Phishing-Resistant Identities

Protect against account takeover (ATO) attacks with secure high-assurance identities.

Security challenges organizations are faced with

Cyberattacks continue to increase in both number and sophistication, with attackers successfully breaching the defenses of many organizations. Services such as phishing-as-a-service and generative AI that helps attackers build realistic phishing emails, websites, and malicious code has lowered the bar for entry for bad actors. Identity continues to be the largest attack vector, with compromised credentials and phishing being the leading causes of breaches.

The traditional password adds to the poor user experience and is easily compromised. Even traditional multi-factor authentication (MFA) such as SMS one-time password (OTP) and push authentication are easily bypassed by attackers. Once an attacker gains control of a user's account, they can move laterally within an organization's network and gain persistence, often going undetected for days.

You need to secure your users with phishing-resistant authentication and protect against ATO attacks.

Phishing-resistant authentication

With traditional MFA broken, organizations need phishing-resistant options to authenticate and authorize their users.

FIDO2 keys, passkeys, and certificate-based authentication are a few phishing-resistant MFA authentication mechanisms that organizations can use to enable secure authentication for their users.

Passkeys

Passkeys are cryptographic key pairs used to authenticate users into various applications. A public key is stored on the application server and a private key is stored on the user's device. Passkeys use Bluetooth to communicate between the user's phone (FIDO authenticator) and the device from which the user is trying to authenticate. Bluetooth requires physical proximity, providing a phishing-resistant way to leverage the user's phone during authentication.

Learn more about our Zero Trust solutions at entrust.com

Phishing-Resistant Identities

FIDO2 keys
FIDO tokens are physical keys like USBs, which are plugged into the desktop. In some of them, there is also a place for scanning your fingerprint as a second factor of authentication. The key contains encrypted information that authenticates user identity when plugged in. The user is automatically logged into the system as well as gains access to all applications in a single session.

Certificate-based authentication (CBA)
Certificate-based authentication (CBA) provides the highest assurance with respect to security and the best user experience in terms of passwordless login capabilities. With CBA, you can provision a digital certificate onto the user's phone (mobile smart credential), transforming it into their trusted workplace identity.

With Bluetooth/NFC capabilities, as the user walks toward the workstation, a connection is established between the user's phone (where the smart credential resides) and the desktop.

There can be two options to passwordlessly log in from here – either the system gets unlocked when the user is asked to provide their fingerprint/Face ID on the smartphone, or the desktop prompts the user to enter a PIN to login. Both ways do not require any passwords. In the same session, the user can also connect securely with a remote desktop and SSH.

In addition to issuing a certificate for a user, assigning certificates to the devices used by a user ensures a higher level of security when authenticating and accessing resources. This ensures that not only is the user verified and authorized but also the device from which they are accessing a resource is verified and authorized, ensuring a high level of assurance.

Risk-based adaptive authentication (RBA)
Adding risk assessment to the authentication process is a key requirement of any mature Zero Trust framework and helps provide a greater level of security while also allowing for a better user experience, by only adding friction in the authentication process when required.

Evaluating the risk score with contextual information such as time-of-day/day-of-week login, travel velocity, IP address, and behavioral biometrics allows for a more accurate assessment of the validity of an authentication request and protection against fraud. If risk levels exceed a pre-defined threshold, challenge the user to authenticate via a configured 2nd MFA authenticator or block access in case of extremely high risk scores. RBA is also useful in ensuring high-value transactions are secured with an additional layer of security.

Single sign-on
Combining CBA and RBA with single sign-on allows for seamless but secure access to applications and services once authenticated. SSO helps protect against password fatigue and reuse, combined with orchestration and automation of user and app provisioning, which streamlines the onboarding and offboarding process by ensuring admins can easily activate or deactivate users based on their role and permissions.

Phishing-Resistant Identities

Device identity
With the number of devices easily exceeding the number of users and the explosion of the IoT space, ensuring organizations have visibility into which devices users are using to connect into their network is critical to further securing access to critical resources and data.

Managing device identities through a centralized, easy-to-use certificate lifecycle management tool helps with better control, compliance, and governance.

Establish a mature Zero Trust strategy that starts with identity

Provision and enable certificate-based authentication across your users and devices through a single platform. Ensure high-assurance identities by requiring that both users and devices are verified and authenticated through the use of CBA. Entrust mobile smart credentials combine CBA with Bluetooth proximity detection to enable seamless passwordless login to your laptop/desktop and to all applications with SSO.

Entrust RBA allows for admins to configure the risk inputs by assigning weights to customize the risk analysis engine for a specific use case and user group.

The Entrust phishing-resistant Identity solution offers you a complete identity and access management platform and a comprehensive certificate lifecycle management platform to implement high-assurance certificate-based authentication for your users and devices.

BENEFITS

- Enable phishing-resistant authentication
- Defend against remote account takeover (ATO) attacks
- Secure hybrid and remote work
- Reduce the attack surface
- Access a broad and integrated ecosystem

Learn more about our Zero Trust solutions at entrust.com

Phishing-Resistant Identities

Features

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

Risk-Based Adaptive Step-Up Authentication (RBA): Find the right balance between security and user convenience. Configurable policies allow you to evaluate the risk of a user based on contextual data such as location, time of day, etc., so you're not unnecessarily adding friction to your user experience. Prevent fraud and secure high-value transactions with risk inputs that assess behavioral biometrics and looks for indicators of compromise (IOCs) based on various threat intelligence feeds.

Robust and Automated Certificate Lifecycle Management (CLM): Our CLM provides full visibility into your entire certificate estate across environments and centralizes control. It helps to ensure strong issuance protection for your certificates.

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

Passwordless: Passwordless MFA options eliminate the use of passwords as one of the factors during authentication. Entrust offers unique MFA authenticators such as high assurance PKI-based mobile smart credential login, FIDO2 keys, and passkeys (FIDO2 multi-device credentials).

Access Management: Secure access to apps, networks, and devices for all of your users. Automate user and app provisioning through the use of orchestration and ensure seamless onboarding and offboarding experiences while enhancing security and reducing operational costs.

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