oneAdvanced

Financials
Security

Stability and Security by Design

Financials has been designed from the outset to be a true Software as a Service (SaaS) solution, delivered using Amazon Web Services (AWS), the global leader in cloud infrastructure, and following the AWS Well-Architected Framework. The Well-Architected Framework is built around six pillars: operational excellence, security, reliability, performance efficiency, cost optimisation and sustainability.

We work closely with AWS Solutions Architects to ensure that Financials is scalable, responsive, and above all, secure. Regular monitoring and evaluation, using a variety of cyber detection tools and processes, including the AWS Well-Architected Tool, Alert Logic, AWS WAF, AWS Shield and CloudWatch help us identify or block potential issues before they become problems.

Controlled Access

We carefully control where data is stored and who, if anyone, can access it. Comprehensive identity and access controls are combined with continuous monitoring to ensure that access is both controlled and audited.

Harnessing a variety of security capabilities, that are uniquely available on the AWS Cloud. Routine security tasks are automated, reducing the need for human intervention therefore mitigating the chance of errors and improving security.

Encryption, Detection and Prevention

AWS provides world-class secure global infrastructure, and your Financials connections are always encrypted.

- Network inspection tools help us detect and protect against malicious or unauthorised traffic

- Centralised logging, reporting and analysis provide visibility and security insights

- User identity, access policies and entitlements are carefully designed and managed to help enforce business governance. This includes user authentication, authorisation, and single sign on

- Application code and deployments are regularly scanned for security vulnerabilities using a variety of both AWS tools for deployed code and code analytic tools to monitor and report on known and emerging vulnerabilities in 3rd party frameworks and libraries

Flexible, Reliable and Available

Financials is delivered from multiple servers, across multiple data centres in the AWS London Region. It is monitored for performance, stability, and accessibility with automatic recovery/ restart if a component is found to be unreliable.

- Auto-scaling technology - Predictable capacity provision

- Non-intrusive maintenance

- Automatic reaction to changes in demand - Right-sized environment

- Silent upgrades - Regularly upgraded

- Managed daily backup service - 15-minute snapshot & recovery capability

Designed to provide 99.5% availability and a recovery point objective (RPO) of 60 seconds.

Penetration Testing and Data Protection

Penetration Testing (Pen Testing) is a crucial security practice that helps OneAdvanced identify whether there are any potential vulnerabilities in our products by simulating real-world attacks. Financials has been fully tested by a CHECK-accredited penetration testing company and will continue to be tested and audited regularly by a National Cyber Security Centre approved, CHECK-accredited penetration testing company.

All customer and proprietary data is protected through a robust Information Security Management System (ISMS) that is certified to ISO 27001. OneAdvanced is an accredited Cyber Essentials Plus and NHS Digital Data Security and Protection Toolkit supplier. Our ISMS meets the ten mandatory clauses and all 114 controls of ISO 27001, including:

- Data in transit protection

- Asset protection and resilience

- Separation between consumers, each consumer has a separate database schema and application instance

- Governance framework

- Operational security

- Personnel security

- Secure development

- Supply chain security

- Secure consumer management

- Identity and authentication

- External interface protection

Application Security

Financials guards against unauthorised access through its own robust security functionality, providing granular control over options and data available to software users. Logging-in requires a valid username and password, utilising Multi Factor Authentication, to determine users' access to data and functionality, which is controlled by one or more security profiles.

Comprehensive tools enable administrators to easily audit all system access for peace of mind and accountability.

UK GDPR Compliance

At OneAdvanced we take the protection of personal data seriously and comply with the Retained Regulation (EU) 2016/679 (UK General Data Protection Regulation) and the Data Protection Act 2018 as applicable to general processing of personal data (UK GDPR).

We have taken the appropriate and proportionate technical and organisational measures to ensure the security of any personal data processed in accordance with UK GDPR. When necessary, OneAdvanced will conduct a data protection impact assessment (DPIA) to identify any potential security risks and how to mitigate them.

Our appointed Data Protection Officer oversees our compliance with UK GDPR and enforces strict policies, procedures and staff training is in place to protect personal data from unauthorised or unlawful use and accidental loss, destruction, or damage.

Secure Support

All staff across OneAdvanced undertake mandatory annual security training, and are contractually bound by our Security Policy, Data Security Agreement, Acceptable Use Policy, Data Protection Policy, and our Patient Data Policy. Access to customer systems is only allowed following explicit authorisation from the customer each time, and all access is recorded and regularly audited.

A Safe Choice

We have taken great time and care to make sure Financials is as flexible, scalable, and secure as possible. We invested right from the outset to make sure the underlying design and architecture held these principles at their core, and continued that through into the solution's development, deployment, and ongoing support. Helping protect your people, your data, and your investment too.

For information on upgrading to Financials
please contact your OneAdvanced Account Manager or speak to our support team

Get in touch

Want to find out more?
Contact one of our team members today!

oneAdvanced

+44(0) 330 343 4000   www.oneadvanced.com   hello@oneadvanced.com