Forsta Plus hosted on the Microsoft Azure Platform Cloud Security

This document describes the Forsta Plus on Azure Cloud Native environments, and the security mechanisms we have in place to protect your data.

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. Forsta makes no representations and gives no warranties of whatever nature in respect to this document.

Contents

Copyright © 2023 Forsta

Copyright © 2023 Forsta

Data Compliance

Data Ownership

Unless agreed otherwise, all data stored and processed is owned and controlled by PG Forsta's clients, who are designated as data controllers. Forsta cannot classify or represent the data, all data is treated as confidential and processed equally. Clients are responsible for classifying the data and deciding when to delete the data, according to their data retention and deletion policy.

Technical and Organizational Measures

Forsta maintains appropriate technical and organisational measures (TOMs) to ensure that personal data is processed and stored securely. The TOMs can be viewed at https://legal.forsta.com/legal/forsta-technical-and-organizational-measures/. An extract is shown below, please refer to the website for the most up-to-date version. Such measures provide assurance that the offering aligns to both the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). In addition, we offer to agree to GDPR compliant Data Processing Agreements (DPA) and/or EU Standard Contractual Clauses. Our standard template is available for download and signature here: https://legal.forsta.com/legal/forsta-data-processing-agreement/.

Table 1 Forsta Technical and Organisational Measures

Measures of pseudodonymization and encryption of personal data	Forsta will encrypt all client data at rest and while in transit over public networks.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Forsta will regularly apply security patches to computing devices and monitor for exploitable vulnerabilities. Forsta will engage partners to perform external and internal penetration testing to look for potential risks to confidentiality, availability and integrity of SaaS products and Client Data.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Forsta will design and implement disaster recovery plans for its software and Client Data. Restorability of backups will be tested regularly. Systems storing Client Data will be protected against environmental impacts (water, fire, electrical). Physical security and resilience systems will be regularly maintained by qualified personnel. Disaster recovery plans will be tested periodically.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Forsta will implement security monitoring technologies and internal and external audits to confirm ongoing compliance with its security policies.
Measures for user identification and authorization	All Forsta users will authenticate using unique credentials and strong passwords. Multi-factor authentication will be

Copyright © 2023 Forsta

	used for remote access to private services. Forsta will maintain proper controls for requesting, approving, granting, modifying, revoking and revalidating user access to systems and applications containing personal data. All access requests will be approved based on individual role-based access, least-privilege principles, and reviewed on a regular basis for continued business need. All systems must meet Forsta's security standards and employ security configurations and security hygiene practices to protect against unauthorized access to operating system resources. Forsta will follow a documented process for timely revocation of access for terminated staff.
Measures for the protection of data during transmission	Forsta will encrypt all data in transit over public networks. Forsta will employ encrypted and authenticated remote connectivity to its computing environments. Remote access to private Forsta systems and applications will be done through use of an encrypted private network (VPN).
Measures for the protection of data during storage	Forsta prohibits the transfer of Client Data onto personal removable media. User workstations and SaaS infrastructure will be protected through encryption, malware prevention, and security monitoring.
Measures for ensuring physical security of locations at which personal data are processed	Forsta will implement physical security measures at its offices and data centers. Controls will be based on likelihood and impact of unauthorized access to each site. Access controls will ensure only authorized personnel have physical access to systems and applications containing personal data. Visitor procedures will ensure all visitors are logged and escorted. Where data centers are owned/managed by subcontractors, Forsta will regularly confirm subcontractor compliance with substantially similar physical security controls and by requiring data center subcontractors to perform third-party audits (such as a SOC 2 type II). Forsta will enforce a clean-desk policy for all staff with access to Client Data in shared spaces.
Measures for ensuring events logging	Forsta will ensure that all system logs are collected and monitored by automated systems in near real-time. Suspicious events will be investigated.
Measures for ensuring system configuration, including default configuration	Forsta will use hardened configurations to deploy all computing devices, including network, storage, and computing resources.

Copyright © 2023 Forsta

Measures for internal IT and IT security governance and management	Forsta will create and maintain security and privacy policies. Policies will be reviewed periodically and updated to reflect Forsta's commitment to securing Client Data. All Forsta staff will be trained on security practices and policies when hired and annually thereafter.
Measures for certification/assurance of processes and products	Forsta will engage qualified third party auditors to review its information security program and to issue opinions or certifications validating the quality of the information security and privacy program.
Measures for ensuring data minimization	Forsta Clients are responsible for determining how much data is collected and stored it Forsta SaaS products.
Measures for ensuring data quality	Forsta offers software tools to enable clients to update and/or delete inaccurate personal data.
Measures for ensuring limited data retention	Forsta Clients are responsible for data deletion within their SaaS subscription.
Measures for ensuring accountability	Forsta will grant Clients the right to perform audits and will ensure that all subcontractors allow Forsta to perform audits. Audit rights ensure ongoing accountability for securing and protecting personal data.
Measures for allowing data portability and ensuring erasure	Client can at any time perform data export from the platform and store in a secure location of their choosing. Forsta will logically delete client data at termination of SaaS agreements. Forsta will sanitize all media at end-of-life.
Measures for securing custom software and software development	Forsta will design and build its software with protection of personal data as a guiding principle. Forsta will use industry standard tools to scan for quality code. Forsta will test all web applications for common vulnerabilities prior to production release.
Measures for reducing attack surface	Forsta will implement firewalls, intrusion detection, system hardening, and mobile device management technologies to reduce likelihood of a security incident.
Measures for managing assets that process or store personal data.	Forsta will implement an asset lifecycle program to maintain an inventory and ownership for all assets that process or store personal data.
Measures for managing sub-processors	Forsta will ensure all subprocessors agree to implement and maintain substantially similar technical and organizational measures. Forsta will assess subprocessors'

Copyright © 2023 Forsta

	technical and organizational measures prior to engagement and regularly thereafter.
Measures for detecting and responding to security incidents	Forsta will ensure that all system logs are collected and monitored by automated systems in near real-time. Suspicious events will be investigated. Forsta will notify Data Controller of any incident impacting personal data without undue delay.

An up to date Forsta sub-processor list can be found at: [Forsta Sub-Processor List | Forsta]

Copyright © 2023 Forsta

What is the Shared Security Model

The Shared Security Responsibility Model (SSRM) is used to segregated security responsibilities between clients and Forsta. A shared responsibility model is a cloud security and risk framework that delineates which cybersecurity processes and responsibilities lie with the Software as a Service (SaaS) provider, Forsta, and which lie with the client. A shared responsibility model promotes tighter security and establishes accountability as it relates to the security of the service.

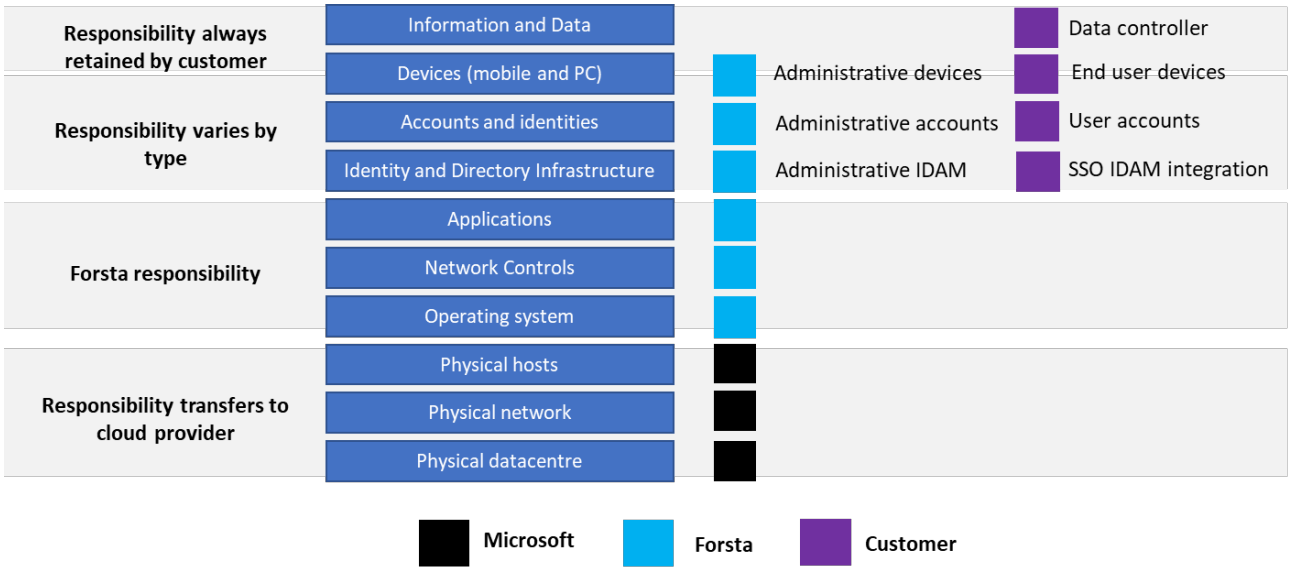

Figure 1 Forsta Plus Shared Security Responsibility Model (SSRM)

Forsta Security Responsibilities

Forsta is responsible for the following:

- Operating System – ensuring that the operating systems, i.e., container host, container images, running containers and software defined network appliances, are correctly configured and kept updated and patched.
- Network controls – Controls are in place to protect the underlying network infrastructure from unauthorised access, misuse, or theft. This is discussed in more detail later in the document.
- Application security encompasses the software and processes implemented to reduce vulnerabilities.
- Identity and Access management – This is limited to the management of identity and access rights granted to administrative users in cloud operations and technical support.

Client Security Responsibilities

Security control responsibility on the client side is defined by the Forsta Plus cloud SaaS service they select. In all cases the client is responsible for:

- Client data. Protection of data as it enters and exits the SaaS service. Inclusive of: classification of data, identification of processing purpose, definition of data retention periods and enforcing data deletion, gaining and maintaining consent, and knowing all of the data you collect. Client is responsible for complying with applicable data privacy law related to Client Data, i.e., for determining which laws or regulations are applicable to Client's use of data, that its instructions to Forsta comply with such laws or regulations, and for

Copyright © 2023 Forsta

determining if Forsta's technical and organizational measures meet the requirements of such laws or regulations.

- End user devices. Management of end user devices used to access the SaaS service. The client is responsible for ensuring the security of all devices that are used by their employees to access and conduct administrative tasks. This includes IT security controls, patch management, and configuration management.
- Account administration. Unless agreed otherwise with the Forsta User Administration team, the client is responsible for the administration of user accounts, and user actions when using the accounts. Clients must provide their users with security and awareness training, especially any users with privileged access.

Cloud Provider Responsibilities

Further detail is provided in each section. Our cloud provider, Microsoft is responsible for all physical security aspects of the cloud computing services that underpins Forsta Plus. Forsta conducts third party risk management activities to ensure that they meet the required standard. Microsoft maintain a number of security certifications. These include ISO27001 and SOC 2. More information can be found at: Compliance offerings for Microsoft 365, Azure, and other Microsoft services. | Microsoft Learn

Copyright © 2023 Forsta

Security Model

The security model applied to Forsta Plus is layered, providing defence in depth through diverse defensive strategies. Layering security defensive controls reduces the chances of a successful attack.

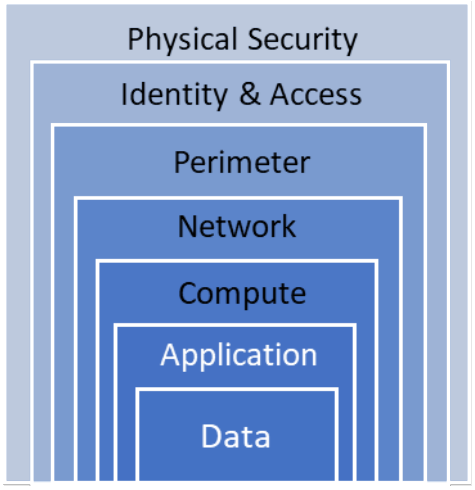

Figure 2 Layered Security Model

Physical Security

Datacentre infrastructure

Azure infrastructure is designed to preserve data residency, and offer comprehensive compliance and resiliency options for clients. A region is a set of datacenters that is interconnected via a resilient network. The network includes content distribution, load balancing, redundancy, and data-link layer encryption by default for all Azure traffic within a region or travelling between regions. Azure regions are organized into geographies. An Azure geography ensures that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries. Availability zones are physically separate locations within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

Physical Security

Managed by Microsoft, they have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:

Access request and approval.

- Access must be requested and approved prior to arriving at the datacenter, with a suitable business justification.
- A need-to-access basis helps keep the number of individuals needed to complete a task in the datacenters to the bare minimum.
- After Microsoft grants permission, an individual only has access to the discrete area of the datacenter required, based on the approved business justification.
- Permissions are limited to a certain period of time, and then expire.

Facility's perimeter is protected by:

- Well-defined access point.
- Typically, tall fences made of steel and concrete encompass every inch of the perimeter.
- There are cameras around the datacenters, with a security team monitoring their videos at all times.

Copyright © 2023 Forsta

- The datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks.
- These security officers also routinely patrol the datacenter, and monitor the videos of cameras inside the datacenter at all times.

Facility's interior is protected by:

- Two-factor authentication with biometrics to continue moving through the datacenter.
- Only access the portion of the datacenter that you have approved access to.
- Only for the duration of the time approved.

Datacenter floor is protected by:

- You are only allowed onto the floor that you're approved to enter.
- You are required to pass a full body metal detection screening on entry to the datacentre.
- Only approved devices can make their way into the datacenter floor.
- Video cameras monitor the front and back of every server rack.
- Pass through full body metal detection screening on exit.

Further detail can be found at:
Datacenter security overview - Microsoft Service Assurance | Microsoft Learn
How deo Microsoft protect its datacenters from unauthorized access?
How does Microsoft protect its datacenters from environmnetal hazards
How does microsoft verify the effectiveness of datacenter security

Responsibility	Forsta	Microsoft Azure
Data center / facility management		
Data center physical security		**X**
Data center access control		**X**
Data center infrastructure		**X**
Data center operations		**X**
Data center support		**X**

Copyright © 2023 Forsta

Identity & Access

Identity & Access management is a shared responsibility. Forsta is directly responsible for managing the identity and access rights of administrative users across cloud operations and technical support. These include:

Access control

- Access limited to suitably trained personnel in cloud operations and technical engineering support (TES)
- Azure Active Directory is used to manage identities
- Access to production environments is limited inline with access policies
- Segregation of roles to ensure least privilege access to data
- Complex password, rate-limiting and MFA required for administrative users

	Production AD user	Production AD administrator
Minimum Length	17 characters	20 characters
Maximum age	365 days	
Minimum age	24 hours	
Account lockout	5 failed attempts within 30 minutes locks the account for 30 minutes	
Password history		
Complexity requirements	The password must not contain three or more characters from the user's account name or full name, and contain at least three of the following: • English uppercase characters (A-Z) • English lowercase characters (a-z) • Numeric digit (0-9) • Special character	
MFA enforced	Yes	

N.B. The password policy is in line with current National Institute of Standards and Technology (NIST), UK's National Cyber Security Centre (NCSC) and the Australian Cyber Security Centre (ACSC) to:

- Implement technical controls, rate-limiting and account lockout
- Reduce password fatigue by increasing the password change interval
- Enforce Multi-Factor Authentication

Application login controls

- All user accounts are named, personal accounts not shared, 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 setting shorter password expiration dates if required.
- 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 Forsta Plus Technical Support.
- Passwords are one-way hashed 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 /

Copyright © 2023 Forsta

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 Forsta employees.
- Forsta Plus automatically locks application access for design, studio and report users after a period of inactivity, 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

 Copyright © 2023 Forsta

Perimeter

Azure Application Gateway is a web traffic load balancer that enables web application traffic management, HTTPS traffic is restricted to TLSv1.2 and above. The application is only accessible via port 80 (used for redirect to port 443), port 443 for all user traffic and port 22 for secure file transfers via SFTP. In Azure, multiple instances of the application gateway have been provisioned. Azure distributes these instances across update and fault domains to ensure that instances don't all fail at the same time

Web Application Firewall

The Web Application Firewall is based on the Core Rule Set (CRS) from the Open Web Application Security Project (OWASP) and can provide protection from:

- SQL injection protection.
- Cross-site scripting protection.
- Protection against other common web attacks, such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion.
- Protection against HTTP protocol violations.
- Protection against HTTP protocol anomalies, such as missing host user-agent and accept headers.
- Protection against crawlers and scanners.
- Detection of common application misconfigurations (for example, Apache and IIS). Configurable request size limits with lower and upper bounds.
- Protect the application from bots with the bot mitigation ruleset.
- Inspect JSON and XML in the request body.

Data Transmission Security

Forsta Plus uses certificates for web-facing applications that can provide a safe and secure method of accessing the Cloud site for both Project Managers and respondents should the secure link be used. Certificates are automatically updated and rolled over every 60 days.

Virtual Private Network

Forsta administer the application and infrastructure using a secure site to site VPN connection to send encrypted traffic between the application production environment and the global operations centres. Monitoring traffic transits the encrypted connection.

Copyright © 2023 Forsta

Network

Network Security Groups. A Network Security Group (NSG) contains security rules that allow or deny inbound network traffic to, or outbound network traffic from several types of Azure resources. Each rule can specify source and destination port and protocol. NSGs are used within Forsta Plus to isolate and segment different parts of the network, limiting access to only those services on the allow list. The high-level diagram below demonstrates the internal segregation into network security groups:

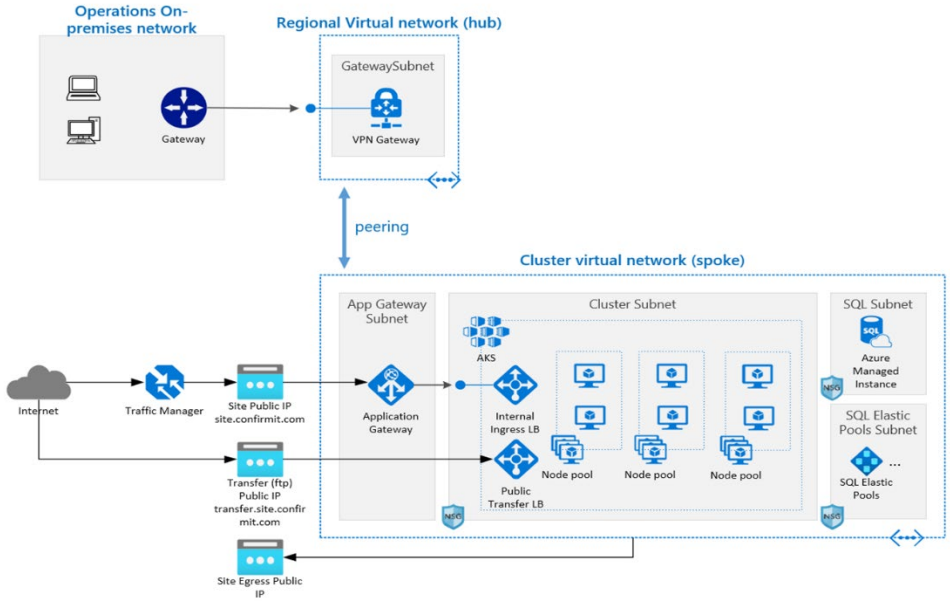

Figure 1 Forsta Plus Network Diagram

Infrastructure deployment. A declarative coding tool enables developers to use a high-level language to describe the software defined infrastructure as code (IaC). This enables the rapid deployment of updates and patches, moves change management to the left of the pipeline and avoids configuration drift, which results in an improved security posture. Access to the data layer where client data is stored is restricted to a limited set of personnel, following compliance rules where applicable, geo-restriction being the most common.

Cloud Security Posture Management. Constant monitoring for cloud vulnerabilities, aligned to common industry standard cybersecurity frameworks.

High Availability

The Forsta Plus application is architected from the ground up to be easily scalable to support rapidly changing capacity and performance requirements of a high-availability platform. All key functional areas are built in high-availability clustered arrangements or in load-balanced pools and in addition spread across availability zones where applicable, allowing for growth through scaling.

Azure Kubernetes infrastructure enables full redundancy of application features, auto scaling during high demand periods and seamless updates. The AzureSQL Platform as a Service (PaaS) where client data is stored is designed with high-availability in mind. High availability is further maintained by running the application in Azure Regions with Availability Zones (at least 3 physical locations) where possible. We are also utilizing Azure Paired region for Disaster Recovery, additional physical location in-country.

Copyright © 2023 Forsta

Denial of Service (Doy.S)

By default, all services in Azure are running a service called DDoS protection basic which is focused on protecting Azure's infrastructure and assures the availability of the Azure region. Azure DDoS protects against attacks on layers 3 and 4. The Standard feature provides protection against the common DDoS Attack types such as TCP SYN Flood, UDP Flood attacks.

The application is protected against attacks at layer 7 by the Web Application Firewall contained within the Application Gateway. There are different ways to stop L7 attacks such as:

a. URI restrictions
b. IP Address blocking
c. Geo-blocking
d. WAF features, blocking known attacks against the OWASP Top 10
e. Rate limiting

- These features are actively managed by the cloud operations team. Please contact your sales or account manager to discuss in more detail.

Enhanced Azure DDoS protection is available, detail will be provided on request.

Responsibility	Forsta	Microsoft Azure
Networking		
Network access (Internet)		X
Firewall ownership	X	
Firewall initial setup	X	
Firewall monitoring	X	
Firewall maintenance	X	
Firewall rule set design	X	
Firewall rule set implementation	X	
DDOS mitigation		X
Load balancer hardware ownership		X
Load balancer initial setup	X	
Load balancer monitoring	X	
Load balancer maintenance		X
Load balancer rule set design	X	
Load balancer rule set implementation	X	
IDS hardware ownership		X
IDS monitoring	X	X
IDS maintenance	X	X
VPN tunnel configuration	X	
Switch hardware ownership		X
Switch setup		X
Switch monitoring		X
Switch maintenance		X
Servers		
Server hardware ownership		X

Copyright © 2023 Forsta

Hardware administration	**X**
Hardware maintenance	**X**

 Copyright © 2023 Forsta

Compute

Azure Kubernetes Service

Azure Kubernetes Service is managed using a shared security responsibility model with Microsoft. Microsoft retain responsibility for the base infrastructure , Microsoft manages and monitors the following components through the control pane:

- Kubelet or Kubernetes API servers
- Etcd or a compatible key-value store, providing Quality of Service (QoS), scalability, and runtime
- DNS services (for example, kube-dns or CoreDNS)
- Kubernetes proxy or networking (except when BYOCNI is used)
- Any additional add-ons or system component running in the kube-system namespace

Microsoft Support can't sign in to, execute commands in, or view logs for these nodes without Forsta's express permission or assistance.

Build Security

Vulnerability assessment and management tools for container images stored in ACR registries and running in Azure Kubernetes Service (AKS).

Linux Nodes

Linux nodes are upgraded to the latest available version when the node is rebuilt. This happens automatically on test sites and manually on a recurring basis on production sites.

Windows Server Nodes

Windows Update are scheduled around the regular Windows Update release cycle and validation process. This upgrade process creates nodes that run the latest Windows Server image and patches, then removes the older nodes.

Environment hardening

Microsoft Defender run-time threat protection is in place **for** file storage.

Responsibility	Forsta	Microsoft Azure
Virtualization		
Virtual infrastructure management		X
Virtualization / DRS management	X	
Virtual machine management	X	
Operating system / Database services		
OS/SQL Server software ownership	X	
OS/SQL Server initial install	X	
SQL Server / cluster configuration	X	
SQL Server monitoring	X	
SQL Server administration	X	
OS administration	X	

Copyright © 2023 Forsta

OS maintenance and patching	**X**
OS monitoring	**X**
HTTP monitoring	**X**

Copyright © 2023 Forsta

Application

Continuous Integration and Continuous Delivery (CI/CD)

The Forsta Plus platform is developed using the agile methodology applied to a Continuous Integration / Continuous Delivery (CI/CD) pipeline. This brings several benefits, faster delivery of new features and bug fixes and improved software quality. In addition, CI/CD enables us to bring security into Development Operations (DevOps) securing the pipeline and ensuring that we meet compliance standards. We introduce testing early in the pipeline to better detect and prevent security issues as early as possible in development, commonly referred to as *'shift-left'*. Some of the tools and techniques we use in the pipeline are:

Environments Management

Environment management helps Forsta to improve the overall quality of software development and support throughout the lifecycle. It also helps to maintain and enforce security by limiting development activities and personnel to lower environments. Several environments are maintained to ensure that development, test and production are kept separate. Strict controls are in place to define and enforce promotion criteria between environments and who is granted access.

Software Composition Analysis (SCA)

Software composition analysis (SCA) is an automated process that identifies the open-source software in a codebase. Analysis is performed to evaluate security, license compliance, and code quality. Our SCA tool inspect package managers, source code, binary files, container images and more, to identify critical security and legal vulnerabilities and quickly fix them.

Static Application Security Testing (SAST)

SAST scanners are used to scan the applications source to identify weakness that lead to vulnerabilities. SAST is an important stage in the Software development Lifecycle (SDLC) as it identified vulnerabilities before the application is deployed and enables developers to code, amend and test again. This helps to reduce vulnerabilities in the deployed application.

Dynamic Application Security Testing

Dynamic application security analyses the web application from the front end to find vulnerabilities through simulated attacks. Since DAST tools are equipped to function in a dynamic environment, they can detect runtime flaws which SAST tools can't identify. This helps to both verify the testing carried out in earlier stages of the software development lifecycle and potentially find vulnerabilities that may have been missed.

Responsibility	Forsta	Microsoft Azure
Application servers		
Forsta Plus application installation	**X**	
Forsta Plus application management	**X**	
Forsta Plus application monitoring	**X**	
Forsta Plus application support	**X**	

Copyright © 2023 Forsta

 Copyright © 2023 Forsta

Data

Separation

Each client has dedicated company-wide databases where collected data is stored. These databases are split into two types, one for storing the collected responses and one for storing data exported from response databases into SmartHUB for reporting purposes, both types dedicated to the company that owns the data. System-level databases contain comingled data for tenants in a multi-tenant site.

Encryption

The SQL databases are encrypted using Transparent Data Encryption

Microsoft Defender for Azure SQL - the benefits and features | Microsoft Learn
Microsoft Defender for Storage - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

Copyright © 2023 Forsta

Systems Maintenance

Recovery Time Objective and Recovery Point Objective

RPO 4 hours, RTO 36 hours

Performance Monitoring

Forsta monitors the availability and performance of Forsta Plus 24/7 by means of

- Application service and access logs using Kibana and Grafana dashboards fed by Elasticsearch and Logstash clusters.
- Platform metrics using Prometheus and Grafana.
- Microsoft Azure monitors the underlying infrastructure 24/7.
- Site24x7 (https://www.site24x7.com/) performs external monitoring of availability and response times on SaaS sites for live applications
- Polling is performed from a global monitoring network.

All monitoring systems set up to alert on error, P1 errors alert 24/7 On-Duty personnel, activating our Incident Management process.

Backup and Recovery Policy

Unless any other agreement has been made, AzureSQL databases are configured with 7-day Point In Time Restore (PITR). In addition to this, backups are performed every 12 hours and kept for 12 weeks using Azure Recovery Services Long Term Storage. The backups include client data on the Forsta Plus platform, including imported data, client projects (e.g. surveys) and configured tasks and reports.

For more details about Azure backups, please refer to https://docs.microsoft.com/en-us/azure/backup/backup-overview.

Offsite Backup

All Azure backups are geo-replicated to another secure Azure location for disaster recovery and long-term retention purposes. The Azure backups are stored securely by Azure, in an off-line state, preventing corruption of the data in the event of a production system virus, ransomware, data corruption, etc. Where possible, we use the Azure Paired Region to ensure quick data transfer to the secondary site, see https://learn.microsoft.com/en-us/azure/reliability/cross-region-replication-azure for more on this.

Backup Retention

The off-site, Long Term Retention period of Azure backup is 12 weeks. After 12 weeks, Azure disposes of the backup data and it is no longer restorable by Forsta.

Data Restore

Forsta Cloud Operations employees oversee the backup and restoration process. For client project restorations, data will be restored either to the original project (overwriting the project) or to a new copy/duplicate of the original database (allowing for the client to later merge records). For countries where personal data privacy legalization applies, only Forsta personnel from within a certain country may be able to restore the data.

Copyright © 2023 Forsta

Responsibility	Forsta	Microsoft Azure
Backup		
Backup server and storage		**X**
Backup setup	**X**	
Backup monitoring		**X**
Backup storage (offline)		
Backup restoration (requestor)	**(X)**	**X**

Support

Unless specifically stated in the contract or any restrictions have been agreed upon in T&C's, Forsta's Technical Support team handles all support for Forsta Plus Platforms. Requests directly relating to the operation of the site are escalated to the Forsta Cloud Operations team.

Copyright © 2023 Forsta