



VERIFICA DELL'IDENTITÀ
PER ACCESSI PIÙ SICURI

MULTIFACTOR AUTHENTICATION

Datasheet



Le aziende del Gruppo MEET IT



Via di Corticella, 89/2
40128 Bologna BO

+39 05 14070383
www.3cime.com | info@3cime.com



Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
info@ntonline.it | www.ntonline.it



PROTEGGI. IDENTIFICA. ACCEDI.

Password forti e conservate al sicuro non sono più sufficienti. Per proteggere i tuoi accessi, utilizza l'Autenticazione Multifattoriale, in modo da essere protetto anche in caso di un furto di password.

Secondo il "2018 Data Breach Report" di Verizon:
"L'uso di credenziali rubate per violare le risorse di rete è la tattica numero uno impiegata dagli hacker."

L'autenticazione multi fattore (*Multi Factor Authentication - MFA*) è una forma di **autenticazione digitale dell'identità dell'utente basata su almeno due fattori di riconoscimento** che consente solo alle persone autorizzate di accedere a determinati asset: servizi, infrastrutture ICT, spazi online e reti.

Il servizio utilizza un **messaggio push, un QR code o una password monouso (OTP)** come fattori per il riconoscimento dell'identità, da inserire a seguito delle proprie credenziali di accesso. L'app informa l'utente di ogni tentativo di accesso, chiedendo se si desidera accettarlo o bloccarlo dal dispositivo prescelto per l'autenticazione.

Il metodo multifattoriale è ideale per proteggere l'accesso a **reti, VPN, servizi web, sistemi operativi, infrastrutture virtuali, applicazioni e cloud**, in modo da ridurre la probabilità di interruzioni della rete e le violazioni dei dati.

**TIPOLOGIE
FATTORI**



Push Message



QR Code



OTP Password

VISITA IL SITO MEETIT.CLOUD

COME VIENE
VERIFICATA
L'IDENTITÀ?



Qualcosa che sai
(password)



Qualcosa che hai
(token su smartphone o
altro dispositivo)



Qualcosa che hai
(DNA smartphone)
per impedire l'utilizzo
ai dispositivi clonati



Oppure, qualcosa che
sei (impronte digitali)

FOCUS ON

Password rubate nel DarkWeb

Il DarkWeb è una raccolta di siti web anonimi e pubblicamente disponibili che nascondono gli indirizzi IP in modo che gli utenti non possano identificare l'host.

In questo contesto accade che **informazioni sensibili e password siano pubblicate illecitamente**, rese disponibili e vendute, a seguito di violazioni andate a buon fine.

L'Autenticazione Multifattoriale per i login evita che le password rubate siano utilizzabili dai non addetti ai lavori.

- Massimi livelli di **sicurezza informatica** enterprise
- **Protezione degli accessi** di tutti gli utenti aziendali
- **Conformità a GDPR** e policy interne
- Ottima **user experience**
- **Semplicità**
- **Scalabilità**
- **Flessibilità**
- **Gestione centralizzata**
- **Integrabilità** con altri servizi
- **Supporto** dedicato
- **Costi molto contenuti**
- **Affidabilità**
- **Mobilità**
- Disponibile **Online/Offline**
- **Non richiede hardware** aggiuntivo

VANTAGGI