# Zero Trust Foundations

## 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.

**Risk-Based Adaptive Step-Up Authentication:** Configurable policies allow you to evaluate the risk of a user based on contextual data such as 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. Prevent fraud and secure high-value transactions with behavioral biometrics and threat intelligence.

**Robust and Automated Certificate Lifecycle Management (CLM):** From providing full visibility into your full certificate estate across environments to centralizing control, CLM and automation are important components of your overall Zero Trust strategy by making sure you have 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:** Manage risk with an enterprise-wide approach to discovering, managing, protecting, and auditing keys, certificates, secrets, and cryptographic assets – while ensuring a crypto-agile approach within your people, processes, and technology. 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.


For more information

**888.690.2424**
**+1 952 933 1223**
**sales@entrust.com**
**entrust.com**


### ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
**entrust.com**




ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
**HSMinfo@entrust.com**



# Zero Trust Foundations

**Start your Zero Trust journey with phishing-resistant identities, secure connections, and secure data.**

## Challenge

The traditional digital security perimeter has disappeared due to factors such as the uptick in cloud adoption and remote workforces. With everyone working from anywhere on multiple devices, the attack surface has expanded, making organizations more vulnerable to risks.

Zero Trust has emerged as a framework of choice that can 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 Zero Trust 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 CA resilience
- Public and private PKI
- Centralized visibility and control of digital certificates

**Learn more about our Zero Trust solutions at entrust.com**

# Zero Trust Foundations

## Solution Overview

Entrust uniquely helps organizations establish a strong Zero Trust framework with a comprehensive portfolio of Zero Trust security solutions that helps secure identities, devices, applications, networks, and data.

### Certificate-based authentication

We help organizations take an identity-first approach to security by establishing secure identities with phishing-resistant authentication that includes certificate-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 post-quantum threat.

**Learn more about our Zero Trust solutions at entrust.com**

# Zero Trust Foundations

## Phishing-Resistant Identities

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 61% involve compromised credentials.[2]

An identity-first approach to security is critical for a successful Zero Trust implementation 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) and risk-based adaptive step-up authentication (RBA) to ensure only verified and authorized users have access to resources. This allows for high assurance 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 required and a seamless user experience when risk levels are low.

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 enabling phishing-resistant identities

- Entrust Identity as a Service (IDaaS)
- Entrust PKI as a Service (PKIaaS)

## Secure Connections

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.

### Digital certificates – both public and private – deliver three key outcomes needed for Zero Trust:

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

1. CyberTalk.org: Top 15 phishing attack statistics (and they might scare you)

2. CPO Magazine: Why Does Every Hack Involve Stolen Credentials? Because It Works Every Time, August 2022.

# Zero Trust Foundations

## Secure Connections (continued)

### 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 short-life certificates for public TLS/SSL and IoT.

In order to properly enforce your Zero Trust strategy, 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 enabling secure connections

- Entrust TLS/SSL Certificates
- Entrust PKI as a Service (PKIaaS)

## Secure 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 can support your Zero Trust journey by providing 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 incontrol to ensure confidentiality, integrity, and access to your critical data – all while facilitatating compliance with security regulations.

### Entrust solutions for enabling secure data

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