

OnBase: Un entorno seguro y protegido

La información confidencial se encuentra segura en todos los estados de los datos

La funcionalidad de seguridad es un estándar, ya sea que su implementación sea en sitio o en la nube

Los administradores pueden configurar fácilmente las medidas de seguridad mejoradas

Hyland cuenta con un equipo dedicado a la seguridad de las aplicaciones

OnBase ha sido diseñado para ser una de las plataformas de información empresarial más seguras en el mercado. Nuestra dedicación a la seguridad le ofrece a nuestros clientes la tranquilidad y confianza sobre la confidencialidad, integridad y disponibilidad de sus datos.

OnBase es desarrollado teniendo en cuenta la seguridad, desde su comienzo hasta su lanzamiento, y más allá. Hyland cuenta con un equipo dedicado a la seguridad de las aplicaciones, que realiza prácticas de seguridad avanzadas en el software, y ofrece capacitación y consultoría en toda la empresa sobre asuntos relacionados con la seguridad.

Cuando estas prácticas se combinan, aseguran que la información confidencial de los clientes se encuentra segura en todos los estados: ya sea que se encuentren en reposo, en tránsito y en uso.

LA INFORMACIÓN SE ENCUENTRA SEGURA DE MANERA NATIVA Y PUEDE SER ENCRIPTADA:



¿CÓMO FUNCIONA?



1 EN REPOSO
Toda la información almacenada en el sistema puede ser encriptada mediante AES-256 o AES-128 (Estándar de cifrado avanzado o AES).

Los valores de palabras clave utilizados para clasificar documentos específicos en la base de datos, pueden también encriptados con AES-256 o AES-128. En caso de que la base de datos sea accedida por un usuario no autorizado, las palabras clave no podrán ser leídas.

Los datos exportados a medios removibles tales como CD o DVD, pueden también ser encriptados.

2 EN TRÁNSITO
La Seguridad de la capa de transporte, o TSL, es soportada para proteger la comunicación de los datos. OnBase siempre soporta la última versión de TLS.

Los Servicios de discos distribuidos de OnBase, o DDS, utilizan una conexión encriptada AES-128, para asegurar que si el tráfico es interceptado, los datos no podrán ser leídos o utilizados.

3 EN USO
Los tiempos de espera de la sesión son configurables, lo que evitan que usuarios no autorizados accedan a cualquier información en la pantalla de un usuario luego de que haya transcurrido un tiempo específico (sin ingresar sesión con credenciales válidas y autenticando OnBase nuevamente).

Los valores de palabras clave pueden ser enmascarados, evitando que usuarios no autorizados vean información confidencial.



La seguridad a través del desarrollo del producto

Hyland considera la seguridad de las aplicaciones en cada etapa del proceso de desarrollo del producto, incluidas las etapas de investigación, desarrollo, diseño y soporte. El proceso de desarrollo de Hyland es informado por un programa de ciclo de vida de seguridad, que fue iniciado por Microsoft, influenciado por prácticas óptimas y personalizado por Hyland. Integra la seguridad en cada etapa del desarrollo.

A través del proceso de desarrollo, “cerkas incorporadas” requieren que el equipo de seguridad apruebe el desarrollo antes de comenzar la siguiente etapa. La última cerca se encuentra antes del lanzamiento.

Se realizan modelos de amenazas y los análisis de riesgo a través de todo el proceso, lo que permite que el equipo identifique y solucione cualquier problema potencial, de manera proactiva.

Soporte a través del lanzamiento y más allá

Hyland considera la etapa posterior al lanzamiento, como un elemento esencial del ciclo de vida del producto, y continúa ofreciendo soporte mediante el monitoreo proactivo, identificando y solucionando cualquier preocupación sobre la seguridad que pueda surgir una vez que se ha lanzado OnBase.

Para realizar pruebas continuas sobre las vulnerabilidades de seguridad, vectores y errores, el equipo utiliza métodos variados entre los que se incluyen:

- Prácticas seguras de desarrollo
- Escaneos automatizados de seguridad
- Pruebas de penetración manual

Si se identifica un problema o una vulnerabilidad de seguridad, el equipo de seguridad de Hyland recibe una alerta. El equipo realiza una revisión, prioriza y soluciona los problemas, y luego se pone en contacto con los clientes de OnBase para que puedan remediar la situación inmediatamente.

“OnBase ofrece seguridad a nivel del documento, lo que permite restringir en detalle lo que los usuarios pueden hacer, cuando se trata de lo que pueden ver, si pueden imprimirlo o incluso enviarlo por correo electrónico. Nadie más ofrece esa funcionalidad”.

- Eric Olson, Director de administración, Sistema de Pensión de los Oficiales de Policía de Houston



Equipo dedicado de seguridad

Hyland cuenta con un equipo dedicado a la seguridad de las aplicaciones que monitorea la seguridad del producto OnBase, buscando continuamente nuevas maneras de mejorar la seguridad de manera proactiva. El equipo ofrece extensa capacitación inicial así como continua para todo el personal de Investigación y Desarrollo, incluyendo tanto a desarrolladores como a los probadores. También ofrecen su pericia en temas de seguridad y consultoría a toda la compañía.



Seguridad integrada

La funcionalidad de seguridad es un estándar OnBase, ya sea que su implementación sea en sitio o en la nube. Estos controles de acceso incluyen políticas estrictas con requisitos de complejidad configurables; administración granular de derechos que permite a los administradores controlar el acceso en cada parte del sistema, para asegurar que los usuarios tengan acceso sólo a la información que tienen autorización para ver. Ofrecen a su vez palabras clave de seguridad que aseguran que los usuarios no autorizados no puedan ver la información asociada con una palabra clave a la que no tienen permiso de acceso.



Medidas mejoradas

Los administradores pueden configurar fácilmente las medidas de seguridad mejoradas en sus implementaciones de OnBase. Pueden utilizar grupos de discos encriptados y palabras clave alfanuméricas encriptadas, ambas con una encriptación AES-256 o AES-128. Servicios de discos distribuidos también pueden utilizarse para proteger que los datos sean leídos en caso de ser interceptados, utilizando una encriptación AES-128. Las firmas digitales pueden ser utilizadas para alertar a los usuarios de modificaciones no autorizadas de contenido, luego de que el documento haya sido firmado.



Integraciones sin interrupciones

OnBase se integra con otros sistemas de seguridad externos para crear una experiencia impecable para sus usuarios. Integraciones de inicio de sesión único (SSO) incluyen Active Directory (AD), Active Directory Federation Services (ADFS), Security Assertion Markup Language (SAML) and Lightweight Directory Access Protocol (LDAP). Los permisos en las soluciones de Active Directory y LDAP pueden ser replicadas en OnBase.

Obtenga más información OnBase.com/Seguridad »