Product Overview | Security

OnBase: a Secure, Protected Environment

Critical information secure at every data state

Security is at the core of platform

Configuration tools simplify security administration

Meets key federal security standards

OnBase is designed to be one of the most secure enterprise information platforms on the market. Our dedication to security gives our government organizations peace of mind in the confidentiality, integrity and availability of their data. The OnBase platform can be deployed in a DoD 5015.2 environment for records, supports two- factor authentication like Common Access Card (CAC), PIV authentication and can be deployed in a FIPS 140-2 compliant manner.

OnBase is developed with security in mind—from inception through release and beyond. Hyland employs a dedicated application security team that is tasked with carrying out advanced security practices on the software as well as training and consulting company-wide on security-related matters. Together, these practices ensure that government information is secure at every data state: at rest, in transit and in use.

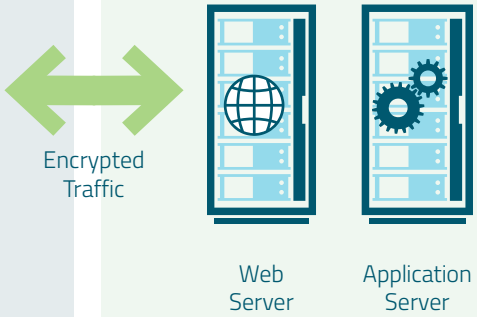
Together, these practices ensure that customers' critical information is secure at every data state: at rest, in transit and in use.

INFORMATION IS NATIVELY SECURED AND CAN BE ENCRYPTED:

1 AT REST
While not actively in use

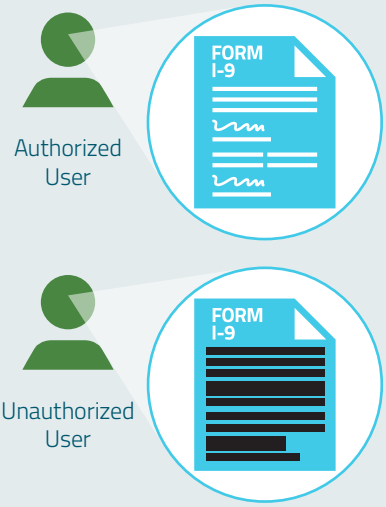
- No one can access private data outside of OnBase.
- Even if the network is broken into, there are additional levels of protection.

2 IN TRANSIT
Being transported between servers and within the database



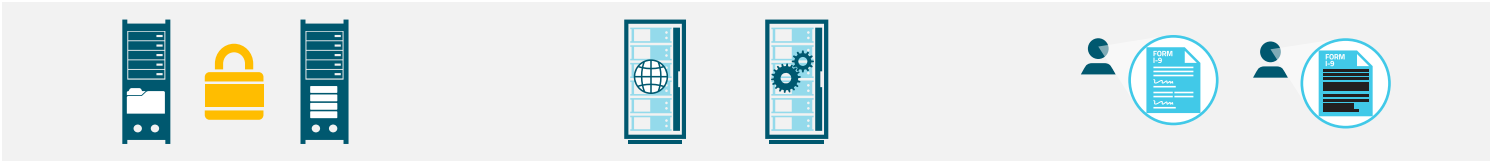
- Even if data is intercepted in transit, encryption ensures that the information can't be used.

3 IN USE
Currently accessed by authorized users



- Only authorized users can access information, as configured by the administrator.

HOW DOES THIS WORK?



1 AT REST

All data stored in the system can be encrypted with AES-256 or AES-128 (Advanced Encryption Standard, or AES).

Keyword values, used to classify specific documents in the database, can also be encrypted with AES-256 or AES-128. Should the database be accessed by an unauthorized user, the keywords will be unreadable.

Data exported to removable media, like a CD or DVD, can also be encrypted.

2 IN TRANSIT

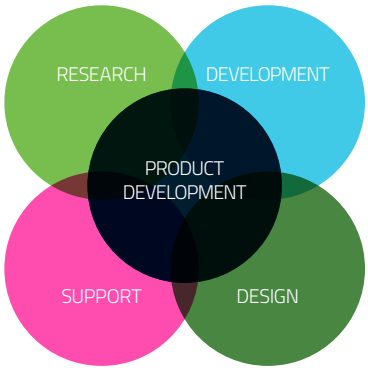
Transport Layer Security, or TLS, is supported to protect communication of data. OnBase always supports the latest version of TLS.

OnBase Distributed Disk Services, or DDS, uses an AES-128 encrypted connection to ensure that if traffic is intercepted, data will be unreadable and unusable.

3 IN USE

Configurable session timeouts prevent unauthorized users from accessing any data on a user's screen after a specific amount of time has passed (without signing in using valid credentials and re-authenticating OnBase).

Keyword values may be masked, preventing unauthorized users from viewing sensitive data.

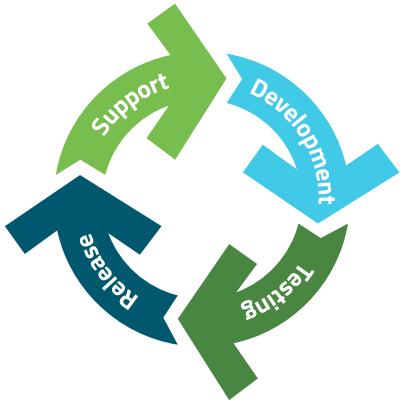


Security Throughout Product Development

Hyland considers application security in every step of the product development process, including research, development, design and support. Hyland's development process is informed by a security lifecycle program that was started by Microsoft, influenced by best practices and customized for Hyland. It integrates security into each development phase.

Throughout the development process, built-in 'gates' require the security team to sign off on development before the next phase can begin. The last gate is directly before launch.

Threat modeling and risk assessments are performed throughout the entire process, allowing the team to proactively identify and address any potential issues.



Support Through Launch and Beyond

Hyland considers the post-launch phase to be an essential element of the product lifecycle, and continues to provide support by proactively monitoring, identifying and remediating any security concerns that may arise after OnBase is launched.

To continuously test for vulnerabilities, exploits, vectors and bugs, the team uses various methods including:

- Secure development practices
- Automated security scanning
- Manual penetration testing

If a vulnerability or issue is identified, the Hyland security team is alerted. The team reviews, prioritizes and fixes the issue, and then communicates with OnBase customers so they can immediately remediate.

Dedicated Security Team

Hyland has a dedicated application security team that expertly monitors the security of the OnBase product, continually searching for new ways to proactively enhance security. The team provides extensive initial and ongoing training to the entire R&D staff—including both developers and testers. They also render security expertise and consultation to the company at large.

Built-In Security

Security functionality comes standard with OnBase, whether it is deployed on-premises or in the cloud. These access controls include strict policies with configurable complexity requirements; granular rights management that enables admins to control access to every part of the system, to ensure that users can only access data they are authorized to see; and security keywords that ensure unauthorized users cannot see any data associated with a keyword they don't have clearance to access.

Enhanced Measures

Administrators can easily configure enhanced security measures in their OnBase deployments. They can use encrypted disk groups and encrypted alphanumeric keywords, both using AES-256 or AES-128 encryption. Distributed disk services can also be used to protect data from being read if intercepted, using AES-128 encryption. Digital signatures can be used to alert users to unauthorized content modification after a document has been signed.

Seamless Integrations

OnBase integrates with other external security systems to create a seamless experience for your users. Single sign-on (SSO) integrations include Active Directory (AD), Active Directory Federation Services (ADFS), Security Assertion Markup Language (SAML) and Lightweight Directory Access Protocol (LDAP). Permissions in AD and LDAP solutions can also be replicated in OnBase.

Meets federal security standards and needs

OnBase offers a DoD 5015.2 environment for records, supports two-factor authentication like Common Access Card (CAC), PIV authentication and can be deployed in a FIPS 140-2 compliant manner so that modernization, efficiency and streamlining efforts can also be secure.

Learn more at **OnBase.com/Security »**

NAVIANT®
Process focus. Excellence.

Naviant is a top-tier Platinum & Diamond OnBase Partner founded in 1986 with our "process-first" approach. Learn more at naviant.com.

OnBase® by Hyland