Affidati a Identity Essentials

Realizza uno schema Zero Trust

Entrust Identity copre l'intera gamma di soluzioni IAM, dalla protezione MFA e VPN per ambienti basati su Windows, all'autenticazione senza password con credenziali ad alta affidabilità, disponibile sia nella versione on premise che in cloud

ENTRUST

IDENTITY
ESSENTIALS

PANORAMICA

Identity Essentials

Identity Essentials è la proposta di Strong Authentication ideale per le aziende alla ricerca di una soluzione rapida ed economica per proteggere le identità dei collaboratori e consentirne l'operatività anche da remoto. Con Identity Essentials potete partire da una soluzione MFA o n premise, facile da usare e da distribuire, per poi migrare s al cloud con Identity as a Service, se e quando lo riterrete opportuno. La perfetta integrazione tra Identity Essentials e Identity as a Service garantisce una configurazione ibrida senza attriti, potendo contare su tre opzioni di autenticazione:

- Autenticazione con impronta digitale sul dispositivo
- Autenticazione push mobile
- Autenticazione grid card

Identity Essentials fornisce, alle organizzazioni basate su Windows, le basi per realizzare nel tempo un approccio Zero Trust con Identity as a Service.

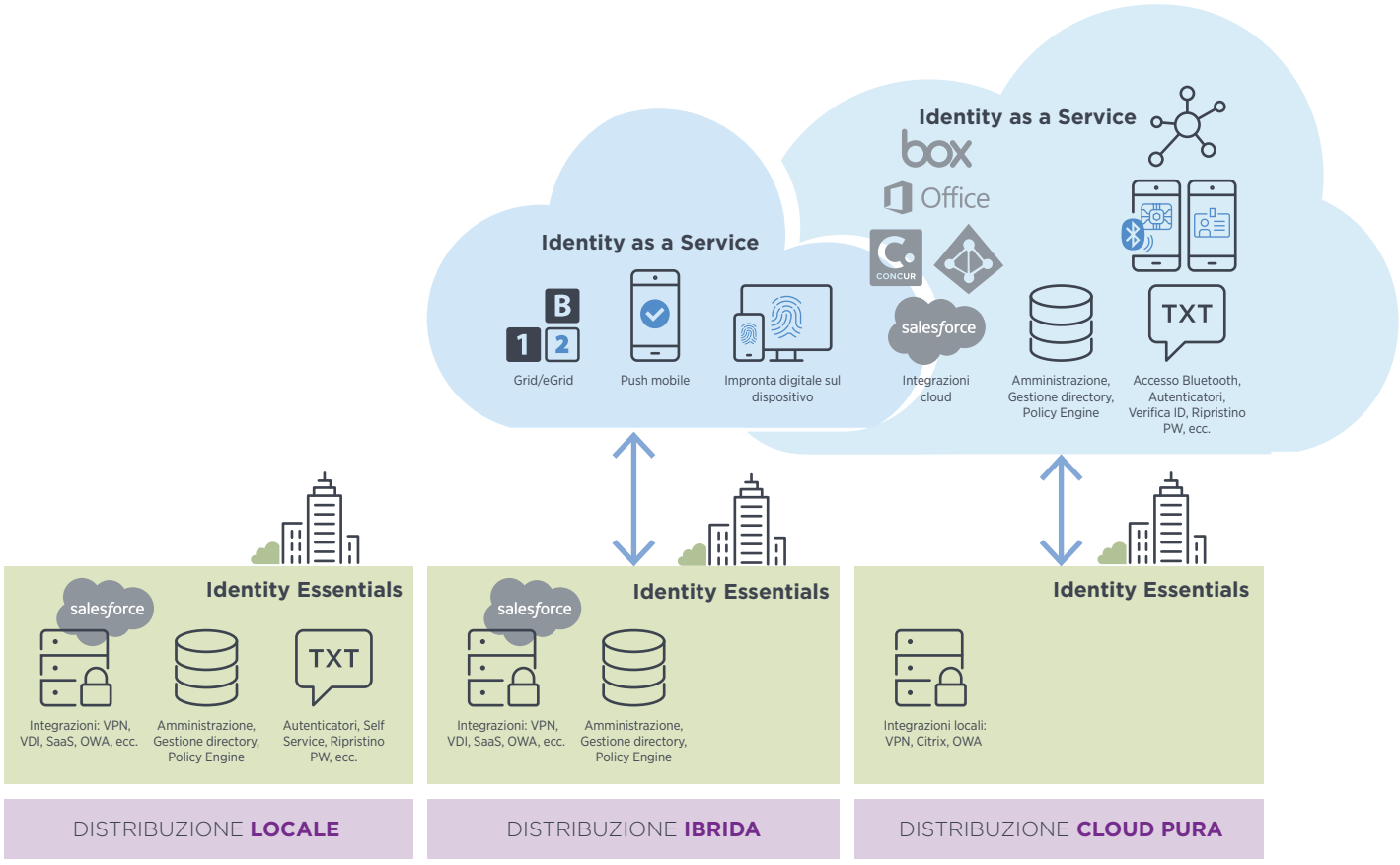
Facilita l'operatività dei lavoratori in remoto.

COME FUNZIONA

Combattiamo contro le peggiori minacce grazie ad una valida tecnologia

Se un hacker ottiene la password di un dipendente, può accedere a tutte le sue risorse : nel cloud e il locale. E poiché la maggior parte delle organizzazioni rende disponibili più servizi cloud (per file system, intranet, siti di collaborazione, ecc.,) una grande mole di dati viene in effetti esposta. Fortunatamente, al giorno d'oggi, l'utilizzo di sistemi di strong authentication presenta meno difficoltà rispetto al passato, sia per gli utenti sia per gli amministratori. E, grazie all'integrazione fra Identity Essentials e Identity as a Service,potete accedere al l cloud come preferite, con accesso senza password e Smart Login per Windows 7, 8, 10 e MacOS.

Identity Essentials consente accedere al cloud fino al livello desiderato, grazie alla perfetta integrazione con Identity as a Service.*



*Solo per i clienti di Identity Essentials con licenza in abbonamento.

PER APPROFONDIRE: ENTRUST.COM/IDENTITY-ESSENTIALS

Opzioni di licenza: che cosa comprende*

Le aziende che scelgono il pacchetto in abbonamento ottengono il massimo vantaggio dalla stretta integrazione tra Identity Essentials e Identity as a Service.

	Garanzia software	Bundle in abbonamento
Miglioramenti di Identity Essentials	●	●
Supporta Windows Server 2019	●	●
Impronta digitale sul dispositivo con AD FS (Identity as a Service)	●	●
Autenticazione push mobile (Identity as a Service)	●	●
Provisioning di dispositivi ActiveSync per Office365 ed Exchange locale	●	●
Identity as a Service “Plus”, include motore di rischio, autenticazione da cloud a cloud, ecc.		●
Servizio di invio globale di OTP basato su SMS, app e voce		●
Portale Single Sign-On Identity as a Service per tutti i servizi cloud, da un’unica piattaforma protetta		●
Assistenza per Identity Essentials in orario lavorativo (può essere esteso)		●
Supporta grid card	●	●
Funzionalità avanzate per l'autenticazione dell'accesso a Windows da console	●	●

*Identity Smart Login è una funzionalità aggiuntiva a pagamento.

Il motore adattivo, risk-based di Entrust Identity fornisce un ulteriore livello di sicurezza quando le condizioni lo richiedono, ad esempio quando un lavoratore accede per la prima volta da un nuovo dispositivo, in orario anomalo nell’arco della giornata o da una diversa posizione geografica. La richiesta un’autenticazione aggiuntiva, quale una notifica push sul dispositivo mobile, richiesta solo in presenza di queste situazioni, riduce al minimo le azioni aggiuntive richieste agli utilizzatori, proteggendo al contempo le risorse aziendali.

Ampia gamma di autenticatori supportati

Con Identity Essentials puoi scegliere i metodi di autenticazione più adeguati alle tue esigenze. A seconda dei diversi fattori, come l'accesso alle risorse, il dispositivo utilizzato e il livello di capacità tecnica dell'utente, puoi scegliere metodi di autenticazione diversi.

Tre sono le funzionalità disponibili (elencate di seguito) tutte possibili grazie all'integrazione di Identity as a Service, che consente ai dipendenti di accedere a workstation, reti e applicazioni in modo sicuro, senza il problema di dover immettere una password o di impiegare in ogni sessione i tradizionali metodi a due fattori. Garantisce un'esperienza di accesso autenticamente sicura, senza password e senza problemi.

Autenticatori di Identity Essentials

PIÙ 3 FUNZIONI DI AUTENTICAZIONE BASATO SU IDENTITY AS A SERVICE

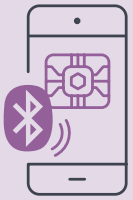
Autenticazione dell'impronta digitale sul dispositivo

Quando si accede alle app sul cloud tramite ADFS, è possibile acquisire una nuova propria impronta digitale, il che consente il rilevamento automatico di un dispositivo utilizzato in precedenza e fornisce un ulteriore livello di sicurezza che consente di evitare l'uso di OTP password.

Anche l'uso del motore di rischio di Identity as a Serviceo può rappresentare un aspetto da considerare, insieme alla geolocalizzazione, all'indirizzo IP, all'ora di accesso, alla velocità del trasferimento, ecc.

Autenticazione push mobile

Aggiungi un ulteriore livello di sicurezza quando i dipendenti i desiderano accedere in un momento o da un luogo insolito. L'app di autenticazione push brandizzabile fornisce la sicurezza biometrica grazie alle tecniche native di biometria mobile, per impedire accessi non autorizzati. L'app dispone dei pulsanti "Conferma", "Nega" e "(segnala un)Problema"; i problemi vengono registrati e viene inviato un rapporto a un amministratore.



Autenticazione senza password

L'autenticazione con grid card fornisce alle organizzazioni uno strumento di autenticazione semplice ma efficace che garantisce maggiore sicurezza e controllo dell'accesso logico. Agli utenti viene presentata una richiesta di verifica dell'autenticazione quando accedono a una rete, a un'applicazione, a un servizio cloud o a un sito ad accesso limitato. Ogni grid card è unica e ha un numero di serie, quindi ogni utente può essere identificato e autenticato in modo univoco. Ogni volta che a un utente viene richiesta l'autenticazione, viene presentata una domanda di verifica diversa da convalidare con una coppia diversa di coordinate della griglia. La richiesta delle coordinate cambia per ogni verifica di autenticazione.

Autenticazione con impronta digitale sul dispositivo: accesso facile e sicuro

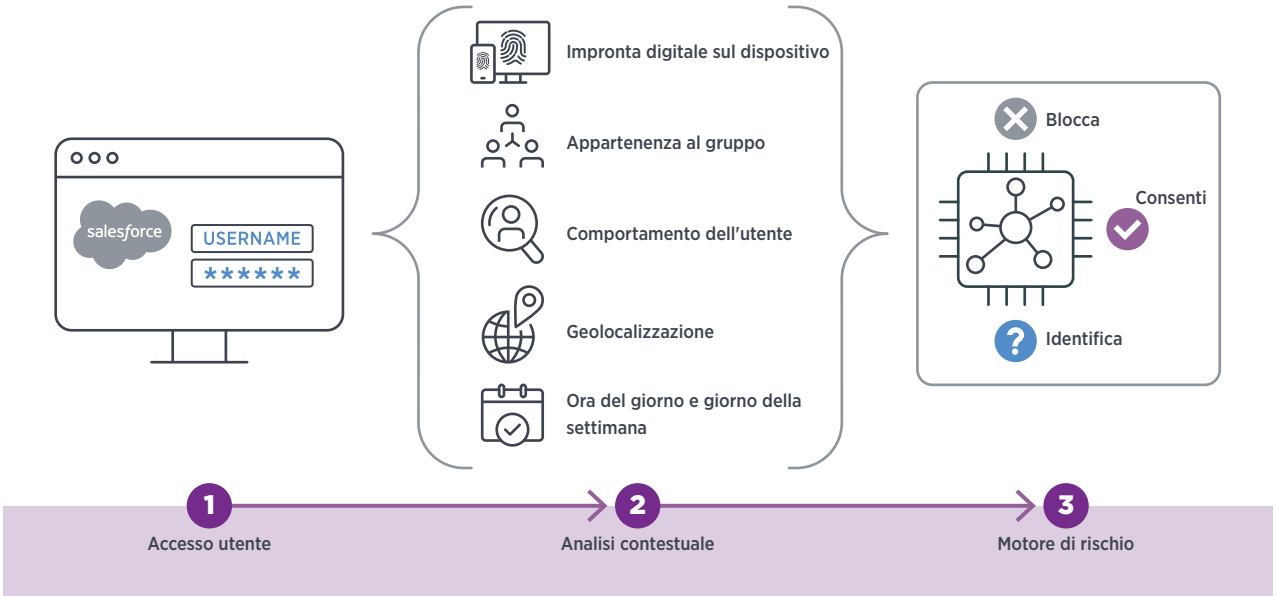
Oltre l'80% di tutte le violazioni legate alla pirateria informatica sono riconducibili alla debolezza o al furto delle credenziali utente. L'aggiunta della MFA su tutti i servizi aumenta notevolmente la sicurezza poiché toglie agli hacker la loro arma preferita.

Per risolvere il problema relativo all'accesso negato agli utenti, potete utilizzare le capacità di intelligenza adattiva/contestuale, che hanno già migliorato l'esperienza degli utenti di migliaia di organizzazioni.

Identity Essentials ha aperto la strada all'autenticazione adattiva, in cui l'accesso viene concesso a seconda del contesto, ad esempio se l'utente ha effettuato l'accesso tramite VPN, Citrix, RDP o i servizi cloud.

L'impronta digitale sul dispositivo è l'ultima aggiunta e fornisce maggiore sicurezza rispetto a un cookie di autenticazione per convalidare un dispositivo già utilizzato per l'accesso.

AUTENTICAZIONE CON IMPRONTA DIGITALE SUL DISPOSITIVO – Basata su Identity as a Service



Identity Essentials elimina la necessità di accessi ripetitivi (e frustranti) grazie al motore di Identity as a Service, di facile configurazione, che rileva i rischi in tempo reale basandosi su dati contestuali e sul comportamento degli utenti.

Protezione ActiveSync: nessuna gestione dei dispositivi mobili

ActiveSync, il protocollo che semplifica la sincronizzazione di e-mail, contatti, ecc., determina un rischio per la sicurezza che viene spesso trascurato. Se un utente può configurare facilmente l'accesso a informazioni importanti utilizzando soltanto un indirizzo e-mail e una password, può farlo anche un hacker. E, quando proteggi OWA/Office365 con MFA, non devi dimenticare ActiveSync.

ESISTONO **TRE MODI PRINCIPALI** PER ACCEDERE AI CONTENUTI DI OFFICE 365/OWA

Client Outlook
su PC/Mac 50% del tempo dedicato all'e-mail

ActiveSync
tramite iPhone/Android/Tablet 40% del tempo dedicato all'e-mail

Browser
Office.com o OWA 10% del tempo dedicato all'e-mail

Nel corso degli anni, la nostra soluzione ha aiutato migliaia di organizzazioni supportando le azioni “Consenti”, “Blocca” o “Quarantena” in Office 365 ed Exchange Server 2013/2016/2019. Il provisioning intuitivo e sicuro dei dispositivi consente agli utenti di eseguire da soli l'onboarding rapido e semplice dei nuovi dispositivi ActiveSync senza compromettere la sicurezza e senza dover contattare l'help desk per ricevere assistenza.

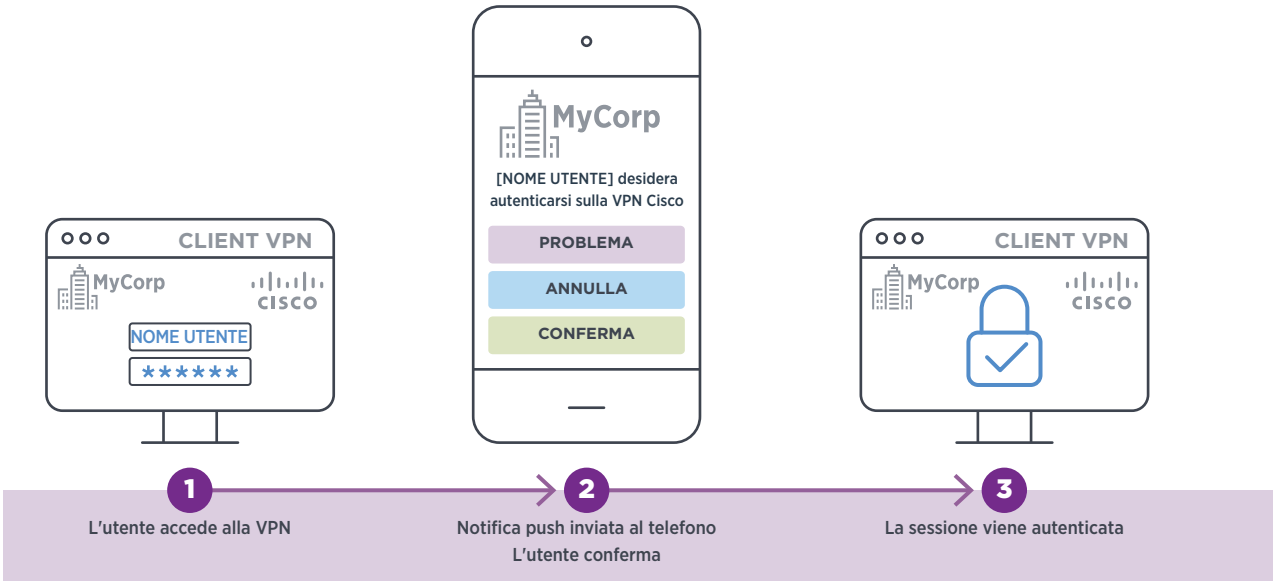
Il provisioning dei dispositivi semplice, sicuro e guidato dall'utente si adatta perfettamente alle culture BYOD. Non è necessaria una soluzione MDM completa. Semplifica la vita dei tuoi utenti consentendo loro di integrare i nuovi dispositivi e ottenere l’accesso di cui hanno bisogno, in modo semplice ma oltremodo sicuro, tramite il loro indirizzo e-mail.

Autenticazione push mobile: perfetta per i lavoratori tecnologicamente avanzati

Insieme all'integrazione di Identity as a Service, Identity Essentials include l'autenticazione push per consentire l'accesso tramite VPN/Citrix (Radius) e AD FS. Una volta attivata la funzione, sullo schermo del cellulare dell'utente appare un messaggio con "PROBLEMA", "ANNULLA" o "CONFERMA". Premendo il pulsante “PROBLEMA” l'accesso viene bloccato e registrato nel sistema per avvisare l'amministratore.

È possibile aggiungere una convalida biometrica (ad esempio, tattile o con identificazione del volto) per impedire l'uso non autorizzato delle app mobili o l'accesso di un hacker agevolato accidentalmente dall'utente. L'app visualizza anche le informazioni contestuali (ad esempio, "Tentativo di accesso dall'Hotel Hilton di Bangkok, Thailandia").

AUTENTICAZIONE PUSH MOBILE – Basata su Identity as a Service



L'app funziona sia per Android sia per iOS ed è disponibile in due forme: con o senza funzionalità di certificazione. L'autenticazione push è un'ottima funzionalità per gli utenti IT avanzati. Altri metodi di autenticazione che non richiedono installazione e configurazione sul telefono (SMS/testo, chiamata vocale, ecc.) rappresentano soluzioni tuttora valide per molti lavoratori di prima linea e per un pubblico meno preparato tecnicamente.

Autenticazione senza password: accesso semplificato alle app

Entrust Identity

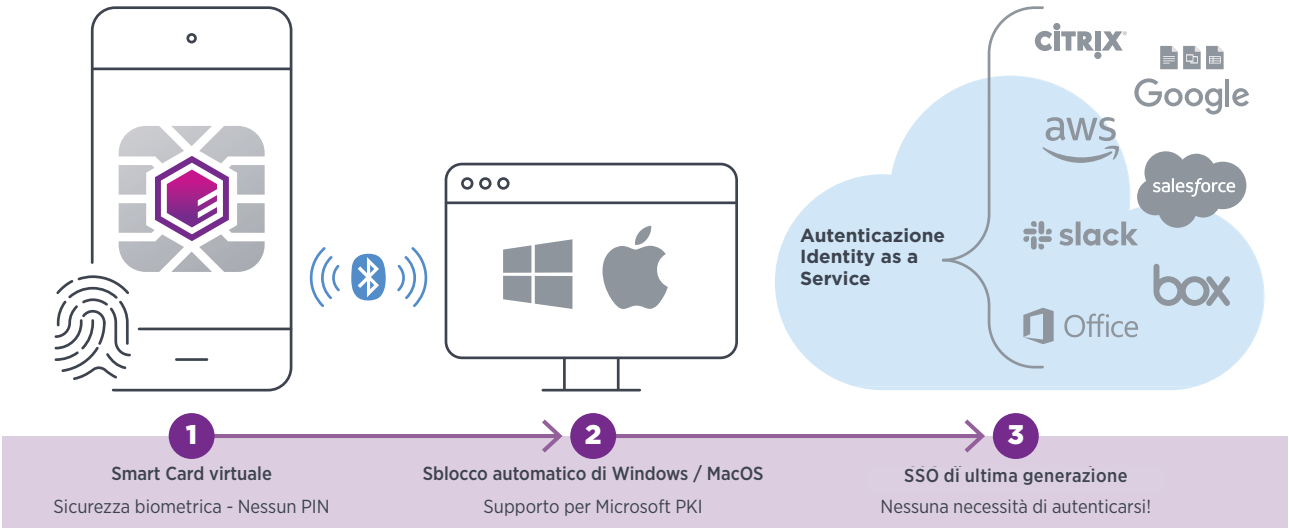
L'autenticazione multifattoriale che fornisce da molti anni un livello di sicurezza indispensabile, in aggiunta alle password. Tuttavia, il nostro mondo ha continuato a evolversi, sia dal punto di vista tecnologico, sia da quello delle minacce informatiche, e questo ha creato problemi con la MFA tradizionale.

In primo luogo, gli utenti si aspettano un accesso immediato a dati e applicazioni e l'MFA rappresenta un passaggio complicato. Dalla digitazione di codici di accesso una tantum (OTP) al trasporto di chiavette USB, l'MFA rallenta la produttività. Inoltre, se la chiave USB viene smarrita o si scarica la batteria del token hardware, l'accesso diviene impossibile. In secondo luogo, gli hacker stanno trovando modi per aggirare alcuni metodi della MFA, causando costose violazioni.

Lo Smart Login risolve i problemi principali della MFA massimizzando la sicurezza e riducendo al minimo le resistenze da parte dell'utente. La combinazione della sicurezza dei certificati digitali e della comodità del telefono cellulare ci consente di fornire soluzioni avanzate semplici per gli utenti finali.

Lo Smart Login di Entrust Identity consente ai dipendenti di accedere alla propria postazione di lavoro e alle applicazioni, avendo semplicemente con sé il proprio telefono. Niente più password e 2FA, come le domande basate sulle conoscenze o le OTP. L'accesso al computer e alle applicazioni è semplice e veloce, e presenta meno ostacoli per la sicurezza, aumentando la produttività. Inoltre, non è più necessario ricordarsi di bloccare le proprie postazioni di lavoro. Smart Login li disconnette automaticamente quando se ne vanno.

AUTENTICAZIONE SENZA PASSWORD – fornita da Identity as a Service



Caratteristiche di Identity Essentials

Integrazione senza interruzioni: la piattaforma MFA di Identity Essentials si integra perfettamente con i sistemi di accesso e le soluzioni cloud, per un'esperienza di accesso remoto intuitiva e facile da usare.

Autenticazione adattiva: adatta automaticamente il livello di autenticazione in base alle condizioni attuali dell'utente, unendo l'elevato livello di sicurezza con una grande facilità d'uso.

Failover automatico: è possibile impostare meccanismi di failover altamente flessibili per garantire che le OTP arrivino sempre. La soluzione può anche cambiare il tipo di trasmissione, a seconda del contesto di accesso che l'utente sta usando.

Ampio supporto delle directory: gli utenti possono essere sincronizzati da Active Directory e dalle directory LDAP generiche come OpenLDAP o AD LDS. Gli utenti possono essere importati selezionando un gruppo di utenti specifico o utilizzando un filtro LDAP.

Protezione in tempo reale: tutti i codici OTP vengono generati in tempo reale al momento del login. Non esistono codici d'accesso predefiniti o file seed che potrebbero essere violati. Nel contempo, il funzionamento in tempo reale è un prerequisito per fornire OTP specifiche per ogni sessione.

PowerShell: Paese

Feedback sullo stato: consente all'utente di seguire lo stato di avanzamento dell'accesso; infonde fiducia negli utenti e riduce il numero di chiamate all'help desk.

Consapevolezza della posizione e del comportamento: sfrutta informazioni contestuali come i modelli di comportamento d'accesso e la geolocalizzazione per concedere o negare l'accesso agli utenti. Il geofencing consente agli amministratori di inserire in whitelist o in blacklist basandosi su sistemi e posizioni (ad esempio, per limitare l'accesso tramite Citrix NetScaler da determinati paesi).

Provisioning sicuro dei dispositivi: consente agli utenti di registrare automaticamente e rapidamente nuovi dispositivi ActiveSync senza compromettere la sicurezza e senza dover contattare l'help desk per ricevere assistenza.

Metodi di invio delle OTP: ug-in e metodi di invio standard delle OTP, come app, SMS, chiamate vocali, e-mail sicure, chiavi cloud e token hard/soft, a supporto delle esigenze aziendali attuali e di quelle future.

Controllo avanzato dei database: aiuta i clienti a rispettare le rigide normative di settore e a soddisfare i requisiti dei controlli di audit.

Funzionalità aggiuntive tramite l'integrazione di Identity as a Service

App per autenticazione push mobile (brandizzate): aggiunge un livello di sicurezza di facile utilizzo nel caso in cui i dipendenti accedano in un momento o da un luogo insolito. Sul telefono cellulare appare un messaggio di notifica che chiede all'utente di confermare la propria identità per l'accesso.

Autenticazione con impronta digitale sul dispositivo: Dopo essere riusciti ad accedere a un servizio cloud tramite AD FS, l'impronta digitale sul dispositivo può essere acquisita e utilizzata per future valutazioni di sicurezza, semplificando l'accesso.

Autenticazione senza password: fornisce una credenziale sul telefono del lavoratore, abilitando l'accesso senza password alla workstation (Mac e PC) e l'SSO dell'applicazione (cloud e locale) tramite Bluetooth quando il telefono è nelle immediate vicinanze e viene sbloccato con l'impronta digitale dell'utente o il riconoscimento facciale.

Single sign-on (SSO): Identity as a Service offre l'SSO a tutte le app, cloud e locali, comprese le app legacy. Federazione con app cloud mediante standard come SAML e OIDC.

Integrazione con Azure AD: si integra con Azure AD per la sincronizzazione degli utenti, ecc.

Crittografia di e-mail e file: l'integrazione con i principali fornitori di MDM, inclusi Microsoft, IBM e VMware, garantisce la sicurezza delle comunicazioni sul luogo di lavoro con la crittografia di file ed e-mail.

Firma dei documenti: l'integrazione con i fornitori di MDM supporta transazioni sicure sul luogo di lavoro e non ripudio, grazie alla firma dei documenti.

Verifica dell'identità: verifica in modo sicuro le identità di dipendenti, lavoratori a contratto, partner e altre parti.

Autenticazione del consumatore: Identity as a Service va oltre l'autenticazione della forza lavoro. Può essere utilizzato anche per soddisfare tutte le esigenze di autenticazione del consumatore.

Portafoglio di identità di affidamento: Identity Essentials fa parte del portafoglio unificato "Entrust Identity" che include anche Identity as a Service e Identity Enterprise. Entrust Identity offre soluzioni IAM (Identity and Access Management) della forza lavoro per supportare organizzazioni dalle dimensioni più svariate, da 50 utenti fino a 1 milione.

Sistemi supportati

Identity Essentials supporta una vasta gamma di sistemi di accesso utilizzati per l'accesso remoto. La piattaforma è progettata per integrarsi perfettamente con centinaia di VPN e garantisce un processo di accesso sicuro e intuitivo. Di seguito viene riportato un elenco con esempi di sistemi di accesso remoto supportati.

Client VPN RADIUS VPN/SSL

- Check Point
- Cisco ASA
- Citrix Netscaler (Citrix ADC)
- Juniper
- Pulse Secure
- Firewall Barracuda NG
- VMware Horizon View
- Netop Remote Control
- Palo Alto
- F5 BIG-IP
- VPN NCP
- Altri client RADIUS

Siti web Internet Information Services (IIS)

Supporto dei seguenti tipi di siti Web:

- Outlook Web Access 2010/2013/2016/2019
- Remote Desktop Web Access (Windows Server 2012 R2 / 2016 / 2019)
- Siti Web IIS che utilizzano l'autenticazione di base integrata Windows e l'autenticazione basata su form ASP.Net

Accesso a Windows, Servizi Remote Desktop

Supporto dei seguenti server e servizi:

- Servizi Remote Desktop (connessioni RDP)
- Windows Server / 2012 / 2012 R2 / 2016 / 2019
- Windows 8, Windows 8.1 e Windows 10
- Portale e accesso client VMware Virtual Desktop

Provisioning sicuro dei dispositivi

Protezione per i dispositivi ActiveSync sui seguenti sistemi:

- Exchange 2010 SP3
- Exchange 2013
- Exchange 2016
- Exchange 2019
- Exchange Online

Protezione AD FS Microsoft

- Adattatore AD FS 3.0/4.0/5.0 per autenticazione multifattoriale

Supporto dell'autenticazione multifattoriale per:

- Accesso ad applicazioni cloud come Salesforce.com, Microsoft Office 365, Google Apps, ecc. (AD FS 3.0/4.0/5.0)
- Accesso ai siti Web pubblicati tramite Microsoft Web Application Proxy (AD FS 3.0/4.0/5.0), come Outlook Web Access
- Approvazione dei dispositivi in connessione con join al luogo di lavoro (AD FS 3.0/4.0/5.0)

Per maggiori informazioni

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

INFORMAZIONI SU ENTRUST CORPORATION

Entrust protegge un mondo in rapida evoluzione grazie al rilascio di identità, pagamenti e protezione dei dati affidabili. Viaggi, acquisti, accessi ai servizi della PA o alle reti aziendali: oggi più che mai, le persone vogliono vivere ogni esperienza in sicurezza, senza interruzioni in qualsiasi momento. Entrust offre un'ampia gamma di soluzioni per la sicurezza digitale e l'emissione delle credenziali su cui tutte queste interazioni sono basate. Oltre 2.500 colleghi, una rete di partner globali e clienti in oltre 150 Paesi: non c'è da meravigliarsi se siamo scelti dalle più importanti organizzazioni del mondo.

Ulteriori informazioni su
entrust.com

ENTRUST

Numero verde USA: 888 690 2424
Numero telefonico internazionale: +1 952 933 1223
info@entrust.com