Trantor®

AUTENTICAZIONE E MFA · ON-PREMISE

Imago

Gestione centralizzata dell'identità, per ogni punto di accesso dell'azienda.

Il server di autenticazione e MFA on-premise: password verificate sulla tua directory o IdP aziendale (qualsiasi server LDAP, Active Directory, OIDC, SAML, RADIUS), secondo fattore con TOTP/FIDO2 e con la carta biometrica Imago BioCard. SSO moderno e protocolli legacy, tutti con le stesse policy.

PROTOCOLLI MULTIPLI · AUTENTICAZIONE A PIÙ FATTORI · CARTA BIOMETRICA FIDO2 · APPLICAZIONI LEGACY · PROTEZIONE AVVIO COMPUTER CON PBA · SISTEMA ANTI-COERCIZIONE · ON-PREMISE

PORTA L'AUTENTICAZIONE A UN LIVELLO SUPERIORE

Imago esiste per uniformare gli accessi e le policy di autenticazione, portare l'MFA in tutti gli applicativi, e rafforzare la sicurezza del perimetro più vulnerabile, come le postazioni di lavoro.

trantor.it · info@trantor.it

10 agosto 2026

PERCHÉ IMAGO

Cosa risolve Trantor® Imago

01

Password ovunque

Agli utenti non piace memorizzare password lunghe, né tantomeno cambiarle ogni 90 giorni. Con Imago puoi portare l'autenticazione senza password in tutta l'azienda, sfruttando la tecnologia FIDO2 oppure i certificati client.

Policy e audit frammentati

Applicazioni diverse impongono regole diverse per gli accessi (massimo numero di tentativi falliti, ecc.), e ogni applicazione ha i suoi log e il suo registro dove si tiene traccia dei login riusciti/falliti, logout, cambi password (sperando che questo registro effettivamente esista). Per tenere tutto sotto controllo, c'è bisogno di un unico posto dove definire tutte le regole, e dove poter vedere tutti i log.

MFA eterogeneo e non sempre attivo

Il problema dell'autenticazione a più fattori? Alcune applicazioni la supportano, e altre no. Alcune applicazioni permettono di sfruttare la stessa MFA usata altrove, e altre no. Il risultato: l'utente si ritrova a gestire più canali 2FA diversi, oltre a non poterla usare affatto su alcuni applicativi.

Le applicazioni legacy rendono difficile una modernizzazione degli accessi

Le applicazioni rilasciate anni fa, e che adesso sono in manutenzione correttiva, non corrono il rischio di rompere il codice per introdurre nuovi metodi di autenticazione. Il risultato: dimenticati di usare tecnologie moderne come le card biometriche per fare login in quelle applicazioni. Imago risolve il problema in due modi: si integra nativamente con tutte le applicazioni, esponendo protocolli come LDAP e RADIUS, e poi con Imago 4Legacy puoi far autenticare gli utenti da un portale moderno prima di farli atterrare sulle applicazioni legacy.

L'autenticazione dei tuoi utenti non avviene nella tua azienda

Molte soluzioni che vengono proposte richiedono obbligatoriamente che l'autenticazione passi attraverso il cloud del vendor, causando lock-in (es. per avere autenticazione FIDO2 all'accesso di Windows bisogna usare il cloud Microsoft Entra ID, e Microsoft non dà alternative), e mettendo a rischio l'integrità della tua infrastruttura, oltre a rendere impossibile attuare soluzioni omogenee tra dipartimenti online e air-gapped/isolati.

Vuoi accedere con la tua impronta digitale, senza condividere i tuoi dati biometrici

Molti sistemi di autenticazione biometrica memorizzano questi dati in un server o sul computer. Far transitare le informazioni biometriche come impronte o scansioni facciali presso dispositivi terzi è un incubo di privacy e sicurezza. Con le carte biometriche Imago BioCard, la tua impronta digitale resta sulla carta, sempre con te, e la puoi usare per autenticarti ovunque.

COS'È TRANTOR IMAGO

«Un'appliance server per gestire in maniera centralizzata e uniforme: password, secondo fattore, policy e log. Imago porta l'autenticazione moderna su tutti gli applicativi, funziona anche on-premise, e si può agganciare a un sistema già in piedi come Active Directory.»

COME FUNZIONA

Panoramica tecnica: parte 1

02

Componenti della soluzione

Appliance centrale (**Trantor® Imago Appliance**) basata su AlmaLinux 10. **Trantor® Imago CP** è il credential provider da installare su Windows per portare autenticazione FIDO2/TOTP sulle postazioni di lavoro Microsoft. **Trantor® Imago 4Legacy** è un componente dell'appliance centrale in grado di aggiungere autenticazione moderna alle app legacy. **Trantor® Imago PBA** è il software che porta la pre-boot authentication sui computer Windows. Inoltre, c'è supporto nativo alle **Trantor® Imago BioCard**, carte biometriche FIDO2.

Trantor® Imago Appliance

Server centrale basato su **AlmaLinux 10**, installabile on-premise su bare-metal o macchine virtuali, **x86 o ARM**. Due o più appliance sbloccano **bilanciamento di carico** e **alta affidabilità**.

Protocolli esposti per far collegare applicazioni terze

Imago espone verso applicazioni terze i seguenti protocolli per l'autenticazione: **LDAP/LDAPS** (username con password/password+TOTP), **RADIUS** (username con password/password+TOTP, oppure username con password con challenge-response, oppure **802.1X** EAP-TLS / EAP-TTLS-PAP / EAP-TTLS-GTC / EAP-PWD / EAP-PEAP-GTC), **OpenID Connect** (con PKCE, CIBA, e device-code), **SAML 2.0**. Per l'enumerazione di utenti/gruppi Imago espone LDAP/LDAPS e **SCIM 2.0**.

Protocolli supportati per collegarsi a directory/IdP già esistenti

Imago è in grado di usare come fonte di autenticazione i seguenti backend: **LDAP/LDAPS** (username+password), **RADIUS** (username+password, username+password+challenge, **802.1X** EAP-TLS / EAP-TTLS-PAP / EAP-TTLS-GTC / EAP-PWD / EAP-PEAP-GTC), **OpenID Connect** (con device-code, PKCE, CIBA), **SAML 2.0**. Per l'enumerazione utenti/gruppi, Imago è in grado di usare LDAP/LDAPS, **SCIM 2.0**, oppure importazione tramite file.

Autenticazione a più fattori e autenticazione passwordless

Imago supporta sia la gestione locale del 2FA (tramite **TOTP** o **FIDO2**), sia gestione tramite server **MFA esterno** (tramite interfaccia API Imago + plugin che fa da connettore). Inoltre, si può impostare che alcuni utenti possano usare FIDO2 come unico fattore di autenticazione per consentire **l'accesso senza password** (utile quando usato con le carte biometriche Imago BioCard, che si sbloccano con l'impronta dell'utente). Imago porta l'autenticazione a più fattori anche agli **applicativi legacy** che usano LDAP o RADIUS.

Trantor® Imago CP

Imago CP è il **Credential Provider** per **Windows** x64/ARM64 compatibile con Windows 10/11 e Windows Server 2019/2022/2025. Permette di usare le feature del login Imago anche con le postazioni di lavoro Windows, supportando **password, TOTP, FIDO2, OIDC device-code, autenticazione passwordless, anti-coercizione**, e integrandosi anche con Imago PBA per fare **SSO**. Imago CP inoltre supporta **autenticazione offline** temporanea ed è usabile anche tramite **RDP**.

Trantor® Imago 4Legacy

L'**identity-aware proxy** di Imago mette **FIDO2/TOTP davanti alle app legacy**: il portale autentica, il proxy fa entrare con credenziali effimere monouso. L'applicazione legacy non viene mai in contatto con la password reale dell'utente.

Panoramica tecnica: parte 2

Trantor® Imago PBA

Imago PBA è un software per fare **pre-boot authentication**: è essenzialmente un piccolo sistema operativo basato su **AlmaLinux 10** che viene installato sul computer Windows, a fianco ad esso, e viene **eseguito all'avvio del computer** per effettuare autenticazione tramite Imago. Se l'autenticazione va a buon fine, Imago PBA sblocca il BitLocker della partizione Windows e lo avvia. La partizione Linux Imago PBA è protetta tramite **immagini immutabili firmate digitalmente** (il cui certificato viene inserito nel firmware del computer) e tutti i dati sono crittografati con **LUKS2+TPM**. L'installazione/aggiornamento/disinstallazione di Imago PBA avvengono tutte tramite il **programma Imago PBA Manager** installato sul Windows del computer, in modo da non avere bisogno di boot da ISO o pre-imaging. Imago PBA si può usare insieme ad Imago CP per ottenere il **SSO** (ovvero: l'utente fa login su Imago PBA e poi al boot di Windows si ritrova già loggato). Imago PBA inoltre può opzionalmente esporre un server **RDP** per permettere agli utenti di sbloccare il PC anche a distanza, particolarmente utile per i server, ma non solo. Imago PBA, come il CP, supporta anche l'**autenticazione offline** temporanea. Quando Imago PBA viene usato insieme a Intel Boot Guard o AMD Platform Secure Boot (PSB), permette alti livelli di protezione anche in caso di **manomissione del firmware della scheda madre**.

Trantor® Imago BioCard

Le Imago BioCard sono delle **card FIDO2** che sfruttano la biometria a bordo per autenticare l'utente. La caratteristica principale è l'integrazione nativa con Imago, e il fatto che l'**impronta digitale** rimane sulla card e non viene trasmessa a computer o server. I dettagli si trovano nelle pagine a seguire.

Autenticazione anche per le reti WiFi, con Trantor® SecureWiFi

Chi ha anche **Trantor® SecureWiFi** può usare Imago come backend di autenticazione per la rete WiFi: SecureWiFi si occupa di configurare in autonomia il **connettore RADIUS/802.1X di Imago** in modo che i dispositivi (telefoni/tablet/computer/ecc.) possano **autenticarsi sulla rete WiFi tramite Imago**. SecureWiFi genera anche automaticamente i profili WiFi importabili su Windows/macOS/Linux/Android/iOS **in modo che l'utente non debba configurare manualmente la WiFi**.

Sistema anti-coercizione

Imago include un sistema **anti-coercizione** che permette all'utente di segnalare in maniera indiscreta che per qualche motivo sta effettuando un login perché **sotto costrizione**. Quando si effettua (**da qualsiasi punto di accesso collegato ad Imago**) il login anti-coercizione, Imago invia subito **una segnalazione** a tutti gli amministratori configurati. Inoltre, se si effettua login anti-coercizione su Windows (con Imago PBA o Imago CP), si può **eseguire in automatico uno script su Windows** (definito dall'amministratore) che può preparare l'ambiente in modo che sia realistico ma senza dati troppo confidenziali (ad esempio, lo script può smontare unità di rete confidenziali e montare unità di rete con dati falsi).

Trantor® Imago come proxy di protocollo/SSO

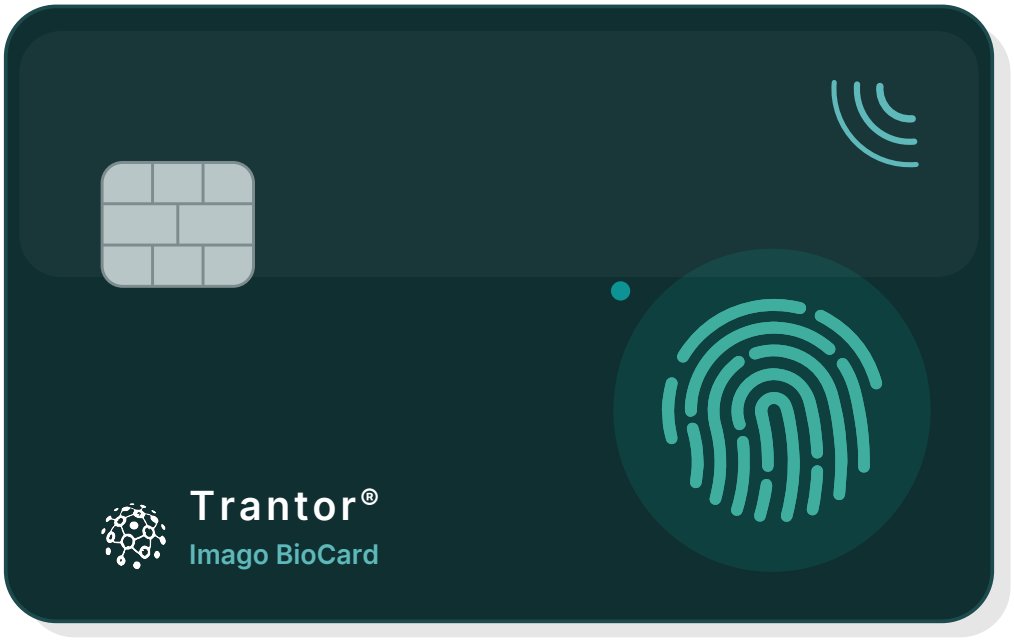
Imago permette diverse **combinazioni di protocolli esposti e protocolli usati dai realm** sottostanti: così facendo permette di fare da proxy per **convertire diversi protocolli**. Di seguito alcuni esempi: un'applicazione si può collegare con RADIUS+challenge a Imago, e Imago lo converte in OIDC+device-code verso il realm; un'applicazione può collegarsi con OIDC+SCIM a Imago, mentre Imago si collega con RADIUS+LDAP al realm; un'applicazione può collegarsi con FIDO2 password-less a Imago, e Imago si collega con Active Directory per ottenere il token di accesso.

LA CARTA

Imago BioCard

04

Codice completo: **Trantor® Imago BioCard**. La carta FIDO2 biometrica della gamma: NFC e lettori smartcard, la credenziale si libera al tocco dell'impronta.



	Specifiche della carta
Formato	Card di dimensioni standard, perfetta per portarla sempre con sé
Tecnologia	FIDO2 / WebAuthn: credenziale a chiave pubblica, resistente al phishing
Biometria	Sensore d'impronta a bordo: la carta si sblocca col tocco e il dato biometrico non lascia mai la card
Interfacce	NFC contactless e lettori smartcard
Dove funziona	Applicativi web che supportano nativamente WebAuthn, logon delle postazioni Windows/Linux/macOS, e anche applicativi legacy grazie a Trantor® Imago 4Legacy
Enrollment	Dal portale self-service Imago, in autonomia
Smarrimento	La carta si revoca dal centro; il TOTP resta come riserva sui canali che lo usano

L'IMPRONTA RESTA SULLA CARTA

Il sensore verifica l'impronta a bordo: nessun dato biometrico viaggia in rete o finisce su un server. La carta sblocca se stessa; Imago verifica la credenziale.

POSIZIONAMENTO

Trantor® Imago e le alternative

05

Ogni alternativa qui sotto è un prodotto serio, con punti di forza reali. Il confronto utile non è la lista delle funzioni: è dove vivono le identità, se il legacy è compreso o resta fuori, e che cosa succede quando il collegamento verso il cloud si interrompe.

Soluzione	Dove risiede il controllo	MFA e protocolli	Considerazioni
Trantor® Imago Trantor® · Italia	Server on-premise, nella tua rete: nessun cloud obbligatorio, funziona anche in ambienti isolati	TOTP e carta biometrica FIDO2; password sulla tua directory (qualsiasi LDAP, Active Directory compreso) o via OIDC/SAML; SSO moderno, proxy per il legacy e avvio sicuro con Imago PBA	Un solo motore di policy e un solo audit per tutti i punti di accesso; le credenziali non lasciano l'azienda; supporto diretto del team di sviluppo
Microsoft Entra ID Microsoft · extra-UE	Cloud Microsoft, non opzionale: anche l'ibrido passa dai server Microsoft	MFA con Authenticator, FIDO2 e Windows Hello; SSO OIDC/SAML; il legacy resta sull'AD on-premise	La scelta di default negli shop Microsoft, con l'MFA nei piani per utente P1/P2; gestione, policy e identità vivono nel cloud del vendor; niente PBA; niente proxy per app legacy
Okta Workforce Identity Okta · extra-UE	Cloud del vendor, non opzionale	Catalogo MFA ampio (push, FIDO2, TOTP); SSO su migliaia di app a catalogo; agent per AD e LDAP	Il riferimento del cloud IdP, con l'ecosistema più vasto; prezzo per utente e per modulo; niente PBA; niente proxy per app legacy
Cisco Duo Cisco · extra-UE	Cloud Cisco, non opzionale	MFA a push fra le più semplici da adottare; SSO nelle edizioni superiori; per directory, RADIUS e LDAP serve l'Authentication Proxy	Adozione rapida e buona esperienza utente; canone per utente al mese, e il servizio dipende dalla raggiungibilità del cloud; niente PBA; niente proxy per app legacy
Keycloak open source · Red Hat	On-premise o nel cloud	OIDC e SAML completi, TOTP e WebAuthn/FIDO2 inclusi; federazione su LDAP e Active Directory	Libertà massima e community enorme; hardening, aggiornamenti e alta affidabilità restano manuali del cliente, col supporto commerciale solo via Red Hat; niente PBA; niente Credential Provider per Windows; niente proxy per app legacy
privacyIDEA NetKnights · Germania	On-premise	Server MFA multi-token (TOTP, WebAuthn, smartcard); per SSO e accesso si appoggia a un IdP o ai moduli PAM/RADIUS	L'altra alternativa europea, open source; UI di gestione un po' datata e macchinosa; copre il secondo fattore più che l'insieme: SSO, self-service e legacy vanno composti pezzo per pezzo; niente PBA; supporto app legacy limitato (es. TOTP come suffisso della password)

MODELLO

Trantor® Imago in breve

06

Che cosa offre Trantor® Imago alla tua azienda

- **SSO moderno:** OIDC e SAML per le applicazioni web moderne e per le applicazioni legacy.
- **MFA esteso:** TOTP offline, carte e token FIDO2, e integrazione con servizi MFA esterni (per esempio, per il push SMS).
- **Accesso alle postazioni di lavoro con MFA:** Windows, Linux e macOS; TOTP o FIDO2, anche on-premise e senza cloud.
- **Portale self-service:** enrollment FIDO2/TOTP, cambio e reset password, reset secondo fattore.
- **Proxy per il legacy:** FIDO2 davanti alle app che parlano solo LDAP o RADIUS.
- **Registro e policy unificate e centralizzate:** ogni applicazione, ogni metodo di autenticazione, tutti con policy e audit centralizzati.
- **La carta che sblocchi con l'impronta:** Imago BioCard è una card FIDO2 per l'autenticazione biometrica usabile per l'accesso alle applicazioni e alle postazioni di lavoro, anche senza password.

Come Trantor® Imago garantisce alti standard di sicurezza

- **Appliance hardenizzata:** il server centrale usa immagini immutabili Linux con firma digitale, crittografia disco con LUKS2+TPM, e accesso come root disabilitato e consentito solo tramite chiave di emergenza conservata in cassaforte.
- **Autenticazione FIDO2/WebAuthn:** un sistema anti-phishing e con chiavi crittografiche forti.
- **Card biometriche:** le Imago BioCard conservano l'impronta digitale sulla carta stessa, e proteggono l'autenticazione FIDO2 tramite biometria anziché PIN.
- **Protocolli moderni ovunque:** Imago 4Legacy e le funzioni proxy di Imago permettono di adottare tecnologie moderne (come OpenID Connect con PKCE, SCIM 2.0 e FIDO2) ovunque.
- **Sistema anti-coercizione:** perché la sicurezza informatica è strettamente correlata a quella fisica.

Standard aperti, nessun ricatto

Imago parla OIDC, SAML, RADIUS, LDAP, SCIM e WebAuthn: standard aperti a ogni livello. La tua autenticazione resta leggibile e verificabile, anche senza di noi.

Perimetro di dettaglio e condizioni si dichiarano prima della firma, con la stessa regola di tutta la gamma Trantor®.

LA PROSSIMA MOSSA

Diamo un volto ai tuoi accessi.

Programma subito una consulenza per mappare gli accessi della tua azienda: app moderne, legacy, VPN e postazioni di lavoro. E ti diciamo cosa può fare Imago per te.

trantor.it

info@trantor.it