What Keeps You Secure

Authentication

Authentication services are key to controlling who has access to your systems. This can be implemented directly against client's existing LDAP or Active Directory repository. Multifactor Authentication (MFA) is supported with a range of modern security factors for business implementation flexibility.

Single-Sign-On (SSO)

Integrate with a single sign on portal through SAML 2.0 integration for access to multiple applications and secure identity management.

Transaction Security

Native support for TLS encryption and run-time validation of user actions.

Built-in SOA framework for integration with external authorization and custom authorization rules.

Application logic is carried out through stored procedures based on internally generated session ID, action ID and object ID that are validated by the workflow engine.

Logs and Audit Trails

In addition to producing logs and audit trails these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation.

Data at Rest

Data at rest or data stored in persistent storage is encrypted using the Advanced Encryption Standard (AES).

Latency

Worldwide data center support for OneShield Cloud implementation allows us to meet region based regulatory requirements and lower latency for global customers.

Web Service Security

All web service integrations with external systems are built utilizing transport confidentiality, server authentication, user authentication, transport encoding, and message integrity. Web services are encrypted utilizing TLS with certificates from trusted providers as well as digital certificates for files and documents.

Authorization

Establish specific role-based authorization and access for users and groups. Authorization can be controlled down to the level of every business object.

Secure Client Data

Data masking is utilized to hide original data in configurable fields to protect personal information.

Employee & Vendor Validation

Employee and third-party access is secure at authentication, authorization, auditing with encryption and expiry. Grant secure access only to those employees and partners you trust.

Firewalls

Web Application (WAF) and Next-Generation firewalls with enhanced level of filtering and control. Intrusion detection system (IDS) and Intrusion preventions systems (IPS) monitor all traffic to and from the application.

Regulatory Requirements

Regulators on both sides of the Atlantic are hyper-aware of threats and are placing increased demands on the industry. Staying abreast of pertinent existing and changing regulations strengthens our security strategy.