42Gears Mobility Systems

UEM Privacy and Data Protection Overview

March 2020

Privacy and data protection overview

42Gears offers a wide range of scalable SAAS based products and solutions that can help enterprises manage and secure endpoints, applications, and PCs across Windows, Apple iOS, MacOS, Linux and Android platforms. Currently, 42Gears offers enterprises a seamless, secure and scalable Unified Endpoint Management (UEM) solution. In addition to this, 42Gears is also helping enterprises to manage BYOD programs in a secure and efficient environment. While these solutions enhance workforce productivity and efficiency, such services are also vulnerable to security threats that can put device and data at risk. 42Gears proactively adopts security solutions that help reduce and overcome such possibilities.

While exploring cloud based SaaS solutions, enterprises always vet security and privacy aspects of the products. They typically need answers to questions like:

- Who has access to the enterprise data?
- Where is the data stored?
- Is the data secured in data center or while on the move?
- Who owns the data?

Security and privacy of customer's data is of utmost importance for 42Gears. We are committed to provide answers to any such queries to be in compliance with the data privacy regulations.

This white paper offers an overview of how 42Gears helps secure customers' data and protect their privacy. While in the ever changing world, technical aspects are subject to change, but our commitment to provide you a secured and protected environment will never change.

Data Center Security

42Gears uses Amazon Web Services (AWS) for hosting web services. AWS data center security begins at the perimeter layer. This layer covers many security features such as security guards, fencing, security feeds, and intrusion detection technology. Amazon's data centers operate around the world, with highest security protocols. Entry to these datacenters is highly regulated and controlled. Even regular AWS employees with access to these premises, undergo regular audit to make sure their access is still relevant and necessary. Let's see what security measures are in place in the data centers.

In order to prevent unauthorized entry in data center, there are video surveillance, intrusion detection, and access log monitoring systems in place. There are devices that sound alarms if entrance door is forced or held open.

Source:

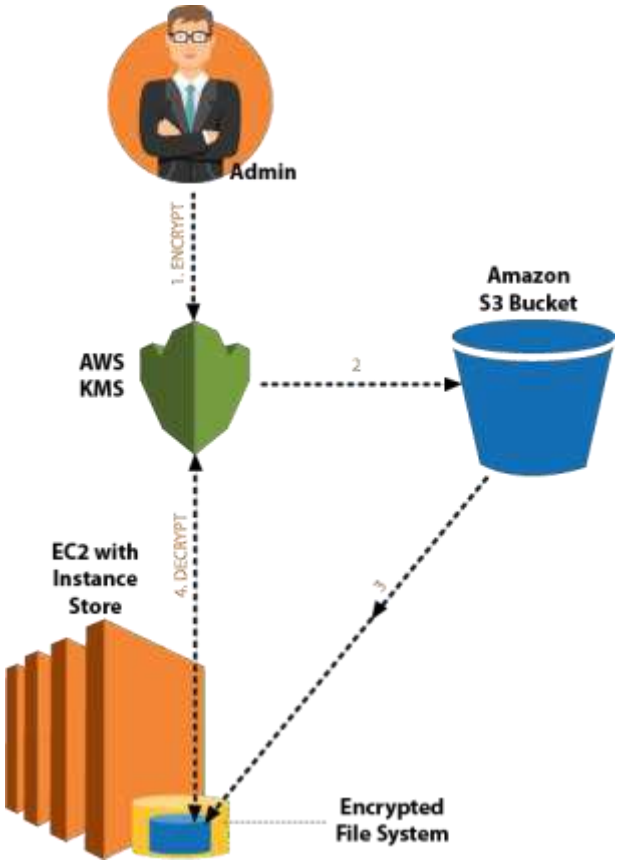
https://aws.amazon.com/compliance/data- center/data-centers/

AWS security operations centers are located around the world and are responsible for monitoring, triaging, and executing security programs for the AWS data centers. They provide 24/7 support to the on-site data center security teams, while also they oversee physical access management and intrusion detection response.[1]

AWS security Infrastructure

42Gears uses AWS Elastic Cloud Compute infrastructure for hosting web application services and database services. Other services like Simple Storage Service, CloudFront and Glacier are used for storage and content delivery.

The high level architecture of the cloud deployment is shown in the diagram below:



Physical and Logical access control

Security highly depends on people who we are hiring to perform the tasks. Amazon also follows standard personnel security measures and appreciates those practices that are made to secure customer data.

All Amazon employees and staff with access to customer data go through standard background checks as permitted by law which includes a review of candidates' education, employment, and criminal history. Apart from this, if any personnel have to access to customer data or manage key physical or logical access controls, they must have to undergo with additional background checks. In order to protect the privacy of its employees and staffs, Amazon doesn't share the results of background checks with customers.

Amazon follows principles of segregation of duties and least privilege. The physical access to data centers is generally limited to AWS staff, while selective AWS personnel have logical access to the web services and data hosted in the data centers.

Employees who are handling customer data, are accountable for data security. These accountabilities are enforces through a system control processes like use of unique usernames, role-based access, and multi-factor authentication. Both the physical and logical access is periodically reviewed to ensure that only appropriate data center access is granted.[2]

Apart from the data center security from AWS, 42Gears also follows standard and strict procedures to ensure customer data security. We have a dedicated system administration team that takes care of the system security. Our servers are administered over a secured network linking the data center to AWS VPC. SSH/RDP is supported by authenticated and encrypted remote log-in access by select and authorized 42Gears staff only. Strict firewall policies and audit logs ensures a very tight access control.

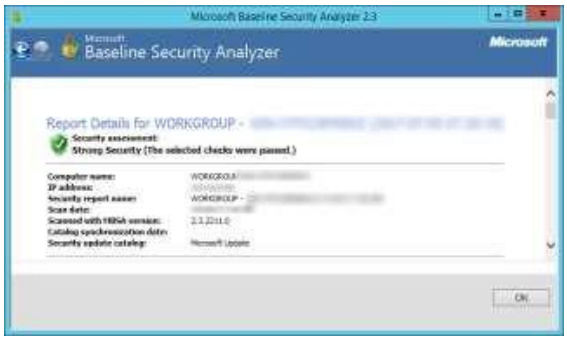
Architectural components security

Security of architectural components such as server security, client installation, enrolled device, app management, admin/self-service portals, identity and authentication are all very important.

Server security

42Gears system administration team routinely performs security assessments of all live systems. We make use of 3rd party auditing tools from time to time to ensure that the systems security is not compromised.

Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations. It determines the security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings.



Secure client installation on mobile devices

Common App Marketplaces such as Google Play Store, Apple App Store and Windows Store have their own security models and processes which ensure secure client installation on mobile devices. 42Gears follows the rules each store has set up for publishing 42Gears' Unified Endpoint Management (UEM) agent application.

Secure client communication

42Gears uses Secure Sockets Layer (SSL) to secure communication between endpoints and the UEM server. The end points include mobile devices based on platforms such as Android, iOS and Windows. 42Gears UEM communicates with iOS devices using the Apple Push Notification Service (APNs). 42Gears UEM uses a certificate to communicate to the Apple MDM services, which the admin must download from the Apple Push Certificates Portal. For Android devices, Google Cloud Messaging is used and

for Windows devices Windows Push Notification Services (WNS) is used.

For more details about mobile device management and enrollment, click here.

To know the 42Gears UEM enrollment process, click here.

Mobile Application Management (MAM)

42Gears UEM allows IT pros to manage the mobile apps that a company's employee uses. Often times these apps are proprietary enterprise apps that should be available to only authorized users. Also, data stored in these apps can be sensitive hence needs to be protected. MAM provides admins capabilities to perform various App management functions like secure distribution of these apps to only authorized uses, policies to protect company's data in apps, software license allocation and management associated with these apps.

42Gears UEM is also one of the few UEMs to be approved for Google's Android Enterprise MAM solutions set.

To learn more about 42Gears MAM, click here.

42Gears UEM Portals

42Gears offers two portals to manage 42Gears UEM:

- **Administrator Portal:**

42Gears provides user account management interface to IT admins for managing online service. Using this portal, admins can manage user accounts, user groups, and domain names, passwords that have configured and subscribed for 42Gears UEM service. Enrollment rules and policies can be set using this portal.

- **Self-service Portal**

42Gears offers self-service portal via AI based virtual assistant - DeepThought. Using this Self-service Portal, users can check machine status, download software, and contact their company's IT support. In order to access this portal, users must be granted access by Admin and enroll their end points into 42Gears UEM.

Both the above portals use SSL for secure communication between web browser and 42Gears UEM servers. Users need to authenticate themselves to access these portals and there is a session inactivity timeout which logs off the users and forces them to log in again, in case they don't use the portal for some time.

Identity and Authentication

Device enrollment authentication

Any user who needs to enroll his device into 42Gears UEM needs to authenticate himself. 42Gears UEM can integrate with any OAuth endpoint for this authentication. This allows us to use Identity Services like ADFS, Azure AD, G-suite, Office 365 for device enrollment.

Portal login authentication

Access to 42Gears UEM admin and self-service portal is also protected behind user authentication. By default, 42Gears UEM offers its own indigenous user management. But it can also integrate with any SAML2 based Identity Service to offer seamless Single Sign On. Azure AD, Okta and Onelogin are few such Identity Services.

Both the above authentication frameworks and their integration with Identity Services, provides seamless user experience to businesses. They just need to connect their on-premise/cloud user directories with 43Gears UEM. Admins can then just add/remove/manage users in their corporate directories, which in turn will manage users in 42Gears UEM.

42Gears' Commitment to Data Protection

42Gears has established its Information security and Data privacy principles to protect the privacy and information rights of its Customers. We are strenuously committed to GDPR compliance.

Under GDPR we are primarily a data processor for Customer Data, which may include information from devices or other systems that the Customer manages and monitors using our services or products.

We collect some information to conduct our regular business operations and administration that may include some personal information such as Company name, email address and contact details. We outline this below as:

- Data collected from website users;
- Data collected through the use of our products and services; and
- Other data such as cookies etc.

Our servers automatically collect certain information when you visit our website. This information does not necessarily reveal your identity directly but it may include information about the specific device used, such as the hardware model, operating system version, web-browser software (such as Firefox, Safari, or Internet Explorer) and the Internet Protocol (IP) address/MAC address/device identifier. In some countries, including the European Economic Area, this information may be considered personal information under applicable General Data Protection Regulation. We do not use this information to identify you, and do not process this information actively. The collection is a byproduct of using the website.

Where our customers subscribe to our products and services we collect certain technical information obtained from software, systems hosting the services or products and device accessing these products and services which do not directly identify the end user herein referred to as Usage Data.

The extent of this collection is configurable by our customers, but as an indication, our collection of technical information that constitutes personal data includes (but is not limited to):

- IP Address
- Email address
- Company name
- Mobile number
- Data Usage details
- Password Strength
- Device Notes
- Other usage statistics

Use of Personal Data

The personal data we collect is used for the following purposes:

- To conduct and develop our business with the customers and with others;
- To engage with customers & prospects about events, promotions, the websites updates and our products and services;
- To operate, evaluate, maintain, improve and develop our products and services or our websites (including by monitoring and analyzing trends, access to, and use of the website for advertising and marketing);
- To customize our websites, products or services to users' needs;

For Customers in the European Union (EU), our processing (i.e. use) of your personal information is justified on the following legal basis:

- the processing is in our legitimate interests, subject to Data Subject's interests and rights, and notably our legitimate interest in using applicable data to conduct and develop our business activities; or
- Data Subjects have clearly consented to the processing of their personal data for a specific purpose.

Disclosure of Personal Data

We share customers' personal data with third parties to render services for which they have been engaged by us, to perform on our behalf, subject to appropriate contractual restrictions and security measures, or if we believe it is reasonably necessary to prevent harm or loss, or it believes that the disclosure will further an investigation of suspected or actual illegal activities.

The third parties may include:

- Cloud infrastructure providers such as Amazon Web Services (AWS).
- Cloud application and productivity providers to support our internal office operations such as email and document management.
- Administration and support: to enable customer support and assist in sales management.
- Marketing and Newsletters: To manage our email communication with our customers and prospects for marketing purpose such as newsletters etc.
- We do not share, sell, rent, or trade any of our customers' personal information to third parties, other than what is necessary to deliver the services, we provide to customer or to administer our business.

Security

We aim to safeguard and protect your personal data from unauthorized access, improper use or disclosure, unauthorized modification or unlawful destruction or accidental loss, and have adopted reasonable technical and organizational security measures to ensure that this is the case, in line with established commercial good practice.

It is nevertheless important that our Customers recognize their responsibility in maintaining effective security in the use of our services.

Retention of Personal Data

We retain personal data for as long as required to fulfil the purposes for which it was collected. A summary of our approach to retention is outlined in our Privacy Policy.

https://www.42gears.com/privacy-policy/

In some circumstances, we may retain personal data for a different period of time, for instance where we are required to do so in accordance with legal, tax and accounting requirements, or if required to do so by a legal process, legal authority, or other governmental entity having authority to make the request, for as long as required.

Individual Rights

For Customers in the European Union, rights are outlined under the GDPR in the Privacy Policy. For Customers outside the European Union, may have some or all of the rights available to them in respect of their personal data, as mentioned in the Privacy Policy, depending on the reason for processing the data.

The purpose of this Privacy statement is to outline how we have established measures to protect customers' privacy and data protection rights.

Data Locality

42Gear UEM servers are hosted in AWS data centers in US, EU and India.

Data Disposition

Customers at any point of time can choose to discontinue our services. This can be done in various ways. They can directly delete their account from the UEM admin portal. Or they can send us a request for account deletion. Or implicitly, customer can stop renewing our subscription for more than 30 days.

In case customer want to terminate the services, we follow a procedure to remove the data from our live as well as backup system.

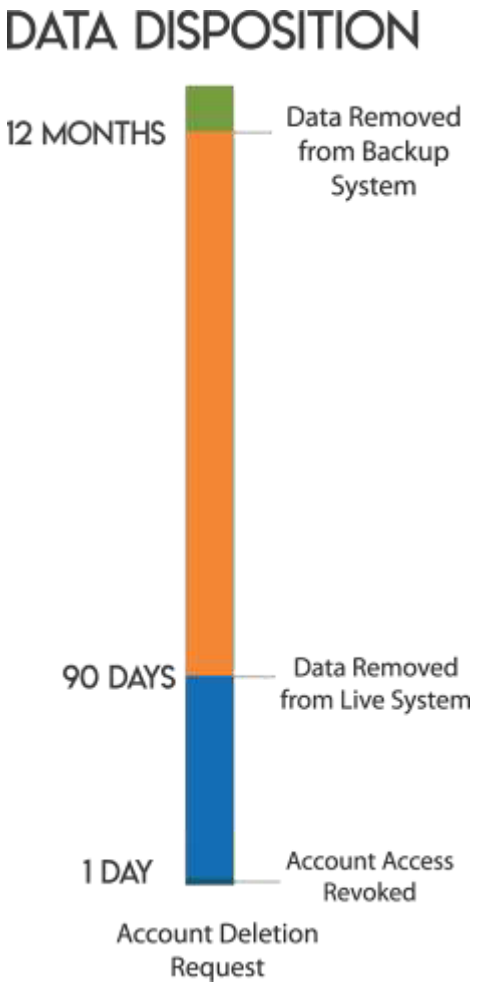
Removal from Live system

Once we receive a request for account deletion, customer's access to the account is

revoked immediately, but customer's data is retained in our live system for upto 90 days. Post 90 days, customer data will be deleted from the live system.

Removal from backup system

After deleting customer data from the live system, it still exists in our Backup system. We delete the data from our backup system in 12 months.



Conclusion

Managing PCs, end points and applications is a very challenging and complex task for businesses. 42Gears helps businesses to overcome these challenges in a cost effective and secure way. Our seamless and robust Unified Endpoint Management (UEM) solution is capable of managing end points for numerous use cases like COSU, BYOD and MAM. Additionally, 42Gears is prompt in adopting innovative technologies such as IoT and AI.

For businesses seeking cloud-based services, it is important to know the security practices and technologies followed in the Data Centers and by Cloud Services providers. 42Gears rely on the most trusted AWS data centers for hosting its servers and also follows comprehensive and robust in-house security processes and guidelines to administer and manage our customers' data.

References

1. https://aws.amazon.com/compliance/data-center/data-centers/
2. https://aws.amazon.com/compliance/data-center/controls/

Disclaimer

This White paper is for information purpose only. The information contained herein is subject to change. No part of this document is legally binding or enforceable. There is no guarantee as to the accuracy of or the conclusions reached in the White Paper, and this white paper is provided "as is". 42Gears does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or non-infringement; (ii) that the contents of this White paper are free from error; and (iii) that such contents will not infringe third-party rights. 42Gears shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this White paper or any of the content contained herein, even if advised of the possibility of such damages.

In no event, 42Gears shall be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this White paper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses.

This document does not constitute or form part of, and should not be construed as, an offer for a sale or subscription for any products or services offered by 42Gears.

42Gears expressly disclaims any liability for any direct or indirect loss or damage of any kind arising directly or indirectly from: (i) any reliance on the information contained in this document; or (ii) any error, omission or inaccuracy in said information.