uniqkey

Parola d'ordine:
Azienda e Gestione degli accessi

Securing your business in a digital world

Best Meets Requirements WINTER 2023

Best Results WINTER 2023

Users Most Likely To Recommend WINTER 2023

Top 50 Security Products BEST SOFTWARE AWARDS 2023

High Performer Europe WINTER 2023

Proteggi il tuo business nel mondo digitale
Perché la sicurezza informatica deve essere una priorità assoluta per le aziende nel 2022 e oltre

Gli attacchi informatici sono diventati una minaccia esistenziale per le organizzazioni

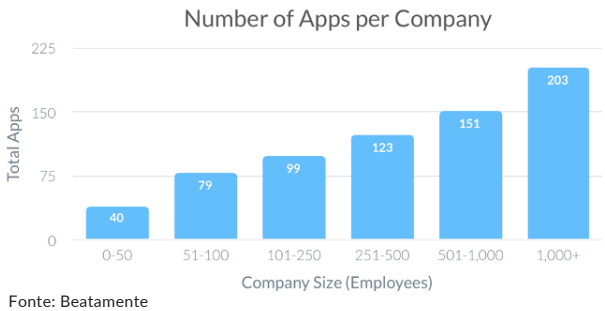
Alimentato da un'impennata nell'adozione globale del cloud, nella trasformazione digitale e nel lavoro remoto, il crimine informatico è cresciuto fino a diventare la più grande minaccia che le organizzazioni devono affrontare oggi. Secondo TechJury (1), il **64% delle aziende in tutto il mondo ha subito almeno una forma di attacco informatico**, con danni che vanno dalla rovina della reputazione del marchio e dalla fiducia dei clienti infranta a gravi costi finanziari.

Questa tendenza allarmante esercita una grande pressione sulle aziende - in particolare in Europa, poiché l'Europa è una delle aree più digitalizzate del mondo - per investire pesantemente nella sicurezza informatica o affrontare i costi paralizzanti di un inevitabile incidente informatico.

> *La criminalità informatica rappresenta il più grande trasferimento di ricchezza economica della storia, **per un totale di 10,5 trilioni di dollari di costi annuali** entro il 2025.*
>
> - Cybersecurity Ventures (2)

Più servizi. Più password. Più rischio.

Mentre la rapida adozione di servizi cloud e desktop e il lavoro remoto abilitato per VPN stanno spingendo la produttività e l'innovazione aziendale, queste circostanze stanno anche introducendo nuovi gravi rischi informatici poiché le aziende iniziano a perdere il controllo e la supervisione della loro crescente presenza digitale. Per darti un'idea di quanto sia dilagante questo problema, un'azienda media con 251-500 dipendenti gestisce oltre 123 diverse app aziendali.



Fonte: Beatamente

La trasformazione digitale non è un problema in sé e per sé. Con più servizi arrivano più accessi e password che i dipendenti devono ricordare, e quindi ogni nuovo servizio aggiunto è anche un nuovo potenziale punto di ingresso per gli hacker. Nel 2020, ad esempio, **gli attacchi mirati al desktop remoto sono aumentati del 768%** (3).

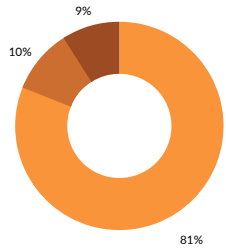
Secondo il Data Breach Investigations Report 2021 di Verizon, **la scarsa sicurezza delle password contribuisce all'81% di tutte le violazioni dei dati.** Considerando questo fatto, i rischi associati a questa nuova superficie di attacco in espansione non dovrebbero essere ignorati.

Cause di attacchi informatici e violazioni dei dati

Passwords: 81%
Password deboli o riutilizzate

Ransomware: 10%
Riscatto o estorsione

Altri: 9%



Fonte: Verizon

Molte aziende cercano di mitigare il rischio delle password implementando Single Sign On (SSO). Tuttavia, mentre SSO semplifica gli accessi, non aumenta necessariamente la sicurezza, in quanto copre solo una certa gamma di app e servizi. La migliore pratica di sicurezza è sempre stata quella di applicare password lunghe e univoche per ogni servizio, ma questo storicamente è stato sempre difficile da mettere in atto.

Una cattiva gestione delle password è solo una parte del problema. Un'altra cosa che sta mettendo a repentaglio la sicurezza delle aziende è la mancanza di visione d'insieme e controllo di chi ha accesso a cosa. Se non è possibile controllare quali dipendenti hanno accesso a quali sistemi , diventa sempre più difficile mantenere gli standard di sicurezza in tutta l'organizzazione.

Il lato oscuro della trasformazione digitale

Il problema principale della trasformazione digitale è che la maggior parte delle infrastrutture di sicurezza aziendali non è progettata per proteggere i servizi cloud e desktop. Peggio ancora, molte aziende non sono consapevoli della loro "impronta digitale", con conseguente aumento dell'uso sconosciuto di cloud, desktop e SaaS, noto come Shadow IT.

> *"L'80% dei lavoratori ammette di utilizzareApplicazioni SaaS al lavoro **senza ottenere l'approvazione dall'IT.** " (4)*

Come stare al sicuro in un mondo digitale

Oggi, chiunque può iniziare a utilizzare servizi off-premise , il che rende difficile per i responsabili IT gestire e mantenere un elevato livello di sicurezza in tutta l'organizzazione. Protetti solo da un nome utente e una password, questi servizi condividono tutti la stessa vulnerabilità di violazione.

Oggi, per mitigare il rischio di queste nuove superfici di attacco, le aziende devono migliorare la loro sicurezza di accesso, e il modo più efficace per raggiungere questo obiettivo è recuperare il controllo e la panoramica di tutte le risorse digitali, diffondere l'uso di 2FA e applicare una migliore sicurezza delle password in tutta l'organizzazione.

In teoria, queste iniziative sono difficili da implementare nel frenetico ambiente di lavoro digitale di oggi. In un tale ambiente, affidarsi a un comportamento umano impeccabile per rimanere al sicuro è un piano destinato a fallire perché l'errore umano è coinvolto nel 95% di tutti gli incidenti informatici (5). Invece, per avere successo, le aziende hanno bisogno di una soluzione **che rimuova il più possibile il fattore umano dall'equazione.**

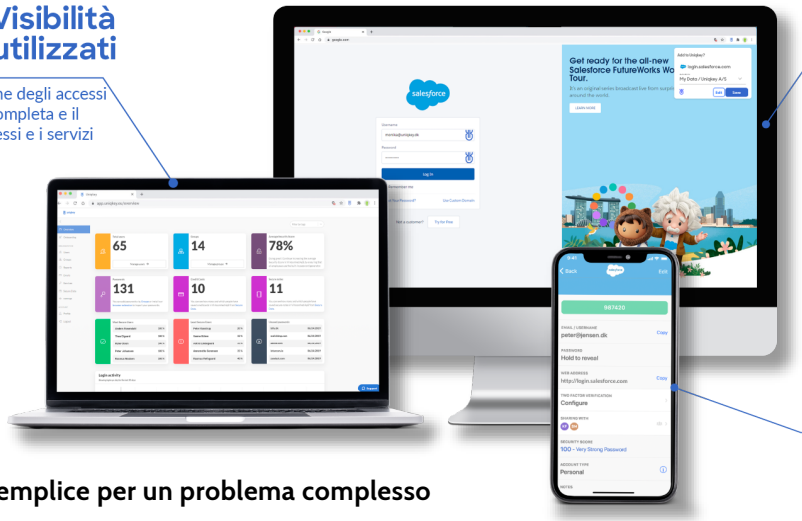
(1) TechJury "Quanti attacchi informatici al giorno nel 2022? ", 2022
(2) Rivista sulla sicurezza informatica, 2020
(3) Rapporto sulle minacce Q4 2020 di ESET., 2020
(4) Microsoft, 2022
(5) Global Risks Report 2022, World Economic Forum, 2018

Uniqkey aiuta le aziende a rimanere al sicuro in un mondo digitale semplificando la sicurezza informatica

In un'epoca di esplosione del cloud, del SaaS e dell'uso del desktop, i dipendenti stanno annegando nelle password e le aziende hanno perso la loro visione digitale. Uniqkey protegge le aziende dall'81 % **di tutte le violazioni dei dati** automatizzando l'uso delle password sul posto di lavoro, offrendo al contempo agli amministratori la panoramica e il controllo di cui hanno bisogno per mantenere l'organizzazione protetta e produttiva.

Guadagna Visibilità nei serivizi utilizzati

la piattaforma di gestione degli accessi offre una panoramica completa e il controllo di tutti gli accessi e i servizi dei dipendenti.



Login automatico dipendenti

L'estensione del browser inserisce automaticamente le credenziali e il codice 2fa sui servizi mobili e desktop cloud.

Archivia e gestisci le password in sicurezza

Il gestore password ricorda e archivia password private e di lavoro in totale sicurezza.

Una soluzione semplice per un problema complesso

Combinando le funzionalità di password managent con le possibilità umane, con 2FA automatico e con una piattaforma centralizzata di gestione degli accessi, Uniqkey offre una soluzione semplice a un complesso problema di sicurezza informatica. I rischi di scarsa igiene delle password infatti, così come lo shadow IT e la mancanza di visibilità, verranno immediatamente ridotti man mano che la tua azienda riprende il controllo delle password e dei servizi e che trasforma i tuoi dipendenti nella tua più grande forza, con una soluzione che rende facile al tuo team fare la cosa giusta per la sicurezza.

Best Est. ROI WINTER 2023

Easiest To Use WINTER 2023

Easiest Setup WINTER 2023

Come Uniqkey protegge i tuoi servizi cloud, desktop e mobile

Per gli amministratori

Gestione delle identità e degli accessi

Sulla piattaforma IAM centralizzata di Uniqkey, gli amministratori hanno una panoramica completa e un controllo granulare dei servizi, degli account e degli accessi dei dipendenti dell'azienda.

Log di controllo che abilita la conformità

La conformità è semplificata con l'Audit Log di Uniqkey. Qui, gli amministratori possono supervisionare tutte le attività di accesso, individuare attività sospette e supervisionare gli accessi condivisi.

Licenze, Onboarding & Offboarding

L'onboarding e l'offboarding possono essere disordinati. Con Uniqkey, gli amministratori possono assegnare agli utenti i relativi diritti di accesso in pochi clic - e viceversa.

Restrizioni di accesso personalizzabili

Per massimizzare la sicurezza, tutti i privilegi di accesso degli utenti possono essere personalizzati per includere restrizioni IP, geografiche e specifiche del tempo.

Per i dipendenti

2FA Automatico

Con il riempimento automatico delle credenziali e l'autenticazione 2FA, accedi 4 volte più velocemente e puoi applicare 2FA su tutti gli accessi senza aggiungere attrito al loro flusso di accesso.

Gestore di password intuitivo

Il Password Manager di Uniqkey memorizza e salva in modo sicuro le password dei dipendenti e le compila automaticamente per loro quando devono utilizzarle.

Generatore di password integrato

Grazie al generatore di password, i dipendenti possono aggiornare la sicurezza delle loro password generandole ad alta resistenza in un istante.

Condivisione delle password facile e sicura

Con Uniqkey, individui e dipartimenti condividono le password tra loro senza rivelarle durante il processo - e per una durata limitata

Specifiche Tecniche

- Certificazione ISAE 3402 in base .ai controlli .ISO 27001
- Utilizza il protocollo Zero-Knowledge Proof & Secure Remote Password Protocol
- Tutti i dati sono crittografati off-line e localmente sui telefoni dei dipendenti
- I dati sono protetti dalla crittografia AES 256 e SHA-3
- Uniqkey non memorizza i dati personali e sensibili dei clienti
- Non abbiamo accesso alle credenziali
- 99.9% di tempo di attività SLA stabile
- Certificazione e revisione di terze parti
- Uniqkey esamina regolarmente gli audit e conduce una valutazione approfondita dei procesi di sicurezza attraverso consulenti esterni
- Supporto completo sia per i responsabili IT che per i dipendenti

Informazioni su Uniqkey

Uniqkey è una società danese di sicurezza informatica che aiuta centinaia di aziende europee a proteggersi dagli attacchi informatici relativi alle password. Fondata nel 2017, Uniqkey ora impiega più di 50 persone di talento provenienti da 6 nazionalità in 3 diversi paesi europei.

Gli architetti della sicurezza e i consulenti senior di HSBC Bank, VISA, UK Parliament e NNIT sono dietro il successo di Uniqkey e, grazie a molti anni di esperienza, il fondamento di Uniqkey si basa sullo sstate-of-the-art specializzato in infrastrutture, hosting, sicurezza e crittografia, che ha portato alla denominazione Deloitte Uniqkey "Imprenditore dell'anno per la sicurezza informatica" nel 2018. Tutti i dati sono crittografati localmente e protetti con la password principale nonché memorizzati sui propri telefoni. Uniqkey non ha accesso a dati o password e non può decrittografare i dati dell'utente o dell'azienda. La nostra soluzione è collaudata dai clienti attraverso approfonditi corsi POV.

G2 Best Est. ROI WINTER 2023

G2 Users Most Likely To Recommend WINTER 2023

G2 Top 50 Security Products BEST SOFTWARE AWARDS 2023

G2 Easiest To Use WINTER 2023

G2 Easiest Setup WINTER 2023

Una selezione di aziende europee che si affidano a Uniqkey

RISMA · Renaissance · astra* · OMG Omnicom MediaGroup · cips · energi ikast hele din forsyning · BORNHOLMS ENERGI & FORSYNING · CROP · CALJAN

Dati di contatto:
Email: hello@uniqkey.eu
Telefono: +45 71 96 99 67

Per saperne di più su Uniqkey o per richiedere una trial gratuita:
www.uniqkey.eu

uniqkey