SaaS / Security

Add-On Products
Resource Central

Add-On Products
Digital Sign Service

Add-On Products
Workspace

Add-On Products
Roms Hule 8 – 7100 Vejle – Denmark
Phone: +45 7944 7000 Fax: +45 7944 7001

Mail: info@add-on.com
Internet: www.add-on.com

Description of SaaS Offering

Facilities

Add-On Products (AOP) servers are all hosted in Microsoft Azure. All datacenters are ISO/IEC, CSA/CCM, ITAR, CJIS, HIPAA and IRS certified.

Physical security, power, and internet connectivity beyond colocation cage doors by is monitored by Microsoft staff 24 / 7.

Data center facilities are powered by redundant power, each with UPS and backup generators.

Azure is currently available in 42 countries, and customers can select any of these locations. However, some may require an additional fee in addition to our standard prices.

All data center facilities feature a secured perimeter with multi-level security zones, 24 / 5 manned security, CCTV video surveillance, multifactor identification with biometric access control, physical locks, and security breach alarms.

Network security

All Production Network systems, networked devices, and circuits are constantly monitored and logically administered by Add-On Products staff 24 / 5.

All data between your users and Add-On Products are encrypted using industry-standard HTTPS and Transport Layer Security (TLS).

We operate a multi-level backup and disaster recovery strategy. Backups and near real-time snapshots are taken at various intervals and multiple copies are securely stored in different locations.

Industry-leading infrastructure is in place to protect against and mitigate the impact of denial-of-service attacks.

Major application data flow ingress and egress points are monitored with Intrusion.
Detection Systems (IDS) or Intrusion Prevention Systems (IPS). The systems are configured to generate alerts when incidents and values exceed predetermined thresholds and uses regularly updated signatures based on new threats.

Our products can be configured to only allow access from specific IP address ranges you define.

Network security scanning gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems.

Access to the AOP Production Network is restricted by an explicit need-to-know basis, utilizes least privilege, its frequently audited and monitored, and is controlled by our team. Data is stored a secured password vault secured with 2fa.

Product security features

All data between your users and Add-On Products are encrypted using industry-standard HTTPS and Transport Layer Security (TLS).

We support (Saml2, OpenID and OAUTH.)

We support Two-factor authentication (2FA)

Single sign-on (SSO)

Secure Credential Storage, all essential data are encrypted.

Our Employees

All new hires are screened through the hiring process and required to sign Non-Disclosure, covering anti-bribery and anti-corruption and Confidentiality agreements.
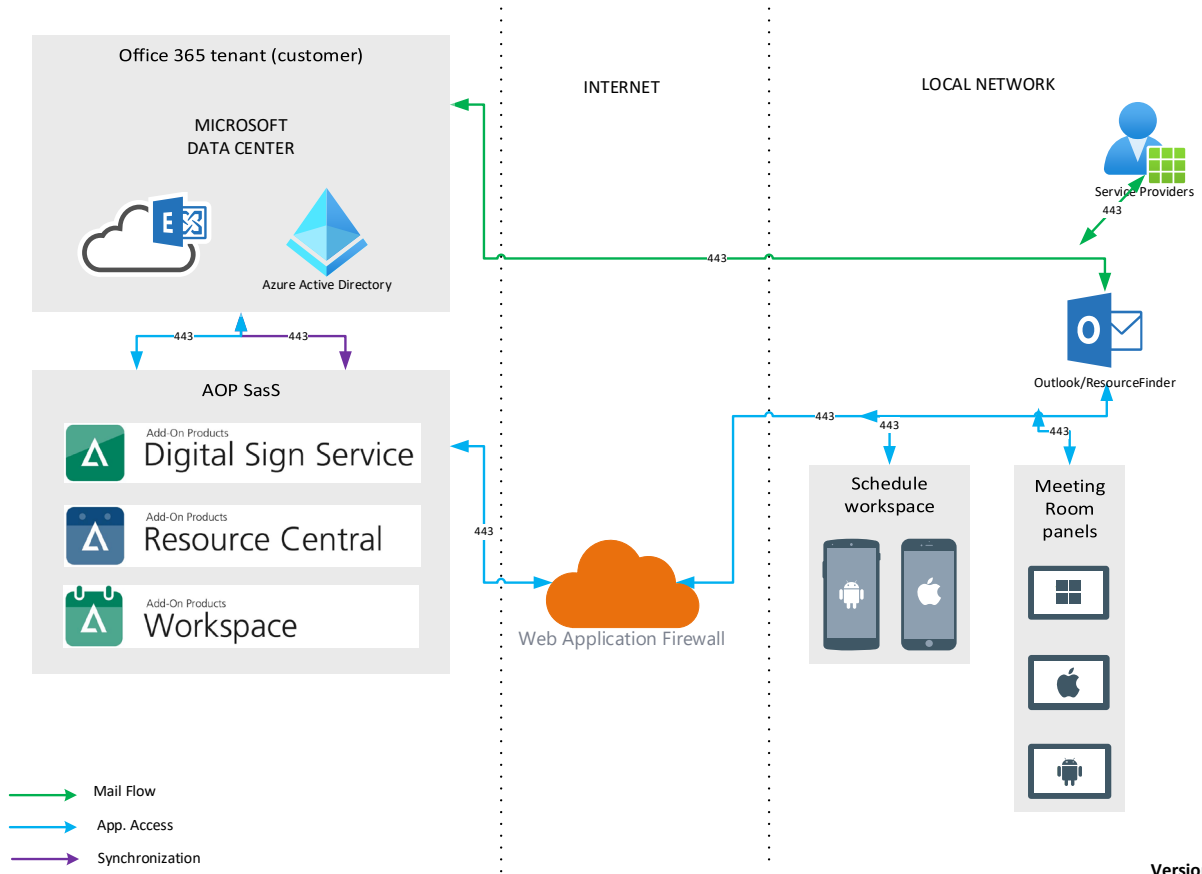
Security Incident Response, in case of a system alert, events are escalated to our 24 / 5 teams providing Operations, Network Engineering, and Security coverage. Employees are trained on security incident response processes, including communication channels and escalation paths.

Data History Storage and Availability

Add-On Products ensures a 24-months period of data history storage and access starting from the date of Subscription Start Date as listed in the End User License Agreement issued by us.

If data storage and access extending further than 24 months is required, this can be provided for an additional ongoing cost depending on your requirements. Please notify such a need to Add-On Products directly before the initial period of 24 months expires.

Platform architecture 1