EBOOK

A Guide to Identity Security

ENTRUST

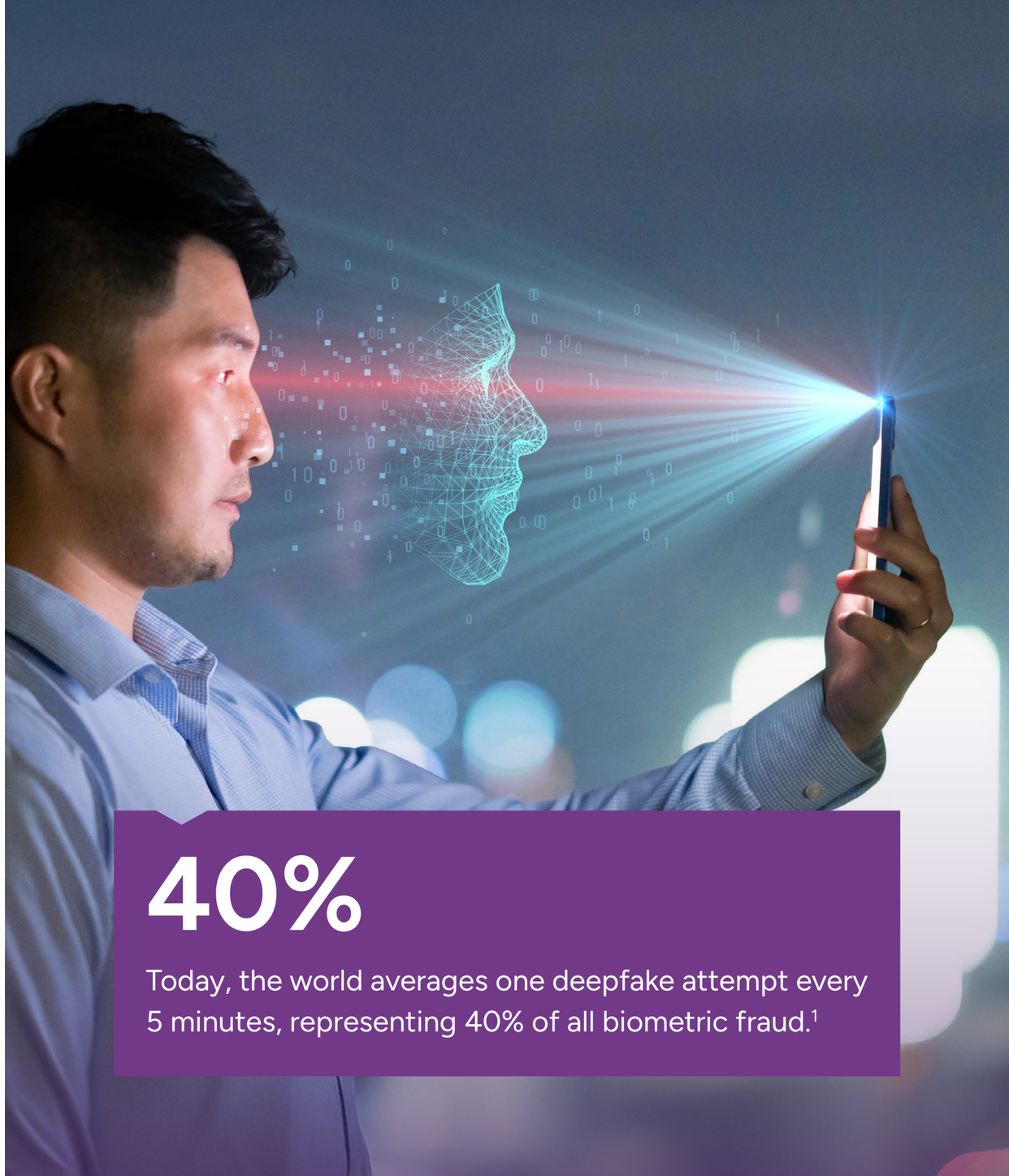
SECURING A WORLD IN MOTION

Introduction

As digital interactions accelerate across industries, verifying who is accessing your systems – and what they can do – has become central to cybersecurity, compliance, and customer trust. Identity is ubiquitous in the modern age.

Yet identity is also under attack. Fraudsters exploit onboarding gaps, hijack credentials, and deploy AI-enabled impersonation at scale. The challenge isn't just keeping pace – it's staying ahead.

This guide explores how modern identity security addresses that challenge. From consumer protection and workforce enablement to digital government, we'll examine the key use cases where identity is both a risk vector and a strategic asset. Whether you're just beginning to modernize your identity strategy or refining a Zero Trust architecture, this ebook will help you chart the path forward – securely and at scale.



40%

Today, the world averages one deepfake attempt every 5 minutes, representing 40% of all biometric fraud.[1]

Protecting the Identity Lifecycle

Identities are no longer confined to physical boundaries. They now encompass everything linked to individuals, organizations, or entities online – from usernames and passwords to biometrics, digital certificates, and online behavior. As the scope of identity grows, so do the challenges of securing it.

Identity-based threats, such as account takeovers and AI-powered deepfakes, are on the rise. Deepfakes alone surged by 3,000% between 2022 and 2023.[2] Today, the world averages one deepfake attempt every 5 minutes, representing 40% of all biometric fraud.[1]

Given these risks, organizations need robust security across the identity journey. This includes:

Onboarding

The first line of defense is critical, yet highly vulnerable. Fraudsters can exploit the issuance and verification process using stolen or synthetic information. If not done securely, it opens the door to identity theft, credential stuffing, and damaged trust right from the start.

Daily Access

As individuals use accounts and conduct transactions, the risks of unauthorized access multiply. Attackers can intercept credentials through phishing, session hijacking, or exploiting weak authentication methods. Strong authentication is especially critical during high-risk moments, like transferring large sums or signing confidential documents.

Upselling

Expanding customer relationships, such as offering credit cards, loans, or new services, creates fresh opportunities for fraud. Without consistent identity verification, these high-value touchpoints can become entryways for bad actors.

Ongoing Safety

The challenge of maintaining security doesn't end after the initial setup or each session. Continuous monitoring is essential, yet the complexity of managing evolving threats, complying with regulations, and ensuring real-time responsiveness can overwhelm many organizations. Without adaptive security protocols, there's a heightened risk of data breaches, regulatory penalties, and costly fraud losses.

As threats evolve, organizations must stay ahead with proactive measures that mitigate risk at each stage of the process. Only through robust, AI-driven identity security can they ensure only the right users access the right resources at the right time.

Consumer Identity

Consumer identity is core to the digital marketplace. Whether banking, shopping, or accessing financial services, customers expect secure transactions every step of the way.

Yet account takeovers were reported to affect about 77 million people in the U.S. in 2023.[3] Victims lost an average of $180, and 40% also experienced broader identity theft.

At the same time, people want instant access without delays or roadblocks. That makes identity security a dual challenge: Keep fraud out without frustrating legitimate customers.

Technologies such as identity verification, multi-factor authentication (MFA), and risk-based analysis are essential to meeting this challenge. Together, they confirm user identities in real time, detect suspicious behavior, and adapt security protocols based on the risk of each interaction. These tools not only safeguard consumers but also enable tangible business advantages.

Benefits of Consumer Identity Security

Prevent Fraud Before it Happens
Establish trusted identities using AI-powered document and biometric verification to stop bad actors at the gate.

Boost Acquisition and Lifetime Value
Verify legitimacy with high assurance users at sign-up, then reuse trusted biometrics across the customer lifecycle to deepen engagement.

Stay Compliant, Globally and Locally
Help meet evolving KYC and AML regulations with flexible, audit-ready identity verification and digital signing tools.

Accelerate Growth With a Unified Platform
Entrust's no-code, orchestrated workflows let you scale identity security without slowing down your go-to-market. Strong identity security doesn't just protect consumers – it powers your business.

Citizen Identity

As governments digitalize services, secure citizen identity is a key enabler for the future. From accessing benefits to filing taxes or voting online, people must prove who they are with speed and certainty – but thus far, that hasn't been the case.

In our survey, 67% of citizens cited long wait times as a top frustration when dealing with public services.[4] More concerning, only 24% rated their trust in the government to protect their data at 9 or higher on a 10-point scale.

This trust gap underscores the need for transformation – not only in how governments deliver services but also in how they manage identity. Digital IDs, mobile credentials, and secure citizen portals can provide that foundation. By combining solutions like biometric verification, AI-powered authentication, and digital signing, public agencies can create fast, secure, and transparent access to essential services. business advantages. These tools not only safeguard consumers but also enable tangible business advantages.

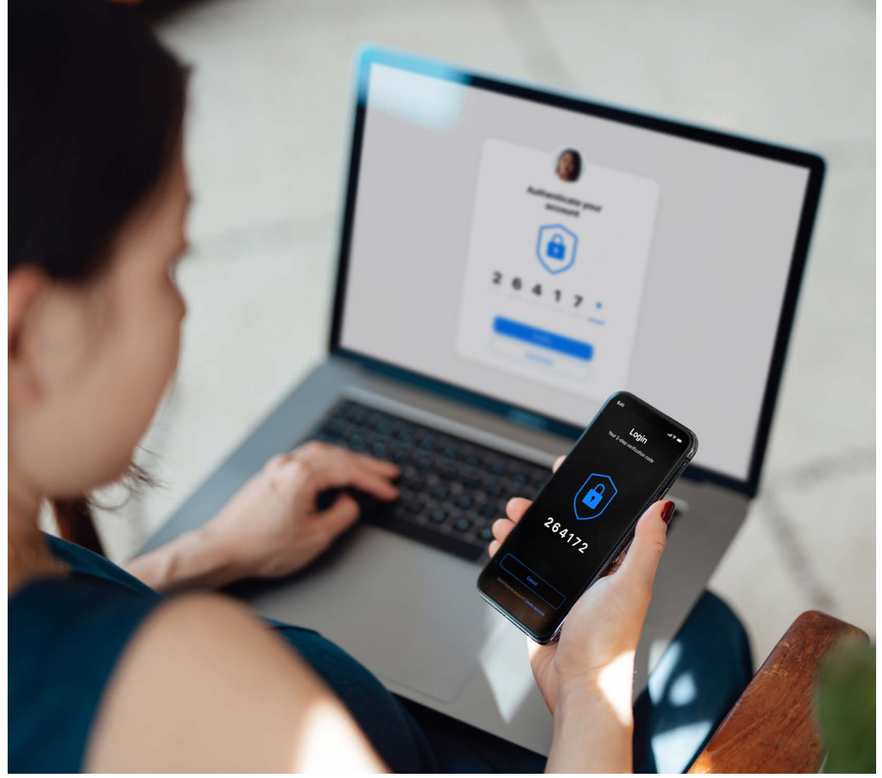
Why Is Strong Identity Security Key to Digital Government?

Seamless, verified citizen identities allow governments to embrace:

- Faster, more efficient service delivery through digital onboarding and authentication
- Fraud mitigation against impersonation, document forgery, and synthetic identity attacks
- Greater transparency and control for citizens over their data
- Compliance-ready infrastructure that supports scale and interoperability
- Streamlined cross-border movement with digital travel credentials and pre-verified identity

Most importantly, strong security ensures that citizens can access the resources they need with the confidence that they're protected from unauthorized access and fraud.

Workforce Identity



Employees, contractors, and third parties are all potential gateways to critical systems. With hybrid work and SaaS sprawl increasing, organizations must manage access across more environments, devices, and applications than ever before, without creating complexity that slows down productivity.

Robust identity security, with identity and access management (IAM), empowers organizations to secure the workforce without compromising efficiency. Solutions like advanced biometric verification, role-based access controls (RBAC), and adaptive MFA ensure users can quickly access only what they're authorized to – no more, no less.

With a comprehensive portfolio of technologies, you can embrace the benefits of strong workforce identity protection:

Zero Trust Readiness
Build a Zero Trust foundation by enforcing least-privilege access and reducing lateral movement.

Operational Resilience
Protect employee credentials and high-value data from phishing, deepfakes, and insider threats.

Frictionless Productivity
Enable fast, secure logins across devices and locations with passwordless options and single sign-on (SSO).

Simplified Compliance
Automate user lifecycle management and access auditing across hybrid IT environments.

Rapid Response:
Detect fraud signals quickly to mitigate threats before the damage is done.

Security shouldn't slow work down. With the right identity framework, it doesn't have to.

Key Components of a Robust Identity Security Strategy

Cybercriminals don't target just one point of access – they probe every phase of the identity lifecycle. A robust identity security strategy must reflect that complexity, combining layered technologies that verify, authenticate, and monitor identities at scale.

The ideal approach is built on an integrated stack of capabilities that adapt to evolving risks and business needs:

Identity Verification (IDV)

Establish trust from day one using document verification, biometric checks, and AI-driven signal analysis to validate users in real time. A recent study found that organizations that invested in IDV solutions reported savings averaging $8 million.[5]

Identity and Access Management

Control access to specific resources with tools like RBAC, adaptive and risk-based MFA, and single sign-on – each essential for enforcing Zero Trust policies.

Digital Signing

Protect the integrity of digital transactions and documents with legally binding, cryptographically secure electronic signatures and seals.

Identity Security Orchestration

Managing your identity experiences should be simple, and the rise of no-code journey time orchestration is making it easier than ever to build identity security experiences at scale. For example, Entrust's orchestration layer connects verification, authentication, and lifecycle management into a seamless user journey.

Strong identity security isn't about isolated tools. It's about how they work together to deliver secure, scalable, and user-friendly access. With the right bundle of solutions, you can protect all types of identities from day one and beyond.

Balancing Security and Customer Experience

Modern users expect more than just speed – they expect confidence. If an application feels clunky or untrustworthy, they'll walk away. In fact, research shows that up to 70% of potential customers abandon an application if it's overly complex or lacks perceived security.[6] For businesses, that's a significant loss of revenue.

Security and convenience are often seen as trade-offs, but they don't have to be. With today's tools, organizations can enhance protection while reducing friction at every interaction.

Entrust addresses this challenge with AI-driven identity security that learns and adapts in real time. By analyzing behavioral signals, device data, and contextual risk factors, these systems detect threats without interrupting the experience for legitimate customers.

70%

of potential customers abandon an application if it's overly complex or lacks perceived security.[6]

Key Advantages of AI-Enhanced Identity Security

Frictionless Onboarding
Automate ID checks and authentication for faster, more intuitive account creation.

Continuous Protection
Detect anomalies across sessions without slowing down access.

Smarter Decisions
Dynamically adjust security based on risk and tighten controls only when necessary.

Improved Conversions
Reduce drop-off by creating a safer, smoother path from first click to account creation. AI turns identity security into a competitive edge that protects the brand and the customer experience simultaneously.

Secure Your Digital Future With Entrust

Identity is at the center of today's digital world, and securing it is non-negotiable. Whether protecting consumers, enabling a productive workforce, or modernizing public services, security is the connective tissue that enables trust, resilience, and growth.

From IDV and IAM to digital signing and more, Entrust brings decades of experience and expertise to our identity security portfolio. With these capabilities, organizations can:

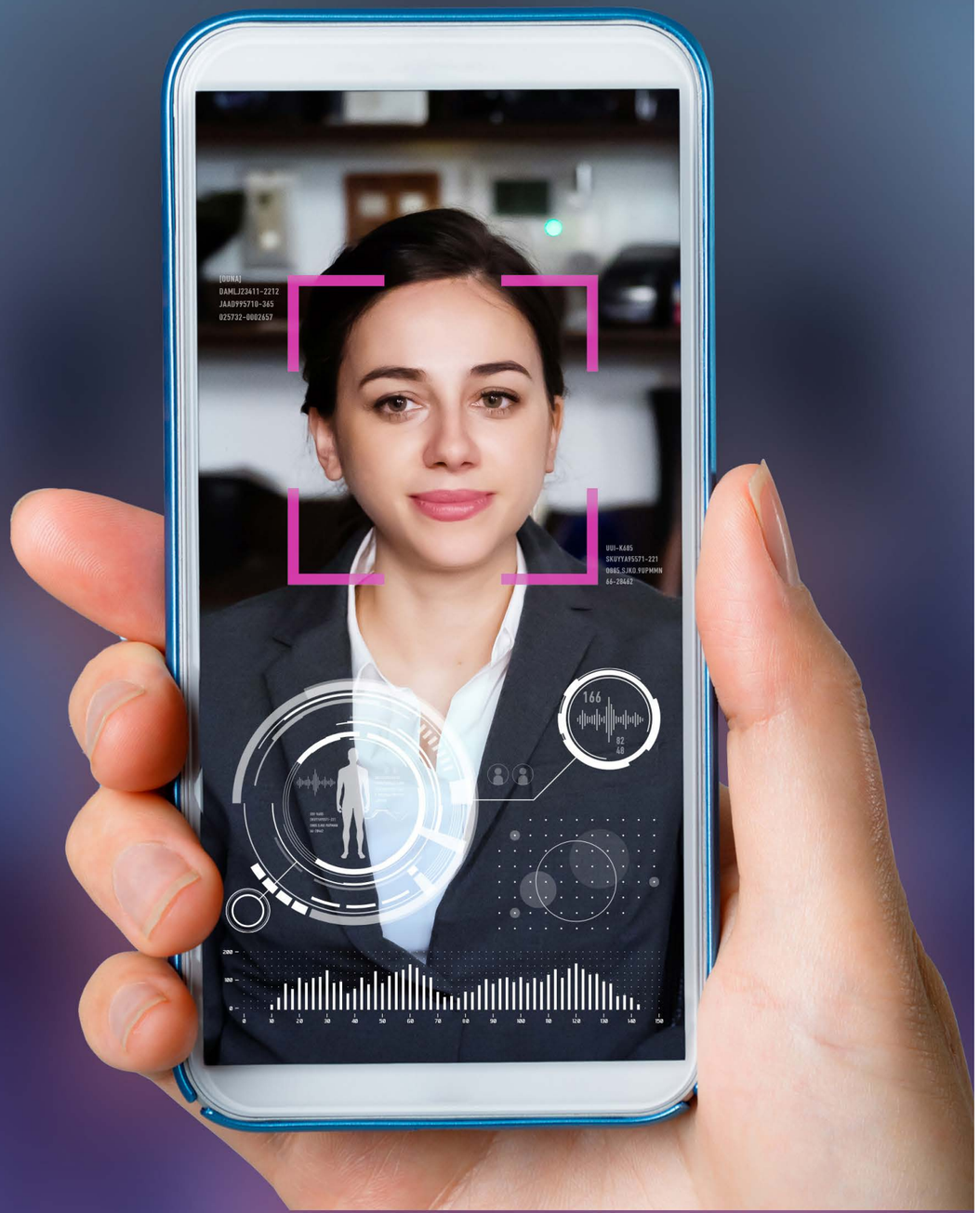
- Deliver seamless and secure access to users across all channels
- Prevent fraud, impersonation, and credential compromise in real time
- Maintain compliance with evolving global standards

Scale securely into digital transformation and Zero Trust initiatives Entrust doesn't just secure identities – we empower your organization to grow with confidence. We process millions of identity verifications annually, helping save an estimated $5.5 billion in fraud losses globally.[1]

Ready to get started?

Contact our team and learn how we can help you build a more secure digital future.

Get in Touch



Sources

1. https://www.entrust.com/resources/reports/identity-fraud-report
2. https://www.entrust.com/sites/default/files/documentation/reports/entrust-fraud-report.pdf
3. https://www.security.org/digital-safety/account-takeover-annual-report/
4. https://www.entrust.com/blog/2024/12/the-role-of-citizen-experience-and-identity-security-in-accelerating-digital-government
5. https://www.entrust.com/company/newsroom/identity-fraud-costs-organizations-an-average-of-7-million-annually-says-new-research-from-docusign-and-entrust
6. https://baymard.com/lists/cart-abandonment-rate

ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

ENTRUST

SECURING A WORLD IN MOTION