ENTRUST

Verifying User Identities in the Era of Deepfakes and Phishing

Combining AI-driven biometrics verification with risk-adaptive MFA helps fight deepfakes, phishing, account takeover attacks, and more

CHALLENGE

The rise of artificial intelligence (AI) brings a new risk to traditional identity and access management

As physical and digital credentials merge, identity has become central to security. AI-driven threats, deepfakes, synthetic identities, and ransomware gangs are driving a rising need for confidence in the identities of the people seeking to connect, access, and transact.

Your organization needs options to authenticate and authorize users in a digital era where no person or thing can be trusted by default anymore.

SOLUTION

Next-level identification and authentication for high assurance transactions

FIDO2 keys, passkeys, and certificate-based authentication are phishing-resistant multi-factor authentication (MFA) mechanisms that you can use to enable secure authentication for your users. These should be combined with a risk-based strategy focused on behavior analysis with biometrics verification as step-up for both onboarding and authentication.

BENEFITS

- Fight phishing and fraud with an identity-centric security solution
- Leverage AI techniques to detect deepfakes, ensure accuracy, and enhance client verification
- Safeguard user identity data while maintaining a good user experience
- Follow compliance best practices by aligning with regulatory standards when implementing Zero Trust or preparing for post-quantum

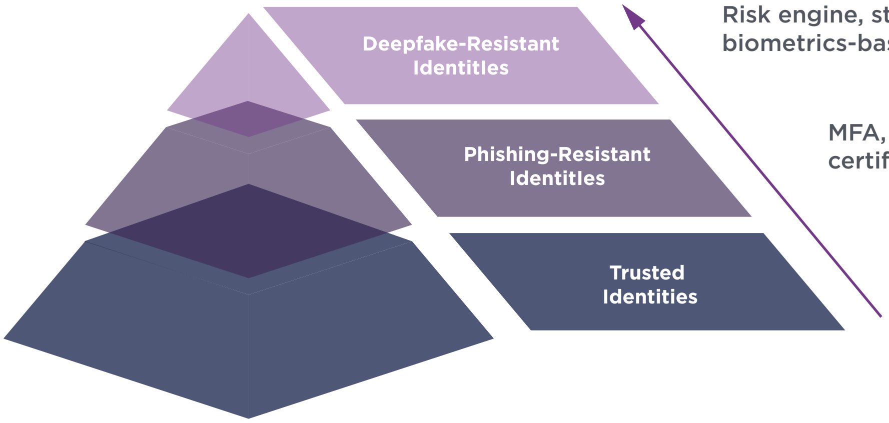
Learn more about our user-centric Zero Trust solutions at entrust.com

Enhancing Biometric-Based Identities

Your user-centric security strategy starts with a layered approach for identification and authentication

Identity is the new perimeter for digital security, and it spans beyond machines and devices: Humans are the most complex thing to verify and authenticate. Our **2024 Identity Fraud Report** reveals that in 2023, there was an 18% increase in digital forgeries over the 2022 report – and roughly 5x more digital forgeries compared to 2021.

AI-driven biometrics verification can help you stay ahead of rapidly evolving impersonation fraud risks, but it can only be as good as your baseline identity management practices are.



Risk engine, step-up authentication, biometrics-based identity verification

MFA, single sign-on, passwordless authentication, certificate-based authentication

User onboarding, access management orchestration

The user identity management pyramid: The most advanced practices still require solid foundations

THE ENTRUST DIFFERENCE

Top-to-Bottom Integration

Entrust is the only provider that can integrate top-to-bottom identity verification (IDV), public key infrastructure (PKI), and identity and access management (IAM) solutions to enhance fraud prevention, reduce manual intervention, and improve user experience.

With the combined power of our solutions, you can:

- **Securely and efficiently authenticate users and validate their identities** in real time to protect against fraud, phishing, and other account takeover (ATO) attacks
- **Seamlessly deploy IDV with ID and biometric checks as step-up authentication** for employees or customers attempting a privileged action, such as a high-value transaction or being issued a passkey or phishing-resistant token
- **Help prevent lateral movement in the event of a breach** by incorporating AI-driven facial biometrics and the IDV process enabled by risk-based adaptive authentication to enforce a higher level of assurance

Learn more about our user-centric Zero Trust solutions at entrust.com

Enhancing Biometric-Based Identities

USE CASES

Identity and authentication use cases

Digital Onboarding: Offer users “anytime, anywhere” onboarding to increase engagement with your organization without compromising on security and trust.

Identity Verification with AI-Driven Biometric Checks: Fight impersonation fraud and build trust using a flexible, end-to-end identity verification platform that orchestrates document and biometric verification, trusted data sources, and fraud-detection signals.

Access Management: Secure access to apps, networks, and devices for all your users. Automate user and app provisioning and ensure seamless transactions while enhancing security and reducing operational costs.

Single Sign-On (SSO): Users can access all applications after authenticating once instead of re-authenticating with different credentials for every unique cloud or on-prem application they need to access.

Passwordless Experience: Our unique passwordless MFA authenticators include high assurance, PKI-based mobile smart credential login; FIDO2 keys; and passkeys (FIDO2 multi-device credentials).

Certificate-Based Authentication (CBA): By ensuring that both the user and device are verified and authenticated using digital certificates, you can provide users with secure and seamless access to resources – with the highest assurance identity that can defend against remote ATO attacks.

Risk-Based Authentication (RBA): Prevent ATO attacks and secure high-value transactions with configurable policies allowing you to evaluate the risk of a user based on contextual data (location, time of day, etc.) and risk inputs that assess behavioral biometrics and look for indicators of compromise (IOCs) based on various threat intelligence feeds.

Biometrics-Based Step-Up Authentication: Deploy IDV with ID and biometric checks as step-up authentication for employees or customers attempting a privileged action, such as a high-value transaction or being issued a passkey or phishing-resistant token.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223