TRUSTERA

Zero-Trust Cybersecurity & Unified Identity as a Service (UIaaS)

Hardware-Anchored Identity

Zero Trust Architecture

Unified Access Platform

One Card · Every System

PRODUCT OVERVIEW · TEAM EDUCATION GUIDE

Inteveo, LLC · March 2026 · Confidential

CLOUD SOLUTIONS inteveo

Trustera

What Is Trustera?

Trustera is a fully integrated, hardware-anchored cybersecurity platform that eliminates passwords, fragmented tools, and manual access management — replacing them with a single, policy-driven identity that works across every system, application, and door in an organization.

01 One Platform

Replaces up to 8 separate cybersecurity products with a single unified system — identity, endpoint protection, network security, access control, and compliance in one.

02 Hardware-Anchored

Unlike software-only solutions, Trustera's root of trust is a physical hardware module (Bluetooth/NFC HSM). It cannot be spoofed, phished, or bypassed remotely.

03 Zero Passwords

Users never enter usernames, passwords, MFA codes, or SSO prompts. A Trustera card — tapped once — authenticates the user to every authorized system automatically.

04 Policy-Driven

Administrators define who can access what, when, and from where. Role-based policies enforce instantly across the entire environment — onboard and offboard in seconds.

THE PROBLEM

Why Today's Cybersecurity Is Broken

3,322
U.S. Breaches in 2025
Record high — up 14% YoY

$10.2M
Avg. Breach Cost
Double the global average

83%
Multi-Breach Orgs
Hit more than once

1-in-6
AI-Driven Attacks
Now using AI to breach

WHY LEGACY SOLUTIONS FAIL

- Software-only — no hardware root of trust, easily bypassed
- Fragmented tools create gaps across identity, IoT, and cloud
- Passwords and credentials are the #1 breach entry point
- Reactive architecture — breaches discovered after damage done
- Legacy codebases carry decades of unpatched vulnerabilities
- Distributed environments (edge, cloud, hybrid) create blind spots

ACTIVE NATION-STATE THREATS

CHINA	Salt Typhoon — breached 9 U.S. telecoms, accessed senior officials' communications
CHINA	Volt Typhoon — pre-positioned 'digital booby traps' in utilities, transport & manufacturing
IRAN	CyberAv3ngers/APT33 — targeting U.S. water systems, power grids, hospitals, and ports
RUSSIA	Persistent espionage & destructive campaigns against NATO-aligned critical infrastructure
N. KOR	Lazarus Group — ongoing cryptocurrency theft and financial system targeting

SECTION 02 · PLATFORM ARCHITECTURE

How Trustera Works

A three-layer platform built on hardware trust — no software-only shortcuts.

Hardware-Anchored Identity — Cryptographic Root of Trust

THE PHYSICAL DEVICE



Hardware Security Module (HSM)
Bluetooth/NFC + Tamper-Proof Enclosure

The device is immune to:

- ✕ Remote hacking — no network exposure
- ✕ Phishing — no credentials transmitted
- ✕ Man-in-the-middle attacks
- ✕ Credential theft — keys never leave device
- ✕ Deepfake authentication attempts

HOW IT WORKS

When the card is issued, a unique cryptographic key pair is generated inside the device. The private key NEVER leaves the hardware.

01 PRIVATE KEY
Locked inside hardware enclosure. Never exported. Never transmitted. Used only to digitally sign authentication requests.

02 PUBLIC KEY
Registered with every system. Used only to verify that a signature came from this specific card. Cannot sign or authenticate.

When authenticating:

1. System requests authentication from the card
2. Card signs the request with its PRIVATE key
3. Card sends the signature (no key sent)
4. System verifies using the PUBLIC key
5. Access granted — cryptographically proven

WHY IT MATTERS

✓ **Zero Passwords**
No secrets are ever entered, transmitted, or stored on shared systems. Passwords cannot be phished, guessed, or brute-forced.

✓ **Cryptographic Certainty**
Every authentication is mathematically verified. The system KNOWS exactly which user made the request because only that card's private key could create the signature.

✓ **Hardware Proof**
Because the private key lives in tamper-proof hardware, the identity is bound to a physical object. You cannot copy or steal the credential.

✓ **Future-Proof**
Cryptographic methods are the same defense used by governments, militaries, and financial institutions. They're proven, audited, and compliant with every framework.

The Three-Layer Trust Model — Core · Edge · Cloud

Every layer works independently and together. There is no single point of failure — trust is enforced at the hardware level, the network edge, and in the cloud simultaneously.

TRUSTERA CORE

Identity, Policy & Orchestration

The brain of the platform. Manages all identity definitions, access policies, and cryptographic operations. Every user identity is hardware-bound and cannot be duplicated or stolen.

- Hardware-anchored identity verification — physical card + cryptographic key pair
- Policy creation, distribution & real-time enforcement across all connected systems
- Cryptographic trust operations — sign, verify, encrypt at the hardware level
- Compliance automation — auto-generates audit logs for CMMC 2.0, NIST, SOC 2

TRUSTERA EDGE

Secure Endpoint & Network Enforcement

The enforcement layer. Every device and network entry point is controlled here. Identity is verified at the hardware level before any access is granted — network or application.

- Real-time identity enforcement at every device and network entry point
- Local processing — low-latency decisioning without cloud dependency
- Hardware-anchored protection against spoofing, man-in-the-middle, and deepfakes
- Encrypted, mutually-authenticated tunnels between every node on the network

TRUSTERA CLOUD

Visibility, Intelligence & Control

The visibility layer. AI-driven analytics detect anomalies across the entire environment. Administrators see everything, manage everything, and respond to threats from one dashboard.

- AI-driven analytics & behavioral anomaly detection across all users and systems
- Unified dashboards — enterprise-wide visibility from one control plane
- Centralized monitoring, reporting & policy update distribution
- Native integration with SIEM, IAM, MDM, and MDR platforms

SECTION 03 · UNIFIED IDENTITY AS A SERVICE

One Card. Every Access.

UIaaS — the card becomes the passport to every system, application, and door.

The Card Is the Credential — For Everything

The Core Concept

Think of a VDI golden image — where a new employee logs into a virtual desktop and every application they need is already installed, configured, and ready. They never have to set up anything.

Trustera does this for identity and access across every system in the organization.

When a new user receives their Trustera card, they are immediately live — every authorized application, every system, every door is accessible by simply presenting the card.

No setup. No IT ticket. No username. No password. No SSO portal. No MFA code. No separate door badge.

The card is cryptographically linked to the user's identity at the hardware level. When presented to any Trustera-enabled system, it instantly validates: who the person is, what they are allowed to access, and whether that access is permitted right now — based on role, time, location, and policy.

01 Workstation Login

Card tap = desktop unlocked. Immediate full access to authorized applications.

02 Network & Cloud Access

Hardware-verified network admission. No VPN. No separate cloud login. Zero Trust enforced.

03 Enterprise Applications

Every SaaS and on-prem app auto-configured. No SSO prompts, no app-specific passwords.

04 Physical Door Security

Same card opens authorized doors and rooms. One credential for physical and digital access.

05 IoT & Operational Systems

Secure access to industrial, medical, and OT systems using the same identity framework.

06 Remote & Mobile Sessions

Zero Trust remote access. Authenticated instantly from any device, any location, globally.

USER EXPERIENCE

A Day in the Life — Before Trustera vs. After Trustera

✗ WITHOUT TRUSTERA (Today's Reality)

STARTING WORK

Enter Windows username + password → wait for MFA push notification → approve MFA app → wait for login

OPENING APPLICATIONS

Navigate to SSO portal → select app → re-authenticate if session expired → enter app password if not SSO-enabled

ACCESSING NETWORK RESOURCES

Launch VPN client → enter VPN credentials → wait for connection → separately authenticate to file server or internal tools

ENTERING SECURE AREAS

Swipe separate physical access badge → unlock workstation again if session locked → re-authenticate to secure systems

NEW EMPLOYEE ONBOARDING

IT creates accounts (AD, email, apps, VPN, physical badge) — 1 to 3 days minimum across systems and vendors

EMPLOYEE OFFBOARDING

IT revokes access system by system — AD, each app, VPN, physical badge — typically 2–5 days. High risk of gaps.

✓ WITH TRUSTERA (The New Reality)

STARTING WORK

Tap card on reader → desktop unlocks immediately. All authorized apps are ready. Zero prompts.

OPENING APPLICATIONS

Every application is already open and authenticated. No portal, no prompts, no separate logins.

ACCESSING NETWORK RESOURCES

Network access is granted automatically via hardware identity. No VPN required. No network credentials.

ENTERING SECURE AREAS

Same Trustera card opens doors. Identity is continuous — no re-authentication when moving between spaces.

NEW EMPLOYEE ONBOARDING

Issue one Trustera card with assigned role. User is live on every system in under 60 seconds.

EMPLOYEE OFFBOARDING

Revoke card. Access removed from every system — applications, network, and doors — simultaneously, instantly.

What Trustera Replaces — One Platform for Everything

The average enterprise runs 8–12 separate security and access products. Trustera consolidates all of them into one platform — eliminating vendor complexity, integration costs, and security gaps.

Active Directory / LDAP

Identity replaced by hardware-anchored UIaaS

SSO Platform (Okta, Azure)

No portal needed — card authenticates directly

MFA / 2FA Applications

Hardware identity is stronger than any 2FA method

VPN Client

Zero Trust network access replaces VPN entirely

Physical Access Badge

Same Trustera card controls doors and systems

Password Manager

No passwords exist in the Trustera model

User Provisioning Tools

Onboarding automated via card issuance and RBAC

Endpoint DLP Agents

Hardware-anchored identity controls data access

WHAT REMAINS

One Trustera Card · One Admin Console · Zero Passwords · Zero Separate Tools · 100% Access Coverage

ORGANIZATIONAL VALUE

What Trustera Does for the Organization

01 Instant Onboarding & Offboarding

New employees are live on every authorized system the moment their card is issued. Departing employees lose all access — applications, network, and physical — the moment their card is revoked. No IT queue. No gaps. Average time: under 60 seconds.

02 Role-Based Access Control (RBAC)

Administrators define access by role — not by individual. Change a user's role and every access permission updates instantly across every system. A contractor gets contractor access; a CISO gets CISO access. Policy is enforced at the hardware level, not software.

03 Dramatic Cost Reduction

Eliminate licensing costs for SSO, MFA, VPN, provisioning tools, and physical access systems. Reduce IT helpdesk load by 60–80% for access-related tickets. Remove the overhead of managing and auditing multiple identity systems.

04 Compliance Automation

CMMC 2.0, NIST 800-53, SOC 2, HIPAA, and FedRAMP requirements are automatically met and documented. Audit logs are generated at every access event — hardware-signed and tamper-proof. Zero manual compliance reporting effort.

05 Breach Resilience

Credential theft is eliminated — there are no credentials to steal. Phishing attacks fail — there is nothing to phish. Man-in-the-middle attacks fail — identity is cryptographically verified at the hardware level. The attack surface is reduced to near zero.

06 Global, Infrastructure-Agnostic Deployment

Trustera works on-premises, in the cloud, or in hybrid environments. It integrates natively with existing enterprise systems — Microsoft, AWS, Google Cloud, Salesforce, and hundreds more — without ripping and replacing existing infrastructure.

Why Trustera Wins — No Comparable Solution Exists Today

Trustera is the only platform that combines hardware-anchored identity, tri-layer Zero Trust enforcement, OT/IoT/SCADA native support, deepfake-resistant authentication, and air-gap capability in a single unified system. Every competitor requires 3–5 separate products to attempt the same coverage.

CAPABILITY	Trustera	Okta	CrowdStrike	Palo Alto	Zscaler	SentinelOne
Hardware-Anchored Identity Root	✓	✗	✗	✗	✗	✗
Tri-Layer Core + Edge + Cloud	✓	◑	◑	◑	◑	◑
OT / IoT / SCADA Native Support	✓	✗	✗	✗	✗	◑
Deepfake-Resistant Authentication	✓	✗	✗	✗	✗	✗
Offline / Air-Gap Capable	✓	✗	✗	✗	✗	✗
Zero Passwords / Zero SSO	✓	✗	✗	✗	✗	✗
Physical + Digital in One Credential	✓	✗	✗	✗	✗	✗
CMMC 2.0 Level 2 Ready (native)	✓	◑	◑	◑	◑	◑

✓ Full capability ◑ Partial / add-on ✗ Not available

Where Trustera Applies — Across Every Sector That Manages Access

01 Enterprise & Financial Services

Banks, investment firms, and insurance companies face the strictest access control requirements — and the highest cost when breached.

- Branch and remote worker secure login
- Zero-trust access to trading and core banking systems
- Automated SOC 2 and PCI-DSS compliance
- Contractor and third-party access control

02 Federal & Defense Contractors

CMMC 2.0 compliance is now mandatory. Trustera is purpose-built for DoD supply chain and federal Zero Trust mandates.

- CMMC Level 2 compliance — hardware root of trust required
- Air-gap and SCIF-ready deployments
- CAC/PIV card integration or replacement
- Contractor clearance-level access control

03 Healthcare & Life Sciences

HIPAA, clinical systems access, and clinician mobility require fast, secure, frictionless authentication across shared workstations.

- Shared workstation fast-switch between clinicians
- EHR and imaging system access without separate login
- HIPAA access logging and audit-readiness
- Medical device and IoT identity management

04 Critical Infrastructure & OT

Power grids, utilities, and industrial systems require identity at the OT/IoT layer — where no conventional cybersecurity product operates.

- SCADA and ICS operator authentication
- Physical + logical combined access for facilities
- Anti-spoofing for operational technology networks
- Offline/air-gap capable for isolated environments

Why the Market Needs Trustera Right Now — The Compliance Mandate

THE REGULATORY PRESSURE

Trump 2026 Cyber Strategy

Issued March 2026 — federal Zero Trust adoption mandated. Procurement budgets allocated NOW. Every federal agency and their supply chain must comply. Contracts at risk without Zero Trust certification.

CMMC 2.0 — Level 2 Active

Defense Industrial Base contractors (300,000+) must pass CMMC Level 2 assessment or lose DoD contracts. Hardware-anchored multi-factor authentication is a core Level 2 requirement. Trustera satisfies this natively.

SEC Cyber Disclosure Rules

Public companies must now disclose material cybersecurity incidents within 4 business days and annually report their cybersecurity risk management processes. Board-level accountability has never been higher.

NIST 800-207 Zero Trust

The definitive federal Zero Trust framework explicitly requires hardware-anchored identity as the foundation of any compliant deployment. Software-only solutions do not meet this standard.

THE MARKET SIZE

$345B

Global Cybersecurity TAM

2026 · 15% CAGR

$98B

North America SAM

All serviceable segments

$45B

Zero Trust + Identity + IAM

Trustera's direct market

$18B+

No Comparable Unified Platform

First-mover category

$1.34B

Trustera Year 4 SOM

2.9% Core · 85 Ent. deals

How to Explain Trustera — Key Talking Points & Analogies

SAY THIS to explain it

One-liner:

"Trustera is one card that replaces every password, badge, and login in your organization."

For IT buyers:

"It's Zero Trust with a hardware root — the identity lives in the card, not the cloud, so it cannot be phished or breached remotely."

For executives:

"Your employees tap a card, everything opens. New hire is live in 60 seconds. Former employee loses all access instantly."

For compliance:

"CMMC 2.0, NIST 800-207, and FedRAMP require hardware-anchored identity. Trustera checks every box natively — no bolt-ons required."

USE THESE analogies

The VDI golden image:

"Like a virtual desktop where everything's already set up — except Trustera does this for your identity across EVERY system."

The passport model:

"Your Trustera card IS your passport. One document, verified by hardware, accepted everywhere the organization operates."

Hotel key card:

"Like a hotel key — it opens your room, the gym, the pool. Trustera's card opens your workstation, your apps, and the server room."

Physical locks:

"Imagine if every lock in your office used the same key — but that key also logged you into Salesforce and your email."

HANDLE these objections

"We already have Okta / Azure AD":

Okta is software-only SSO. It doesn't anchor identity in hardware, doesn't control physical access, and still requires passwords somewhere in the chain.

"What if the card is lost?":

Admin revokes immediately from console. Access is gone in seconds — faster and more complete than revoking software credentials across 10 systems.

"Is it hard to deploy?":

No rip-and-replace. Trustera integrates into your existing environment. EcoLink handles the API connections — deployment is measured in days, not months.

"What about remote workers?":

Same experience. Remote Zero Trust access is handled identically — hardware-verified, no VPN, no separate login. Location doesn't change the model.

TRUSTERA AT A GLANCE

The Future of Zero Trust & Unified Identity as a Service

- **Hardware-Anchored Identity**
- **Zero Passwords — Ever**
- **Tri-Layer Zero Trust**
- **One Card · Every System**
- **60-Second Onboarding**
- **Instant Offboarding**
- **CMMC 2.0 Native**
- **8 Products in One Platform**

Trustera is not a feature improvement on today's cybersecurity. It is a foundational replacement.