SecurAccess – 2FA | jednorázová hesla (OTP)

Autentizace uživatelů k firemním zdrojům by na jedné straně měla splňovat ty nejpřísnější nároky na bezpečnost a na straně druhé zajišťovat komfort uživatelů. Vyváženou kombinaci obou požadavků přináší společnost SecurEnvoy se svým nástrojem SecurAccess, zajišťujícím bezpečnou autentizaci pomocí jednorázových hesel zasílaných formou SMS, softwarových tokenů a emailů. Uživatelé se již nemusí frustrovat nároky administrátorů na zapamatování náročných hesel. Svoje jednorázové heslo mají vždy při sobě!

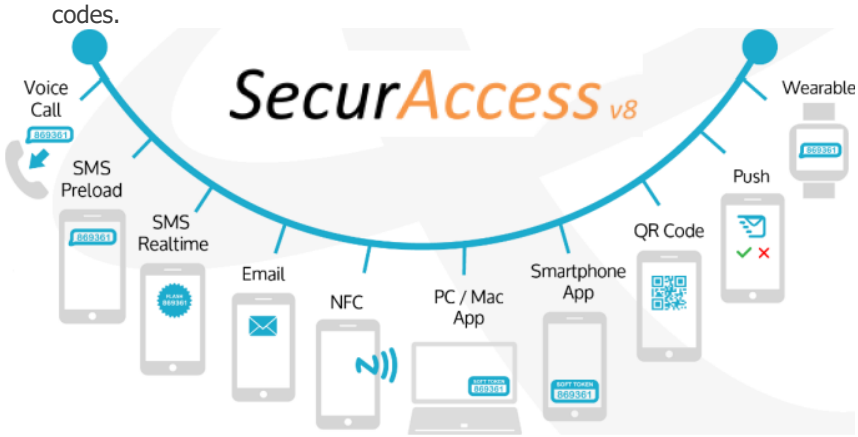
Jednoduché nasazení a správa | Na rozdíl od tradičních řešení zajišťujících dvoufaktorovou autentizaci pomocí jednorázových hesel se SecurEnvoy nemusíte provádět žádné výrazné zásahy do Vašeho existujícího IT a celé řešení nasadíte na několik kliknutí. Díky integraci s Vaším Microsoft Active Directory, Novell eDirectory, Sun Directory Server a OpenLDAP zajistíte jednoduše bezpečný přístup všem Vašim zaměstnancům během pár okamžiků.

Úspora nákladů | Velkou výhodou celého řešení je to, že pro autentizaci využívají uživatelé něco, co již vlastní - mobilní telefon. Není tedy nutné dále zvyšovat náklady pořizováním nového hardwaru v podobě tokenů. Stejně tak každý administrátor uvítá absenci časově náročné distribuce hardwarových tokenů, která může zabrat i několik týdnů. SecurEnvoy řešení nasadíte během chvilky a rozeslání hesel se již děje automaticky prostřednictvím SMS nebo softwarový aplikací.

Moderní autentizační metody | Technologie **OneSwipe** od SecurEnvoy ohlašuje konec hesel, což znamená radikální změnu v přístupu k systémům a informacím v elektronické podobě. SecurEnvoy vyvinul nový nástroj dvoufaktorové autentizace (2FA), která staví na podpoře **NFC** (Near Field Communication) v chytrých telefonech i nových Windows 10. Nyní bude uživateli stačit pouze zadat pin na chytrém telefonu, přiložit ho k zařízení a bude autentizován.

Autentizace pro každého uživatele | Řešení společnosti SecurEnvoy umožňuje výběr, jaký typ autentizace zvolíte pro Vaše uživatele. Máte na výběr z níže uvedených možností:

- ✓ **Pre-loaded SMS =** uživatel má vždy k dispozici heslo pro další použití dopředu (například pro místa bez GSM signálu jako serverovny).
- ✓ **Jednorázová SMS hesla na vyžádání** - uživateli se po vyžádání objeví na telefonu a po určité době zmizí (není třeba je mazat).
- ✓ **Softwarové tokeny** – Aplikace pro smartphony a laptopy.
- ✓ **Hardware tokeny** – v elegantním provedení autentizační karty.
- ✓ **One Time Code** – uživatel dostává vždy nové jednorázové heslo pro další použití (jak při úspěšné, tak neúspěšné autentizaci).
- ✓ **Day Code** – heslo je použitelné po definovaný počet dnů, následně uživatel dostává nové, bez ohledu na to, zdali se autentizoval, či nikoliv.
- ✓ **Tmp Static Code** – definované statické heslo platné po definovanou dobu a po uplynutí doby se vrací zpět na One Time Code či Day Code (nástrojů pro řešení situací, kdy uživatel zapomněl telefon).
- ✓ **NFC / QR code / wearable** – umožňuje využít chytrých hodinek nebo smartphone OTP autentizace s NFC technologií.
- ✓ **Voice Call** – podpora jednorázových hesel zadaných přes pevnou linku.
- ✓ **Jednorázová hesla zaslaná přes email** – preload, real time, three codes.



Klíčové vlastnosti

- ✓ **NOVINKA:** HW token SecurEnvoy – elegantní autentizační karta.
- ✓ **Vysoká míra zabezpečení** autentizace vzdálených přístupů se zachováním uživatelského komfortu (bez dalších portálů, modifikace stávajících portálů).
- ✓ **Pre-loaded technologie** řešící nedostupnost GSM pokrytí a zpoždění doručení SMS zpráv s jednorázovým heslem.
- ✓ Podpora **HW GSM bran či webových poskytovatelů SMS služeb.**
- ✓ **Žádné "seed" informace** uložené na serverech výrobce.
- ✓ Jednorázová hesla uložena na zařízení, které si uživatel maximálně chrání - **případná ztráta je odhalena prakticky ihned.**
- ✓ **Rychlé nasazení** řešení do stávající infrastruktury zákazníka.
- ✓ **Celkové snížení nákladů** na provozování celého řešení (snadno a rychle nasaditelné, snadno použitelné, bez client HW/SW).
- ✓ Administrátor definuje, jaký typ tokenů bude pro uživatele dostupný.
- ✓ Podpora provozování **více poskytovatelů SMS služeb současně.**

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

SecureIdentity - Data Loss Prevention (DLP)

DLP, tedy technologie určené k ochraně proti úniku dat, jsou v moderní době nezbytnou součástí bezpečnostních nástrojů většiny firem a organizací. Vzrůstající počet hackerských útoků vyvíjí větší nároky na bezpečností standardy a shody, které musí jednotlivé organizace plnit (např. GDPR). S tím je také spojen výběr vhodné technologie, která kromě prostého naplnění těchto regulací dokáže skutečně navýšit úroveň zabezpečení a ochránit důležitá aktiva.

Co je SecureIdentity?

SecureIdentity je jedinečná DLP platforma, která dokáže přesně identifikovat uživatele a v návaznosti na to také zařízení a data, se kterýma tento uživatel pracuje. Tento audit uživatelských aktivit dopomáhá k dosažení shody s bezpečnostními standardy a také hraje důležitou roli v ochraně duševního vlastnictví celé organizace.

SecureIdentity poskytuje komplexní ochranu dat celé organizace - ochrana je zajištěna proti úniku způsobeném malware, ale také záškodníkem uvnitř organizace, a nebo i lidskou chybou.

Manažerské výhody	Stěžejní funkcionality
✓ Poskytuje přehled o hodnotě firemních dat.	✓ Umožňuje stejné zobrazení a politiky aplikovat na všechny kompatibilní ODBC databáze.
✓ Snižuje riziko možných pokut a sankcí.	✓ Funkce OCR pro data v pohybu i data v klidu.
✓ Ochraňuje duševní vlastnictví a majetek organizace.	✓ Široké možnosti automatizovaných nápravných opatření.
✓ Zajišťuje dodržování firemních politik a zásad.	✓ Možnost manuální klasifikace dat při vytváření dokumentů.
✓ Kontrolujte tok dat třetím stranám a mezi. obchodními jednotkami.	✓ Označuje data jako taková, nikoliv pouze soubory.

Možnosti nasazení

S předinstalovanými virtuálními appliancemi trvá implementace řešení až do nainstalovaného stavu přibližně 30 minut. Díky velkému množství předdefinovaných DLP politik je řešení velmi rychle nasazeno do plnohodnotného provozu a návratnost investice je tedy téměř okamžitá.

Tato předdefinovaná pravidla jsou postupem času automaticky aktualizována a optimalizována, čímž je zajištěno, že žádná citlivá data neopustí Vaši organizaci.

Cloudové API DLP skenery umožňují nasazení stejných sad pravidel a funkcionalit ve všech cloudových prostředích, včetně Office 365, G Suite, Box a další.

Správa DLP řešení

SecurEnvoy DLP poskytuje bezkonkurenční množství Meta dat v souborech včetně Majitele souboru, naposledy vytištěno, naposledy zpřístupněno, tagy a mnoho dalších. Systém zahrnuje výkonný generátor reportů s intuitivním uživatelským rozhraním, kde lze také libovolně reporty přizpůsobit.

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz