

Highlights

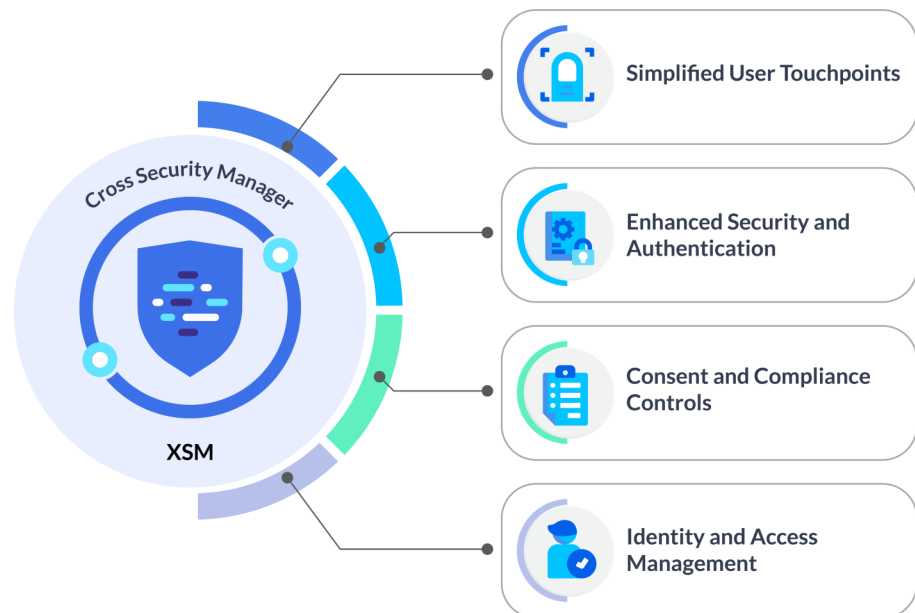
- *Enhanced security across all applications*
- *Complete Identity and Access Management*
- *Improve the customer/user experience*
- *Simplify the entire account management lifecycle*
- *Fraud prevention*
- *Drive and enforce compliance policies*

No matter if it's stored on site or in the cloud, the data that companies create is one of their most valuable assets. Protecting that data is a top priority. The **Cross Security Manager (XSM)** from **3Insys** provides additional layers of security that enables companies to increase their security, protection, and compliance to security policies while improving the user experience.

Today's utility Information Technology (IT) organizations have multiple complexities that bring tremendous challenges to overcome, including:

- Today's consumers have multiple channels (devices, applications, mediums) to access their data, including via a voice portal.
- Older applications may not support current authentication protocols.
- Internal applications can connect the users to external applications that are provided by 3rd party partners or located in the cloud.
- Pressure from their customers to improve the overall user experience.

To overcome these challenges, the Cross System Manager delivers multiple layers of security, that can be deployed in full or just the components



The Cross Security Manager provides a 360-degree approach to security across the entire IT environment.

Cross Security Manager	Key Features
Enhanced Security and Authentication	<ul style="list-style-type: none"> • Anomaly and Fraud Detection • API Security Management • Multi-Factor Authentication (MFA) • Adaptive Authentication
Identity and Access Management	<ul style="list-style-type: none"> • User/Identity Provisioning and Lifecycle Management • User Profile and Identity Administration • Centralized User Management • Bidirectional Access Control
Simplified User Touchpoints	<ul style="list-style-type: none"> • Single Sign-On • Omni-Chanel • Progressive Profiling
Consent and Compliance Controls	<ul style="list-style-type: none"> • Consent and Privacy Management • Compliance Policy Management

Anomaly and Fraud Detection—Information is evaluated for risk by an **advanced risk/fraud detection engine** which selects the appropriate authentication mechanisms and permit or deny access, or transaction completion. Identity analytics can be used to identify a returning user and generate a risk score based on the device, IP address, geolocation or user behavior.

API Security Management—Applications that support internal operations and the applications that support external facing applications (e.g., B2B partners, cloud applications, portals) communicate using Application Programming Interfaces (APIs). XSM **removes access vulnerabilities** and delivers the necessary security for APIs to protect user data from access by other applications, users, and teams.

Multi-Factor Authentication—With increases in computing power, today’s security threats require much more robust protection the just passwords to protect information.

Adaptive Authentication—A non-static authentication system which takes into account the profile of the agent requesting access to the system then determines the risk profile associated with that transaction. Based on the rick factors, the system will decide whether to use SMS OTP or use knowledge based authentication (KBA). With increases in computing power, today’s security threats require much more robust protection **the just** passwords to protect information.

User/Identity Provisioning and Lifecycle Management—**Simplifies the user provisioning process** and ensures that the user identities are synchronized across the systems

User Profile and Identity Administration—Provide visibility, detect unauthorized access, and manage profiles.

Centralized User Management—Centralized management for user identities and passwords.

Bidirectional Access Control—Integrate access authentication across application domains.

Single Sign-On—Enables users to login with common credentials across multiple digital applications/systems by supporting the standard federation protocols—such as SAML, OAuth and OIDC.

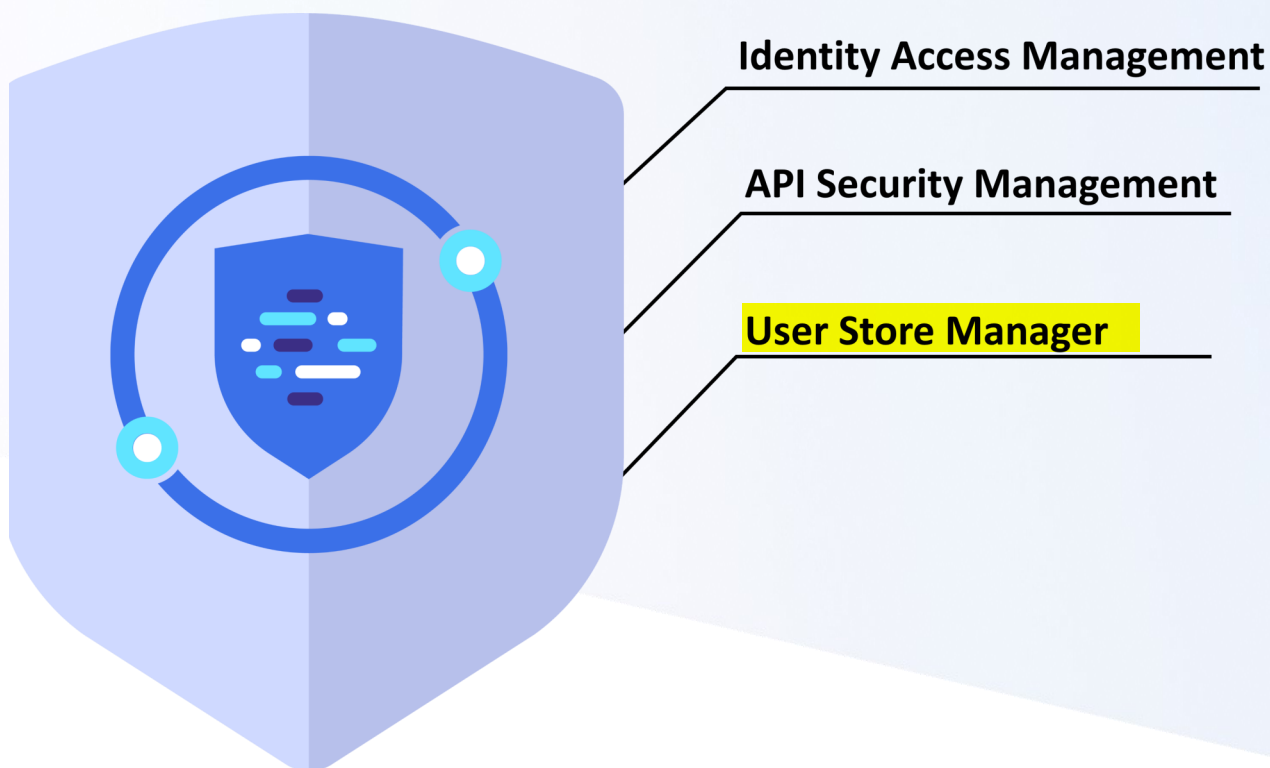
Omni-Channel—The applications, devices, and mediums (i.e., channels) customers use to access data vary from user to user and organization to organization. Omni-channel delivers the ability to authenticate the customer through multiple channels and manages the customer’s preferences through those channels to build a unified customer profile. Omni-channel provides a better overall customer experience no matter which channel they use.

Progressive Profiling—Allows an organization to build a comprehensive profile for each user over time. When an account is first registered, the user isn’t inundated with multiple questions. Instead, users are only asked to provide a few attributes to their profile. As the user becomes more comfortable, smaller additional pieces of information are requested to fill out the profile.

Consent and Privacy Management— As organizations grow, the amount of customer identity data collected to make more personalized and context-based decisions increases. Organizations must follow the rules and regulations pertaining to gathering user data enforced by governments and different industrial bodies. Not complying with these regulations is critical because violations can lead to brand damage, lost customer trust, and fines. A holistic system for managing consents and provides consumers with the ability to view, edit, export, and delete their profile data.

Compliance Policy Management—Unify, maintain, and enforce compliance policies across the organization.

The Cross Security Manager



© 2021 3Insys. All rights reserved. While [3Insys](https://www.3insys.com) intends to provide accurate marketing material, products and features change over time. As such, 3Insys provides no guarantee or promise regarding the completeness or accuracy of this material. The descriptions provided in this paper are for informational purposes to aid understanding.

T: (+1) 323-488-2846 **E:** contactus@3insys.com **W:** www.3insys.com

A: 601 S Figueroa St #4650, Los Angeles, CA 90017