



S

cose che i

CYBERCRIMINALI

ODIANO

e che i

CLIENTI

adorano

La sofisticazione dei cybercriminali conduce a un aumento esponenziale delle violazioni e delle frodi



Aumento del 35% delle violazioni dei dati tra il 2020 e il 2021¹

Nel primo quarter del 2022, le intrusioni sono aumentate di un ulteriore

14%

rispetto a 2021²



però

il
29%
dei CEO e dei CISO...



- ed il -

40%
dei CSO...



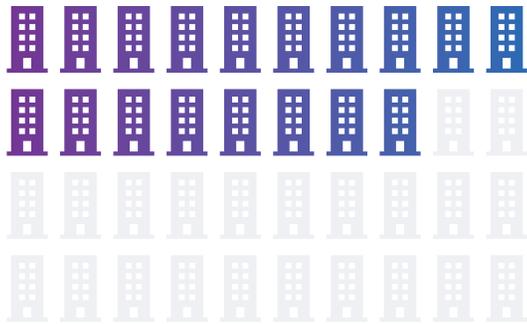
... riconoscono che le loro aziende non sono preparate ad affrontare un panorama di minacce in rapida evoluzione.³

“La prevista crescita dei dispositivi intelligenti, del 5G, dell’edge computing e dell’intelligenza artificiale promette di creare ancora più dati, nodi connessi e maggiori superfici di attacco”.

- Deloitte⁴

Qual è l'anello più debole in cybersecurity? L'identità digitale

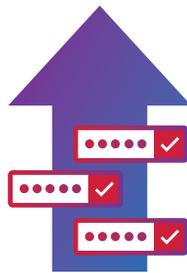
Per ridurre il rischio e proteggere gli utenti, le aziende stanno analizzando i loro ambienti IT alla ricerca di punti deboli. L'identità digitale è in cima alla lista.



Il **45%**
delle aziende ha subito
un'intrusione causata da
attacchi legati all'identità⁵

Il **50%**

delle violazioni di dati sono dovute ad accessi non autorizzati⁶



Gli attacchi di
acquisizione di
account (ATO) sono
aumentati del

307%

(2019 - 2021)⁷

Queste statistiche non sorprendono se si considera che la maggior parte delle aziende utilizza un mosaico di soluzioni interne, obsolete o realizzate ad hoc per la gestione delle identità e degli accessi digitali.

Il CIAM è LA soluzione

È ora di eliminare gli anelli deboli del sistema di gestione delle identità esistente. La gestione dell'identità e dell'accesso dei clienti (CIAM) è una soluzione essenziale per ridurre il rischio di violazione dei dati e di frode e per soddisfare i vostri clienti.

Ecco 3 funzionalità CIAM che i

CYBERCRIMINALI

ODIANO

ma che i

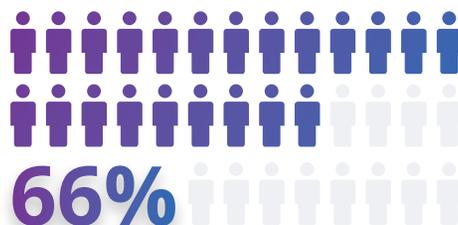
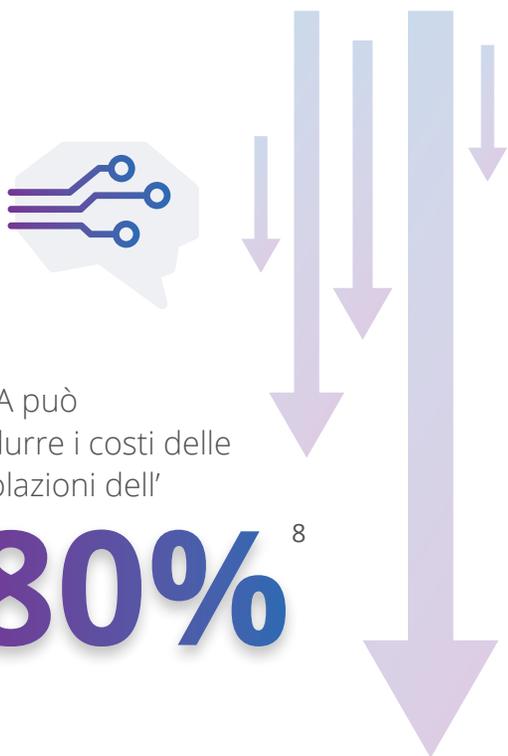
CLIENTI

adorano



1 Protezione contro le minacce e le frodi con l'AI

Utilizzando la potenza dell'intelligenza artificiale (AI) e dell'apprendimento automatico (ML) per il CIAM, è possibile identificare e contenere gli accessi non autorizzati, analizzare e ridurre i rischi di accesso e prevenire l'acquisizione di account (ATO).



Il 66% dei responsabili IT non crede di poter identificare le minacce critiche senza IA⁹



dei responsabili IAM considerano che "la valutazione del customer risk è di fondamentale importanza"¹⁰

I CYBERCRIMINALI **ODIANO**

I cybercriminali odiano quando è possibile rilevare le anomalie con l'intelligenza artificiale stratificata, tra cui l'analisi del comportamento di utenti ed entità (UEBA), che diventa sempre più intelligente nell'identificare la differenza tra il comportamento normale e i modelli di minaccia emergenti.

I clienti apprezzano l'eliminazione di inutili attriti, consentendo loro di contattare la vostra azienda in modo rapido e semplice.

I CLIENTI **adorano**

2 Autenticazione senza password e a più fattori (MFA)

L'autenticazione senza password elimina la necessità di password utilizzando uno standard aperto, FIDO2 WebAuthn, e la biometria. L'MFA autentica gli utenti utilizzando le loro credenziali e altri meccanismi, come le password monouso (OTP) e la biometria.



Il **61%**

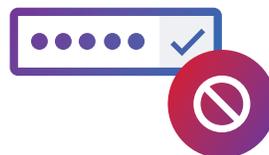
di tutte le violazioni di dati è il risultato di schemi che tentano di rubare le credenziali di accesso.¹¹

Il **43%**



dei responsabili della sicurezza che hanno subito un'intrusione affermano che l'implementazione dell'MFA per tutti gli utenti avrebbe fatto la differenza.¹²

Il **65%**



dei responsabili IAM afferma che l'autenticazione senza password è uno dei principali aspetti legati all'identità¹³

I CYBERCRIMINALI
ODIANO

I cybercriminali odiano il fatto che l'MFA impedisca loro di utilizzare le credenziali rubate per accedere agli accounts. Inoltre, non sopportano che l'autenticazione senza password protegga i sistemi e le applicazioni da ransomware, phishing e attacchi replay.

I clienti apprezzano che le aziende utilizzino l'autenticazione a più fattori (MFA) per proteggerli e combattere le frodi. Inoltre, piace l'idea di non dover più utilizzare un nome utente e una password.

I CLIENTI
adorano

3 Usurpazione di identità sicura per i call centers

L'usurpazione sicura consente ai clienti di concedere il controllo temporaneo del proprio account - ad esempio, attraverso una richiesta tramite un'applicazione mobile - a un altro utente, come un agente dell'helpdesk del call center, per un determinato periodo di tempo. Questa funzione aiuta i rappresentanti dei call centers ad interagire in modo più sicuro con i clienti e i loro dati.



~ || **85%**

delle violazioni di dati avvenute con successo ha coinvolto frodi umane piuttosto che lo sfruttamento di codici deboli.¹⁴

36%



di aumento delle perdite dovute alle frodi nei contact centers tra il 2018 e il 2020.¹⁵

|| **84%**



dei consumatori è più fedele alle aziende che offrono forti controlli di sicurezza.¹⁶

I CYBERCRIMINALI

OPDIANO

I cybercriminali non sopportano che gli agenti del call center non possano accedere a un account senza il consenso del legittimo proprietario tramite una richiesta.

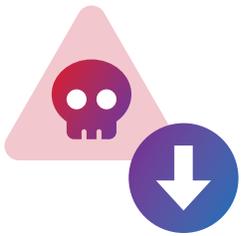
I clienti apprezzano la possibilità di controllare se un agente del call center può accedere al loro account e per quanto tempo.

I CLIENTI

adorano

Sicurezza, soddisfazione e risparmio con il CIAM ForgeRock

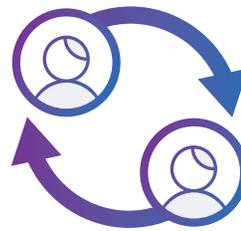
I clienti di ForgeRock hanno l'opportunità di ottenere un ritorno eccezionale sul loro investimento. Scegliendo il CIAM di ForgeRock, sarete in grado di :



Ridurre i casi di frode, il che significa **un risparmio di 4,7 milioni**¹⁷



Ridurre del **40%** le comunicazioni relative alla sicurezza con il call center, generando **24 milioni di profitto**¹⁸



Aumentare il customer engagement del **400%**¹⁹

Per saperne di più sulla protezione dei vostri clienti, leggete [**Come l'identità dei clienti protegge da violazioni e frodi: 6 modi in cui il CIAM migliora la cibersecurity riducendo i costi**](#)

“I principali vantaggi dell’investimento [di ForgeRock] sono: risparmi sull’infrastruttura esistente, riduzione dei rischi di frode e di sicurezza, diminuzione della complessità dell’IAM e del lavoro di sviluppo e, infine, risparmio sui costi grazie all’efficienza del call center e alla riduzione delle comunicazioni legate alla sicurezza.”

– Studio Forrester Total Economic Impact^{TM20}

ForgeRock

ForgeRock consente alle aziende in tutto il mondo di proteggere i propri clienti con l'unica piattaforma CIAM aziendale completa, usando l'intelligenza artificiale e progettata per tutte le identità e tutti i cloud.

FORRESTER®

Wave Leader per la gestione dell'identità e dell'accesso clienti

kuppingercoie
ANALYSTS

Leader globale per le piattaforme CIAM nel Leadership Compass Report

Gartner®

Leader nel Magic Quadrant per la gestione dell'accesso

Informazioni su FORGEROCK

ForgeRock®, (NYSE: FORG) è un leader globale nell'identità digitale, offrendo soluzioni complete e innovative di gestione dell'identità e dell'accesso che consentono ai clienti, dipendenti e oggetti di accedere in modo sicuro e facile al mondo connesso. Attraverso ForgeRock, migliaia di clienti in tutto il mondo orchestrano, gestiscono e proteggono l'intero ciclo di vita delle identità - dai controlli di accesso dinamici alla governance, dalle API all'archiviazione dei dati di autenticazione - in qualsiasi ambiente, fisico, cloud o ibrido. L'azienda ha operazioni in tutto il mondo e ha sede a San Francisco, in California. Per ulteriori informazioni e download gratuiti, visitate www.forgerock.com

Seguiteci



 **ForgeRock®**

Una piattaforma. Tutte le identità.

¹<https://www.forgerock.com/resources/2022-consumer-identity-breach-report>

²<https://www.cnet.com/tech/services-and-software/data-breaches-up-in-first-quarter-of-2022/>

³<https://thoughtlabgroup.com/cyber-solutions-riskier-world/>

⁴https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

⁵ESG eBook, [Securing the Identity Perimeter with Defense in Depth](#), March 2022

⁶<https://www.forgerock.com/resources/2022-consumer-identity-breach-report>

⁷<https://www.helpnetsecurity.com/2021/10/06/ato-attacks-increased/>

⁸<https://www.forgerock.com/resources/2022-consumer-identity-breach-report>

⁹<https://www.capgemini.com/gb-en/research/reinventing-cybersecurity-with-artificial-intelligence/>

¹⁰ESG eBook, [Securing the Identity Perimeter with Defense in Depth](#), March 2022

¹¹<https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/>

¹²<https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/>

¹³ESG eBook, [Securing the Identity Perimeter with Defense in Depth](#), March 2022

¹⁴<https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/>

¹⁵<https://www.datavisor.com/blog/contact-center-fraud-key-trends-and-challenges-for-2021/>

¹⁶<https://www.forbes.com/sites/blakemorgan/2020/06/22/50-stats-showing-why-companies-need-to-prioritize-consumer-privacy/?sh=6eb24ef737f6>

¹⁷<https://www.forgerock.com/resources/analyst-report/forrester-total-economic-impact>

