PaaS Implementation Overview

The Invenias platform uses multiple components and services of Microsoft Azure PaaS platform. Each region where Invenias runs its platform has a complete set of services ensuring performance and availability.



3.3 Patch Management

All patch management and infrastructure security patches are handled by Microsoft as part of the Microsoft Azure PaaS service. All systems are always up to date in-line with vendor best practice guidelines.

3.4 Load Balancers

Invenias utilize the Azure DNS-based traffic load balancer. This enables Invenias to distribute traffic to services across regions as well as providing high availability and responsiveness. DNS is used to direct customer requests to the most appropriate service endpoint in the Invenias platform. Dynamic routing based on end point availability allows for resilience at a load balancer level. All distributed traffic by the load balancer is done securely using encrypted transport.

3.5 Firewalls

Invenias implement network security rules to prevent unauthorized traffic reaching isolated virtual networks within the Invenias platform.

3.6 Network

Invenias utilize virtual network components to segment and isolate different parts of the platform. These technologies also allow Invenias to isolate the Invenias platform from generic Microsoft Azure components and services.

3.7 Active Directory

Invenias depend on Azure Active Directory to secure access to platform resources and infrastructure. Azure Active Directory is a premium identity and access management cloud solution that combines core directory services, application access management capabilities and advanced identity governance e.g. 2FA and threat protection services.

3.8 Web & Services Layer

All web applications and API services run in virtualized application environments, provided by Microsoft PaaS components, with 99.95% availability. These containers enable Invenias to maintain multiple releases of the Invenias software allowing for a controlled and secure release of new features and functionality.

3.9 Database Layer

Invenias utilize Azure SQL database services to store all systems and customer relational data. These services support multiple redundant database replicas provisioned in the primary and sibling datacenter within a single region. Microsoft provides this resilience to failures with 99.99% availability for the Azure SQL database PaaS components. Databases can also be geo-replicated to other regions within the Invenias platform providing further scaling and availability for customers who need to operate in multiple different territories.

3.10 Single-Tenant Isolation

Whilst the Invenias X platform is a multi-tenant platform, within it exists single-tenant isolation from a customer data perspective. Each customer has their own database and storage area within the platform. This means individual customers data is secured independently of all other customer data stores – this approach ensures optimum security and separation of customer data.

3.11 Encryption Keys & Application Certificates

Invenias utilize secure key management to protect data on the Invenias platform. This allows keys and certificates only to be known and used by the Invenias platform. Invenias has designed its production system so that no individual at Invenias or at Microsoft has access to this information to change it or to utilize it for direct access.

3.12 Transport Security

All data inbound and outbound on the platform is encrypted using the latest widely supported TLS protocols along with strong 256-bit ciphers. Data transport within the platform is always also encrypted (SSL/TLS) for all connections.

3.13 Backups

Database backups consist of a combination of full database backups weekly, differential database backups taken every 12 hours, and transaction log backups every 5 - 10 minutes. Binary data is protected by a soft delete mechanism that enables data recovery.

Database backups and binary data are encrypted and stored in replicated storage within another regional datacenter (within the same legal domicile). This means data is durable even in the case of a complete outage or a disaster in which the primary location is not recoverable.

This data is stored for 35 days and represents a point in time restore or RPO of 10 minutes within the previous 35 days. This 35-day data retention is provided by Microsoft's Azure PaaS components that Invenias uses for data storage.

3.14 Monitoring

Invenias has detailed logging and monitoring for its applications, its platform services and the underlying Microsoft Azure PaaS resources.

Invenias proactively ensures that events are tracked, categorized and addressed where needed to ensure Invenias' commitment to its customers.

Escalation of incidents are managed by the Invenias Engineering team. Invenias utilize Microsoft Premier Support to be as reactive as possible to the operational needs of the Invenias platform.

Invenias maintain an Incident Reporting Escalation and Management Process to provide efficient and detailed triage of priorities, threats and remediations.

Invenias also utilizes LogicMonitor (SaaS provider) to ensure monitoring, alerting and escalation of service availability for each region.

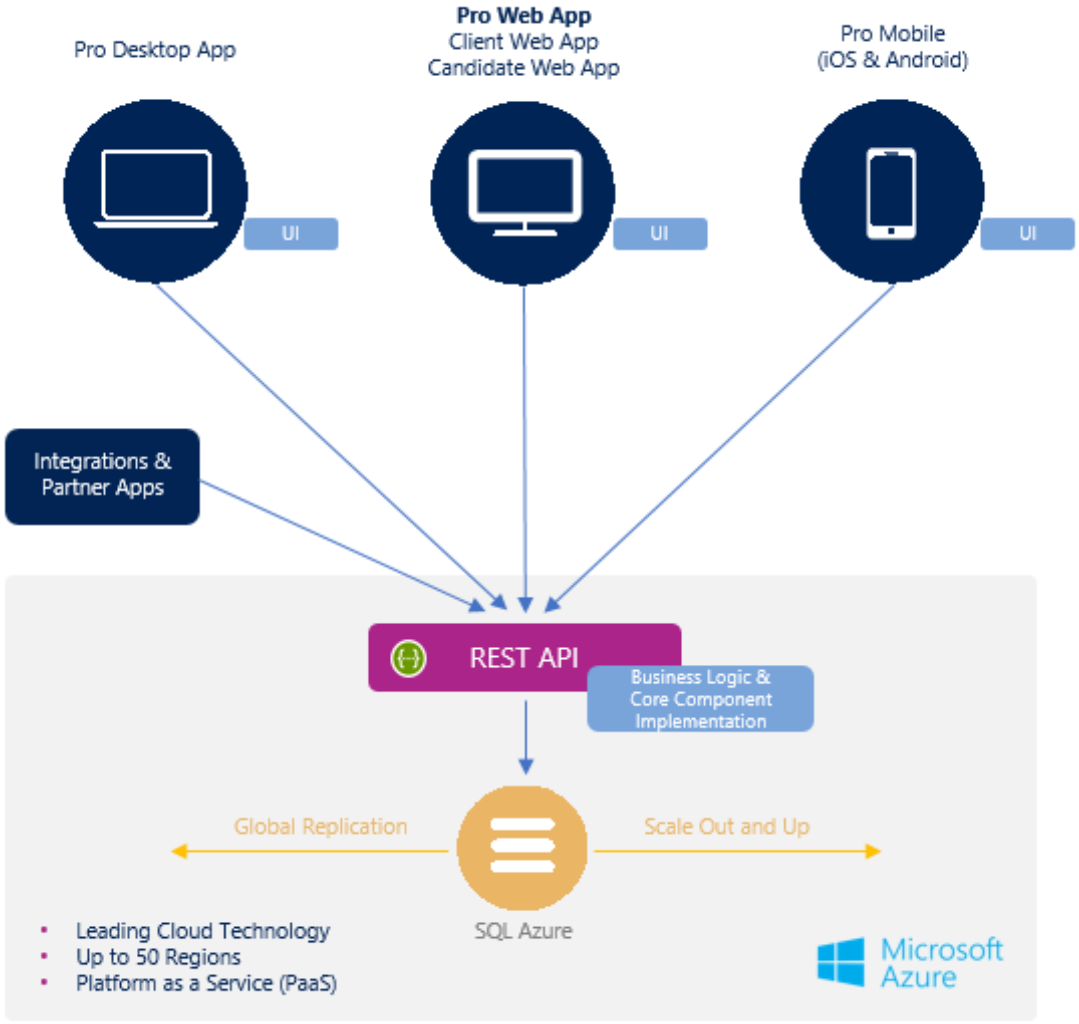
3.15 Data Domicile & Data Replication

Depending on the legal requirements data can be in any of the data center regions utilized by the Invenias platform. Customer data can then be replicated to up to 4 data centers within the Invenias global platform.

4 Application Architecture

The Invenias platform supports simple and easy to use apps that can be accessed seamlessly from inside Outlook, native apps for your iPad, iPhone and Android devices, and web browser-based applications.

4.1 Application Structure



The platform delivers its functionality through a core REST API. This ensures all applications use the same logic for business functionality and security.

5 Invenias Engineering

5.1 Secure Development Lifecycle

The Invenias engineering team adhere to a secure development lifecycle (SDLC) for all aspects of Invenias X. This is driven with the use of tools and technologies, process as well as consultation with third party security professionals.

Invenias use Microsoft Software Services (SaaS) that provide an integrated set of services and tools to manage software projects, from planning and development through testing and secure deployment. These things include source control, build pipelines, and work tracking, workflow management, sign off and deployments. This enable Invenias to ensure that code reviews for both generic and specialist parts of the application receive the correct level of due diligence without fail. It ensures that no one individual can introduce code into the development pipeline.

Invenias engineering understand industry standards around security like OWASP and Invenias engineering proactively incorporate security measures from exercises like threat modelling. Invenias engineering periodically work with consultants from Microsoft on security principles from generic software engineering to specific topics for Microsoft Azure.

Invenias also implement Dynamic Application Security Testing (DAST) through Qualys scanning and testing tools, the output from this is fed into the SDLC.

5.2 Testing & QA

Invenias have a dedicated QA function within the engineering team. Invenias utilize manual and automated testing as part of the overall development pipeline and sign off process.

Development and testing environments are separate from any production environment. **Invenias never use any production data in any non-production environment.**

5.3 Independent Security Assessment, Vulnerability Checks & Pen Testing

Microsoft conduct strategy and execution of penetration testing against Microsoft managed cloud infrastructure, services and applications that provide Microsoft Azure PaaS. Microsoft conducts continuous security monitoring and practice security incident responses to validate and improve the security of Microsoft Azure.

Microsoft goes above and beyond compliance accreditations to provide the additional assurance that Microsoft cloud services are continuously monitoring, testing, and performing security updates to reflect constantly changing.

Invenias initiate annual pen testing on Invenias applications carried out by independent 3rd party pen test organizations to ensure that the applications built by Invenias are conforming to industry security standards.

Invenias also utilize weekly vulnerability scanning from Qualys on all its applications and endpoints.

All testing and scanning feeds back into the SDLC.

5.4 Configuration Management

The Invenias X platform is defined in code and therefore all configuration management for the platform is controlled through the SDLC.

6 Platform Security

6.1 Administration Access

All Invenias staff who have read-only access to the Microsoft Azure PaaS platform resources are security checked and vetted by an independent security validation service. **This does not include access to customer data.**

The Invenias X platform is isolated and pure a PaaS implementation, therefore **no individual employee has administration access to the platform.**

6.2 Authentication & access

All Invenias X read-only platform access is controlled through role-based access controls. All read-only platform access accounts require 2FA.

6.3 Access to customer data

There is no Invenias or Microsoft access to customer data. All access to customer data is managed by the customer through the Invenias software.

6.4 Accountability & Audit

Invenias have logging at all levels the Invenias applications and across all resources utilized on the Microsoft Azure PaaS components. This includes access logs, error logs and performance logs. As a minimum all logs are retained for 90 days. Additionally, some logs are retained for 1 year e.g. Azure Active Directory logs.

7 Business Continuity

7.1 Customer Data Loss Protection

The Invenias data model contains duplicate data storage to store records that have been removed. This means that any customer data deleted by a user through an Invenias application is automatically removed from the main data set and stored in this removed data set.

Any deleted records are therefore automatically retained within a customers' database with a record of the user who completed the delete action.

Invenias log every write operation made to the core API on an individual customer basis. This data is logged into the customers binary storage area and provides an audit log of data changes.

7.2 Platform Data Loss Protection

Microsoft Azure PaaS provides availability and redundancy in datacenter facilities and further replication/distribution to regional and global data centers. The Invenias platform leverages all these features to prevent data loss.

7.3 Disaster Recovery Plan

If the live platform goes offline due to a critical data center incident, then a process of recovery will be used to either restore the existing infrastructure or deploy new Microsoft Azure PaaS and migrate data where necessary.

The data used for the resumption of client services is provided by the redundancy and backup process of the existing Microsoft Azure PaaS infrastructure.

8 Invenias Architecture, Security & Policy Values

The following summarizes common information on how Invenias approach Architecture, Security and Policies with consideration to customer data and business operations.

Principle Facts and Policies	Invenias Response
Secure Development	Invenias services are engineered with strict industry standard practices (security by design, threat modelling, OWASP). Information Security is fundamental part of our Software Development Lifecycle (SDLC).
Hosting Provider	Invenias has partnered with industry leaders that have governance and industry certification in place. Specifically, with Microsoft Azure PaaS, there is a wealth of global and local governance/compliance (https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings).
Data in Transit	Invenias protects all data in transit with the latest widely supported TLS protocols along with strong 256-bit ciphers.
Data at Rest	All customer data is encrypted at rest no matter where it resides within the Invenias platform.
Customer Platform Isolation	Invenias services are single-tenanted. This ensures no unintended disclosure is permitted or possible between Invenias customers. Confidentiality, privacy and ownership is always maintained. Access must always be explicitly granted by the customer.
Secure Platform Administration	Invenias services are governed by management policies and processes which includes the utilization of industry standard practices governing change management. Through technical control measures no individual can make any changes to the platform. All changes are delivered through the SDLC and tracked accordingly. The governance practiced by Invenias ensures the security, integrity, confidentiality and performance of the platform.
Secure User Management	Invenias services allow for detailed role/permission-based security, enabling access control and other security centric principles.
Identity & Authentication	Customer devices and web browsers are secured and authenticated by the industry standard OAuth 2.0. Invenias provide single sign-on (SSO) integration with leading industry providers thus allowing customers to have further controls for authentication and identity management.
Information Security	Invenias maintains an information security policy, to effectively manage its information security threats in order to support its business and information security objectives and maintain its legal, regulatory, internal and contractual compliance obligations.
Backups & Retention	All data is backed up with data retention of up to 35 days.

Supplier Security	Invenias suppliers are subject to a due diligence processes to ensure all third-party access and/ or services meet contractual requirements, comply with legal and regulatory requirements, minimize integrity/reputational risks to the business, protect all restricted and confidential information.
Certification and Best Practices	Invenias' information security policy defines responsibilities for protecting information assets based on industry best practices (ISO 27001), including asset management, personnel security, physical, environmental, equipment, and media security, communications and operations management, access controls, incident management, business continuity management, and compliance.
Legal Compliance and Privacy	Invenias act on the lawful requests of our customers as a processor. Our privacy policy complies with GDPR.
Asset Protection	Invenias maintains an up-to-date inventory of Company assets and an information classification that specifies appropriate security and handling controls based upon defined classifications.
Operational Security	Invenias has implemented industry standard security controls to protect customer data from loss or unauthorized disclosure.
Personnel Security	Invenias ensures it hires skilled professionals with relevant experience and conducts employee background screening commensurate with the level of access provided, including criminal, financial, and/or employment background screening.