Data Security Teams:
Our approach to cloud security

Introduction

At Tax Systems, we are proud to have a history of working with over 1,500 clients across the UK and Ireland for nearly 30 years. Some of these clients are amongst the largest financial institutions in the world and we also work with 23 of the largest 25 accountancy firms in the UK & Ireland. Working with this broad range of clientele requires us to adhere to the highest standards of data protection to ensure that our clients' data is always secure.

This document is intended to give security professionals peace of mind when considering Tax Systems as a vendor. We will take you through our approach to security and provide an overview of the full range of measures we have put in place to protect our customers. This includes our approach to Web Application Firewall (WAF), our use of Windows Defender, and how we encrypt data both at rest and in transit. In addition to this, we cover our approach to ISO certification.

ISO27001

During 2020 we began work to achieve ISO27001 certification, a well respected international standard that verifies the ability of the organisation to manage data securely.

We are due to be formally assessed in late June 2021, and should achieve our formal certification during the third quarter of 2021. Once we have this certification in place we will be sure to inform you!

The Tax Systems 'Security Six'

As well as ensuring we are compliant with the ISO certification process, we wanted to go further. To that end, we have six key areas that we focus on to ensure that data is secure on an ongoing basis, that we call the '**Security Six**'. These are:

Antivirus protects users from new malware by holding suspicious files and sending samples to the cloud protection service to rapidly make a verdict (advanced real-time defense).

Windows Defender

Encryption

- Data is encrypted both in transit and at rest
- We use TLS 1.2 and AES-256 to encrypt data

Web Application Firewall (WAF) protects from harmful incoming web traffic by blocking threats.

- Isolates end points from incoming threats during sharp traffic increases.
- Security perimeter outside of internal or cloud infrastructure, helping to keep malicious traffic a safe distance from your application and data servers.

WAF

'Security Six'

Business Continuity

- Microsoft Azure Disaster Recovery technologies are in place 24/7 to ensure business continuity in the case of disaster.
- Our Business Continuity Plan is tested each day due to the measures in place to allow all staff remote access to our systems.
- All services have a Disaster Recovery Plan, which includes the recovery of technology, access to off-site technology and telephony. We have successfully decentralised our business so that employees can be on-site or off-site as deemed necessary.

MFA is a multi-layered security system that verifies the identities of users for login. By leveraging multiple authentication layers, even if one element is damaged or disabled, the user's account will remain secure.

- Offers additional protection through multiple layers of security and checks
- Microsoft's OpenID Connect is integrated with Azure AD provides MFA through password and a one time SMS/call.

MFA

Backups

Microsoft Azure's standard backup and geo-replication facilities.

- Data is Geo-replicated to the secondary UK datacentre using Geo-redundant storage.
- All backups are secured with Azure Storage encryption.
- Files stored with Azure Storage use "Soft-deletion" - if they are deleted or overwritten a snapshot is taken and is available for 365 days.

Outside of our "Security Six", there are other areas we cover to ensure that we meet the highest standards of Information Security:

Coding standards

Development practice: The development of software within Tax Systems follows Agile/SCRUM methodology, with all code peer reviewed before being committed to the codebase.

Code analysis: Static code analysis is performed, which includes reporting on security issues from the SANs Top 25 and OWASP Top 10. The CTO, Tax Technology Directors, Architects and Senior Software Engineers are involved in controlling and applying these security standards.

Data loss prevention

We employ the following measures to ensure that sensitive data is not lost, misused or accessed by unauthorised users:

Information classification: We log all service, user and security events on secure infrastructure for 365 days in SIEM which are monitored real-time by the SOC.

Security: Access to data is managed by a uniform manner across the organisation which prevents business data from being accidentally published to the wrong app.

Assurance: All data is automatically protected and attempted breaches are monitored and reported in real-time.

Privileged Identity Management (PIM)

Management: Access to our applications and source code based on the principle of 'least privilege' and restricted to authorised users. This is a small team of core engineers, and administrative access is restricted to just four individuals in the business. Privilege and administrative access is reviewed every 6 months by the CTO.

Logging of access: Timeboxed 'Just Enough Administration' (JEA) reduces risk to all AD accounts. We have added additional logging tracking to show who used which privileges and when.

Control & monitoring: We keep track and audit with a PIM log history review, alerting administrators with a well-established investigation process.

Azure Monitoring – Sentinel SIEM & SOAR

Response: Within Azure Sentinel, we use Microsoft's Fusion technology which employs AI to automatically monitor and respond to threats.

Monitoring & Collection: We also use Azure Sentinel to centralise our security data, and the Tax Systems environment (hosted and endpoint) is monitored 24x7x365 by a SOC team using Microsoft Sentinel SIEM.

Azure Monitoring – Managed Detection & Response (MDR)

Communication: Our established incident and breach management process ensure we provide a swift response, reporting any incidents to the data controller without undue delay. There have been no such events in the past 24 months.

Metrics: Azure Sentinel gives our administrators metrics and logs of all information, so that responding to a breach can be done in a timely manner.

Conclusion

Overall, we are well-versed at having detailed conversations with our customers around security, and part of our role as a business includes responding to security questionnaires to ensure that we meet the standards that expected. We haven't failed one to date, and we don't intend to going forwards!

As an organisation, we believe that security shouldn't be something "after the fact" or a "tick in the box" but something that is actively discussed in the process of licensing our software. We are keen to be on the front foot when it comes to security and ensure that our customers are constantly protected when choosing to work with Tax Systems.