

IntelliAuth:
Enhancing
Consumer
Identity

Table of Contents

The Evolving Cybersecurity Landscape and Identity Risks	03
The Growing Significance of Identity Protection and Authentication	03
Cymmetri IntelliAuth - Smart Authentication for Enhanced Security and User Experience	05
Registration	06
Passwordless Authentication - Maximising Connectivity, Minimising Friction	07
Self-service	07
Support	08
Personalization	09
Privacy	10
Authentication	11
Enterprise connector	12
Scalability and Flexibility	12
A Vision for Tomorrow-IntelliAuth	13



The Evolving Cybersecurity Landscape and Identity Risks

In the fast-paced digital age, the cybersecurity landscape is constantly evolving, with cyber threats becoming more sophisticated and relentless. From data breaches and ransomware attacks to phishing and social engineering, the breadth and complexity of cyber threats have grown exponentially. Amidst this shifting landscape, one of the most critical areas of concern is identity risks. Hackers and malicious actors are increasingly targeting individuals' identities, aiming to gain unauthorised access to sensitive data, financial resources, and valuable intellectual property.



The Growing Significance of Identity Protection and Authentication

As identity risks escalate, the importance of robust authentication mechanisms becomes important. Traditional username-password combinations, once deemed sufficient, now fall short in providing adequate protection against identity-related threats. Cybercriminals have fortified their techniques, exploiting weak passwords, stolen credentials, and social engineering tactics to bypass conventional authentication methods.

The growing significance of Identity Protection stems from the increasing risks posed by cyber threats in today's interconnected digital world. As individuals and organisations conduct a significant portion of their activities online, protecting digital identities has become a critical priority.





Below are some key aspects highlighting the importance of Identity Protection.



→ Identity as the New Perimeter:

Traditionally, cybersecurity focused on securing the network perimeter. However, with the rise of remote work, cloud computing, and mobile devices, the concept of the perimeter has dissolved. In this new landscape, identities have become the primary gatekeepers, and securing them is essential to prevent unauthorised access and data breaches.

→ Proliferation of Personal Data:

The digital age has led to an explosion of personal data being collected, stored, and shared online. Cybercriminals seek to exploit this abundance of personal information to engage in identity theft, financial fraud, and other malicious activities. Robust Identity Protection measures are necessary to safeguard sensitive data from falling into the wrong hands.

→ Rise of Credential-Based Attacks:

Password-based authentication remains a common entry point for cybercriminals. Weak passwords, password reuse, and phishing attacks have made credential-based attacks a prevalent threat.

→ Regulatory Compliance and Data Privacy:

Various data protection regulations, such as the General Data Protection Regulation (GDPR) mandate organisations to protect users' personal data. Failure to comply with these regulations can result in severe financial penalties and reputational damage, underscoring the importance of robust Identity Protection practices.

→ Impact on Business Reputation:

A data breach or identity-related incident can severely tarnish an organisation's reputation and erode customer trust.

→ Importance in Digital Transactions:

Online transactions, such as e-commerce, banking, and payment systems, rely heavily on secure identity verification. Robust Identity Protection ensures the integrity of digital transactions, safeguarding both businesses and consumers.

→ Preventing Insider Threats:

Identity Protection is not solely about external threats; it is equally vital in mitigating insider threats. By implementing appropriate access controls and monitoring user behaviour, organisations can detect and prevent malicious actions by insiders.





Cymmetri IntelliAuth - Smart Authentication for Enhanced Security and User Experience

In response to the increasing complexity that organizations encounter today, a comprehensive and innovative approach to authentication is essential. IntelliAuth Specifically tailored to meet the Authentication needs of enterprises and large organizations & internet facing applications, this solution is user-friendly, AI-driven, and built on the CYMMETRI Identity Cloud, a scalable and high-performance platform that provides a single platform to manage all identities.

How IntelliAuth work





Registration

The first impression your customers have during registration is crucial and often their very first interaction with your platform. A misstep in this process can lead to new users abandoning the registration form, resulting in potential loss of future revenue. To ensure customer delight, it is essential to offer a fast and seamless registration experience by gathering only necessary information or providing alternative registration methods, such as social registration or using third-party identity providers.

The objective is to streamline registration and minimise friction for users. Here's how Cymmetri Intelliauth addresses this challenge:

1 Multiple Registration Options:

Intelliauth supports various registration options, including social registration, standard fields, or registration through other identity providers. This empowers users to choose the method that best suits their preferences and convenience.

2 Single Sign-On (SSO):

Implementing SSO allows users to have a unified registration experience and a single set of credentials to access all applications. This simplifies the login process and reduces the need for users to remember multiple usernames and passwords.

3 Customizable Registration Pages:

Intelliauth offers customizable registration pages, enabling businesses to tailor the experience to align with their brand identity. This customization fosters a sense of familiarity and trust with users during the registration process.

4 Convenient and Secure Password Policies:

To strike a balance between convenience and security, Intelliauth implements password policies that are both user-friendly and robust enough to protect against unauthorised access.

Instead of burdening your customers with a lengthy and cumbersome registration form, offer them the option to register using their existing Facebook or Google accounts. This way, they can complete the process quickly and effortlessly, eliminating the need for redundant data entry.

By adopting identity-driven registration practices, businesses can significantly improve the onboarding experience for their customers. A fast and frictionless registration process enhances user satisfaction, increases user retention, and ultimately leads to a positive impact on revenue and brand reputation.





Passwordless Authentication - Maximising Connectivity, Minimising Friction

Your customers desire a seamless authentication experience without unnecessary complexities. They also prefer a unified sign-on process across all your digital platforms. This is where passwordless authentication emerges as the solution & Intelliauth offer this as out of the box.



Self-service

Your customers prefer not to go through the hassle of contacting customer support to make simple changes to their account information. Self-service, a fundamental identity capability, empowers customers to independently update and manage their personal details, such as mailing addresses, email addresses, or phone numbers. However, the benefits of self-service extend beyond this convenience. Customers also need the ability to make changes once and have those updates applied seamlessly across all applications.

→ Access to a Single Source of Truth:

All applications have access to a central repository of customer data, which serves as the single source of truth. This eliminates data inconsistencies and provides a unified and accurate view of customer information.

By leveraging Intelliauth, businesses can provide seamless self-service capabilities to customers, allowing them to manage their account information effortlessly. This results in enhanced customer satisfaction, reduced support requests, and a consistent and reliable customer experience across all channels.





Support

The objective is to resolve customers' problems quickly and efficiently without adding to their frustration. Here's how intelliauth addresses this challenge:

1 **Face Scan and Trusted Device Verification:**

Identity solutions can use face scans from trusted devices to verify customer identity, making the authentication process seamless and secure.

2 **Persistent Sessions:**

With persistent sessions, customer support representatives can engage with customers without repeatedly asking for identification. This personal touch improves the support experience by focusing on resolving the issue rather than reconfirming the customer's identity.

3 **Delegated Administration:**

Intelliauth offers delegated administration, allowing businesses to control which user data support reps can access or modify. This ensures that sensitive customer data remains protected from unnecessary exposure.

By leveraging Intelliauth solutions, businesses can streamline and enhance the support experience for their customers. A quick and efficient resolution to their issues, coupled with data protection measures, fosters customer satisfaction and strengthens trust in the support services provided.





Personalization

Similar to self-service, personalization focuses on creating consistent customer profiles, encompassing user data, preferences, and any other relevant information, regardless of how customers interact with your brand. Personalization enables businesses to leverage the preferences gathered from various channels to deliver tailored experiences, cross-sell products, and promote relevant content across all touchpoints.

The objective is to provide customers with consistent and seamless multi-channel experiences. Here's how Intelliauth addresses this challenge:

1 Consistent Preferences Across Channels:

Intelliauth ensures that customer preferences remain consistent across all channels, ensuring a unified and personalised experience.

2 Unified Customer Profile:

By maintaining a single customer profile that is accessible to all applications, Intelliauth exposes the same customer profile and preferences across the entire ecosystem.

3 Storage of Custom Attributes and Unstructured Data:

Customer profiles can store any custom attributes and unstructured data required by applications, enabling a comprehensive view of customer information.

4 Consolidation of Unified Profiles:

Intelliauth facilitates bi-directional sync, migration, and coexistence of unified profiles, ensuring seamless data integration and accessibility.

By leveraging Intelliauth, businesses can deliver personalised and relevant experiences across various channels, fostering customer loyalty, and maximising revenue potential.





Privacy

The objective is to provide transparent privacy and consent management to customers. Here's how identity addresses this challenge:

1 Collection and Storage of Consent:

Intelliauth facilitates the collection and storage of customer consent, ensuring that customers' preferences are recorded and respected.

2 Enforcement of Consent and Privacy Policies:

Intelliauth enforces consent and privacy policies seamlessly, without requiring modifications to individual applications or APIs. This centralised capability simplifies compliance and ensures uniformity across all customer-facing applications.

3 Transparency in Data Sharing:

Customers are provided with transparency regarding how their data is shared, offering them clear insights into data usage and building trust.

Enforcing consent and restricting data without requiring changes to apps, data consumers, APIs, or user stores simplifies consent auditing and ensures a seamless and compliant privacy management process.





Authentication



Authentication is the process of verifying the identities of your customers during their interactions with your digital platforms. However, customers prefer authentication methods that are painless and convenient, allowing them to prove their identity seamlessly.

By leveraging IntelliAuth, businesses can achieve a seamless and secure sign-on experience for their customers. A simple authentication process enhances user satisfaction, encourages brand engagement, and ultimately drives revenue growth.

Device Trust:

IntelliAuth examines the trustworthiness of the user's device, considering factors like device health checks to ensure secure access.



Blacklisted IP Address:

IntelliAuth checks against blacklisted IP addresses associated with suspicious or malicious activities, preventing access from potentially harmful sources.



Blacklisted Location:

IntelliAuth incorporates geolocation data to restrict logins from specific countries with higher security risks, safeguarding against international threats.



Impossible Travel Scenario:

IntelliAuth analyses login patterns and detects impossible travel scenarios, where a user's login is attempted from distant locations within an implausibly short time frame, preventing unauthorised access.



Attack Protection

Below are the contextual checks that IntelliAuth incorporates while the user is trying a login process:



Short-Lived Domain:

IntelliAuth conducts real-time checks for short-lived domains that are often used in phishing attacks, fortifying defences against deceptive websites.



IP Reputation:

IntelliAuth utilises IP reputation services to assess the reputation of the IP address attempting to log in, mitigating risks associated with suspicious or compromised IPs.



Unusual Number of Login Failures:

IntelliAuth monitors login failures and identifies unusual patterns, such as an unusually high number of failures, to detect potential brute-force attacks.



Unusual Time of Login:

IntelliAuth intelligently evaluates login times, considering the user's typical behaviour, to identify any unusual login attempts made during atypical hours, providing an additional layer of security.





Using these context-based authentication factors, the organisation can pair risk levels with suitable authentication requirements, such as prompting for MFA, allowing or blocking access to the system or using passwordless authentication for low-risk situations. IntelliAuth helps organisations differentiate between fraudulent users and authorised users.



Enterprise connector

The enterprise connector is a critical component in Consumer Identity Access Management (CIAM) as it establishes seamless integration between an organisation's consumer-facing applications and its internal enterprise systems. By acting as a bridge, it centralises consumer identity data, reducing the risk of data duplication and ensuring consistency across different applications.

Additionally, it facilitates the synchronisation of consumer profile information and preferences, maintaining accurate and up-to-date data across the organisation. Moreover, the enterprise connector enables the collection of consumer data from various sources, providing valuable insights into consumer behaviour, preferences, and engagement patterns, which can be leveraged for effective marketing and business strategies. Overall, the enterprise connector plays a pivotal role in enhancing security, data management, and customer experience within the CIAM ecosystem.



Scalability and Flexibility

Scalability and flexibility are crucial aspects of Consumer Identity and Access Management (CIAM) due to the following reasons:

1 Handling Growing Consumer Base:

Organisations that deal with consumer-facing applications typically have a large and ever-growing user base. As the number of consumers increases, the CIAM system must be able to accommodate the growing demand for user registrations, logins, and other identity-related activities. A scalable CIAM solution can handle this increased workload without compromising on performance or user experience.

2 Handling Peak Loads:

Consumer applications often experience spikes in user activity during special events, product launches, sales promotions, or seasonal peaks. A scalable CIAM system can efficiently handle these peak loads without causing system failures or slowdowns, ensuring a smooth experience for all users.





A Vision for Tomorrow-IntelliAuth

IntelliAuth stands as a cutting-edge Customer Identity and Access Management (CIAM) platform, uniting a powerful array of features designed to deliver a seamless and secure user experience.

As cyber threats continue to advance, the need for robust security solutions has never been more critical. IntelliAuth addresses this demand by offering Adaptive Multi-Factor Authentication (MFA), ensuring that organisations can defend against emerging risks while providing a user-friendly authentication process. With support for Single Sign-On (SSO) and Customizable Registration pages, IntelliAuth streamlines user onboarding and enhances brand identity. Moreover, Passwordless Authentication and Convenient and Secure password policies elevate security without compromising usability. The platform's Self-service option empowers users to manage their information effortlessly, while Personalization features enable organisations to create tailored customer profiles. In a world where data breaches and unauthorised access are pervasive concerns, IntelliAuth emerges as a necessary and essential IAM solution, safeguarding organisations and their users from potential threats, while facilitating a seamless and personalised digital journey.

