Identity-Centric Solutions: the Foundation of Enterprise Security

From enhanced biometric identity verification to protecting critical infrastructure and securing data, a strong security practice starts with a strong, scalable identity-centric foundation.

Challenge

The traditional digital security perimeter has disappeared due to a multitude of factors, including the uptick in cloud adoption, the ever-increasing number of machines, and remote workforces. With everyone working from anywhere on multiple devices, the attack surface has expanded, making organizations more vulnerable to risks.

In response, organizations are looking for new ways to approach their digital security and ensure they are appropriately mitigating evolving threats and limiting their attack surface. Fortunately, we're also seeing the emergence of many frameworks – including Zero Trust – that help organizations establish a set of controls and policies to build a layered approach to security to mitigate and reduce cyber risk.

KEY 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
- Future-proof your security investments

KEY FEATURES

- Certificate-based authentication
- Risk-based adaptive step-up authentication
- Automated certificate lifecycle management
- End-to-end encryption
- Multi-cloud ready
- Compliance management
- Post-quantum-ready solutions
- Built-in crypto-agility and certificate authority (CA) resilience
- Public and private PKI
- Centralized visibility and control of digital certificates

Learn more about our Zero Trust solutions at entrust.com

Identity-Centric Solutions

Solution Overview

Entrust uniquely helps organizations establish a strong and resilient security practice with a comprehensive portfolio of solutions that help secure identities, devices, applications, networks, and data.

Verified identities

We help organizations take an identity-first approach to security by establishing secure identities with deepfake- and phishing-resistant authentication with multiple authentication options such as passwordless and certificate-based authentication and biometrics-based authentication for the highest level of assurance.

In addition to providing public and private certificates to authenticate, encrypt, and sign, we provide tools to centralize the visibility and control of your certificates, including automation throughout their entire lifecycle.

Strong encryption

Data security solutions from Entrust enable strong encryption to secure data in-transit, at-rest, and in-use across public and private cloud environments.

PQ-ready

Entrust is at the forefront of post-quantum (PQ) cryptography, building PQ-ready digital security solutions to future-proof your organization and its data from the

Learn more about our Zero Trust solutions at entrust.com

Identity-Centric Solutions

Enhance Identity Verification

Identity continues to be the largest attack vector, with phishing and compromised credentials being the leading causes of a breach. Studies suggest that 90% of breaches are due to some form of phishing.[1] And in 2023 we saw a 3,000% increase in deepfake attempts during remote authentication.[2]

An identity-first approach to security is a critical best practice for organizations to ensure only verified and authorized users and devices can access resources, reducing the risk of a breach.

High assurance identities

Entrust enables high assurance identity with certificate-based authentication (CBA), biometrics-based authentication, and risk-based adaptive step-up authentication (RBA) to ensure only verified and authorized users have access to resources. This allows for high assurance deepfake- and phishing-resistant authentication as both the user and device need to be verified and trusted in order to gain access to resources.

RBA allows organizations to provide a balance between introducing friction when risk levels are high and a seamless user experience when risk levels are low.

Step-up authentication using AI/ML-driven biometric checks provides the highest level of protection against account takeover attacks.

Once identities have been verified and authenticated, you can use secure access management and single sign-on capabilities to ensure only authorized and verified users have access to critical resources within your organization. Establishing device identities through a centralized, easy-to-manage certificate lifecycle management platform helps ensure only authorized and verified devices have access to your network and resources.

Entrust solutions for enhancing identity verification:

- Entrust Identity as a Service (IDaaS)
- Entrust PKI as a Service (PKIaaS)
- Onfido Real Identity Platform

Protect Critical Infrastructure

Sensitive and confidential data moves over public and private networks constantly, whether it's a user logging on to an online portal or sending an email, or machine-to-machine communication that occurs without any human intervention.

All these connections and endpoints need to be secured. And the most resilient, scalable, and secure way to do that is using digital certificates issued by a certificate authority (CA) to verify identities and grant access.

1. CyberTalk.org: Top 15 phishing attack statistics (and they might scare you)
2. Onfido: 2024 Identity Fraud Report

Learn more about our Zero Trust solutions at entrust.com

Identity-Centric Solutions

Digital certificates – both public and private – deliver three key outcomes:

- Strong device identity – from IoT and mobile devices to servers and virtual machines
- Encryption for web servers, networks, and other systems
- Enforced access control to micro-segmented networks, applications, and systems

More machine identities means a greater need for certificate lifecycle management

With the increasing number of devices and machines over recent years, there's also been a significant growth in the number of certificates organizations are issuing and managing. Plus, additional management challenges and complexities often come with certain use cases, such as the short-life certificates we see for public TLS/SSL and IoT.

Certificate lifecycle management becomes critical to ensure you have strong issuance protection for your certificates and for mitigating common risks such as a rogue certificate being issued and given too much access or privilege. And the more certificates an organization has, the greater the need for management automation tools.

Entrust solutions for protecting critical infrastructure:

- Entrust TLS/SSL Certificates
- Entrust PKI as a Service (PKIaaS)
- Certificate Lifecycle Management (Certificate Hub and Entrust Certificate Services)

Secure Your Data

With attackers having more tools at their disposal than ever before, it's no longer a matter of "if," but rather "when" an organization gets breached. In order to secure your critical data, encryption and cryptographic key management are essential.

You can enable end-to-end encryption for all data at-rest, in-transit, and in-use with secure data solutions from Entrust. We provide the components needed to secure the keys and secrets used by your organization to protect your sensitive data.

By providing data encryption with a FIPS-certified root of trust for cryptographic key generation, our solutions deliver comprehensive keys and secrets lifecycle management. And with innovative centralized compliance management and decentralized key storage, you're in control to ensure confidentiality, integrity, and access to your critical data – all while facilitatating compliance with security regulations.

Entrust solutions for data protection:

- Entrust nShield Hardware Security Modules (HSMs)
- Entrust nShield as a Service
- Entrust KeyControl

Learn more about our Zero Trust solutions at entrust.com

Identity-Centric Solutions

Features

Certificate-Based Authentication: 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.

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 verifications, trusted data sources, and fraud detection signals.

Risk-Based Adaptive Step-Up Authentication: Configurable policies allow you to evaluate the risk of a user based on contextual data (location, time of day, etc.). This helps you find the right balance between security and end-user convenience because you're not unnecessarily adding friction to the user experience. Behavioral biometrics and threat intelligence helps prevent fraud and secure high-value transactions.

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.

Comprehensive Keys and Secrets Management: Centralized visibility and compliance management with decentralized key storage puts you in control to ensure the confidentiality and integrity of and access to your critical data.

Multi-Cloud Ready: Support bring-your-own-key (BYOK) and hold-your-own-key (HYOK) capabilities to give your organization more control over your sensitive data stored and processed by cloud service providers across multi-cloud deployments.

Post-Quantum Ready: Our solutions have built-in crypto-agility and are PQ-ready. Begin testing PQ-safe algorithms within your applications and systems, and future-proof your organization from the post-quantum threat.

Public and Private Digital Certificates: Digital certificates are the most scalable, resilient, and secure way to deliver strong device identity, encryption, and micro-segmenting. Entrust's digital certificates also help you follow best practices and governance with security controls via PKI – including up-to-date certificate policy and operational procedures, as well as issuance, revocation, and change controls.

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