www.apptimized.com | sales@apptimized.com | +44 (0) 1184 050044

apptimized
APPLICATION PACKAGING

Microsoft Partner

Apptimized Security v6.0.14 (6753f3ca)

The purpose of this document is to detail the measures in place to ensure that the Apptimized cloud-based application packaging solution is secure and compliant with industry best practice.

Security Statement

Apptimized puts the security of our systems and customer data at the core of our business. We review our security practices and procedures regularly and carry out regular testing to ensure stringent access controls, secure hosting and storage, as well as safe data transfer in and out of the service.

Basic Security Considerations

- ✓ Apptimized does not process sensitive user data apart from user account information
- ✓ Applications processed are predominantly freely available commercial off the shelf software (COTS)
- ✓ Customer developed software is processed in compiled format only
- ✓ Sensitive data is separated from the application itself (Client-Server architecture)
- ✓ License information required for packaging is protected from unauthorized access and usage

Data Transfer

- ✓ Data transfer to Apptimized is secured using encrypted HTTPS protocol
- ✓ Using SSL for the end-to-end protocol data protect it from man in the middle attacks or cyber thefts
- ✓ Internal communication (virtual machines) is encrypted and protected by IP address validation
- ✓ Infrastructure is regularly scanned and validated for security compliance

Storage and Hosting

- ✓ Apptimized runs on Microsoft Azure, thus taking advantage of the Azure built-in security measures and GDPR compliance : https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/solutions
- ✓ For specific requirements data is physically stored and processed in a hosting and storage centre in Strasbourg, France, Europe, hosted by specialist cloud services provider OVH GmbH
- ✓ Data Centre is ISO/IEC 27001:2013 certified and adheres to PCI DSS Level 1, SOC 1 Type II, SOC 2 Type II, and CSA Self Assessment,
- ✓ All German Data Protection Laws apply

Updated: April 2018

Apptimized Security v6.0.14 (6753f3ca)

The purpose of this document is to detail the measures in place to ensure that the Apptimized cloud-based application packaging solution is secure and compliant with industry best practice.

Data Access

- ✓ Data stored on dedicated servers only
- ✓ Storage partitions encrypted
- ✓ File names encrypted and stored within one directory with random file names.
- ✓ Backups performed via Bareos
- ✓ Passwords stored in an encrypted format only, preventing unauthorized access
- ✓ Password policies can be implemented to ensure individual password requirements
- ✓ Non-persistent Virtual Machines ensure information deletion when the discovery/ packaging/ testing processes have been completed by the user
- ✓ Random passwords are created and random RDP ports used for every Virtual Machine.
- ✓ Ports blocked on Virtual Machines to prevent service vulnerabilities
- ✓ Daily vulnerability scans and quarterly penetration tests by specialist independent third-party testing company ensures secure architecture and operation

Data Retention & Processing (GDPR)

- ✓ Application data is stored for a minimum of 90 days by default
- ✓ Individual application data retention policies can be agreed, e.g. to:
  - ✓ Purge data automatically after a defined period of post-submission
  - ✓ Keep data for longer
  - ✓ Apply individual rules per data type
- ✓ Users are able to delete all application data earlier by retiring the application
- ✓ Personal data – which is limited to user account data - is protected by the principles of GDPR. Data is:
  - ✓ Processed lawfully, fairly and in a transparent manner
  - ✓ Collected for specified, explicit and legitimate purposes
  - ✓ Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
  - ✓ Accurate and, where necessary, kept up to date
  - ✓ Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
  - ✓ Processed in a manner that ensures appropriate security of the personal data
- ✓ Users can:
  - ✓ Access and correct errors in their personal data via the Profile (Art. 15 & 16)
  - ✓ Erase their personal data by deleting the account (Art. 17, “right to be forgotten”)
  - ✓ Request export, restriction of processing or can object to processing of personal data at any time by contacting 24/7 Apptimized support (Art. 18, 20 & 21)

Updated: April 2018