Proteggere Salesforce nel 2023

Identificare le minacce e le sfide

WITH secure

Introduzione

Il 2022 è stato un altro anno di grande fermento per la cyber security. Agli imponenti attacchi ai danni di importanti società e infrastrutture nazionali messi a segno da prolifici threat group come Lapsus$ e Conti si affianca la crescente minaccia di organizzazioni criminali di profilo più basso che utilizzano tattiche come il ransomware mirato.

I cyber attacchi vengono sferrati soprattutto attraverso sistemi IT ed endpoint tradizionali. Tuttavia, dato il numero crescente di aziende che trasferiscono l'infrastruttura e le operazioni nel cloud, gli ambienti basati sul cloud, come Salesforce, rappresentano il nuovo terreno di azione e attenzione per i threat actor.

La piattaforma Salesforce è stata scelta da più di 150.000 società per le loro attività CRM (Customer Relationship Management), per cui contiene grandi quantità di dati preziosi e sensibili dei clienti. Salesforce è anche una piattaforma altamente collaborativa e personalizzabile che supporta una vasta gamma di plug-in di terze parti e opzioni per la connettività.

La combinazione di questi fattori contribuisce a fare di Salesforce un obiettivo allettante per i threat actor. Anche se finora non si sono registrati casi significativi, riteniamo che sia solo una questione di tempo.

Salesforce è una piattaforma molto sicura che prevede un numero considerevole di controlli di sicurezza progettati per realizzare un luogo sicuro in cui archiviare i dati. Molti controlli, però, devono essere configurati correttamente dai clienti stessi per mettere al sicuro i loro dati, secondo il modello di responsabilità condivisa.

In questo report, tre esperti di sicurezza di Salesforce mettono in luce gli aspetti della sicurezza di Salesforce su cui è bene focalizzare l'attenzione il prossimo anno. La loro esperienza è supportata dai dati più recenti emersi da una ricerca di mercato di WithSecure™ sul cloud e sulla sicurezza di Salesforce nel 2022*.

Scopri i risultati della ricerca, quali sono le massime priorità per la sicurezza di Salesforce per il 2023 e cosa fare per prepararti adeguatamente e iniziare a ridurre il rischio.

Temi chiave per la sicurezza nel 2022

- I principali problemi di sicurezza per i professionisti IT e gli amministratori Salesforce
- La minaccia rappresentata dagli errori di configurazione e dagli asset non monitorati
- L'aumento dei file e degli URL malevoli in Salesforce
- L'identificazione dei giusti controlli di sicurezza
- Le nostre otto raccomandazioni principali per la protezione di Salesforce nel 2023

*Ricerca di mercato di WithSecure™: ricerca di mercato B2B su 3072 decision maker e influencer IT condotta tra aprile e maggio 2022 in 12 paesi: Regno Unito, Francia, Germania, Belgio/Paesi Bassi, Finlandia, Norvegia, Svezia, Danimarca, Stati Uniti, Canada e Giappone.

I nostri esperti

Dmitriy Viktorov
Head of Product and Technology, Cloud Protection, WithSecure™

Dmitriy è un professionista esperto di prodotti e sicurezza che mira a risolvere problemi complessi e ad aiutare i clienti a mantenere sicuri e protetti i loro servizi cloud e digitali. Ha ricoperto vari ruoli presso R&D, Product Management and Technology Office e attualmente è alla guida dello sviluppo di prodotto di Cloud Protection for Salesforce.

Pankaj Paryani
Salesforce Technical Lead, WithSecure™

Pankaj è uno sviluppatore e consulente esperto Salesforce che ha sviluppato diversi progetti per clienti negli Stati Uniti, nel Regno Unito e nelle regioni APAC. Di recente ha assunto l'incarico di guidare il team di sviluppo CRM presso WithSecure™ affinché le vendite e i servizi siano allineati alle esigenze dei clienti.

Doug Merrett
Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

Doug è un appassionato sostenitore della sicurezza che ha lavorato in Salesforce per 13 anni come Platform and Security Specialist nel Regno Unito e in Australia. In quegli anni ha aiutato molti clienti a comprendere l'approccio di Salesforce alla sicurezza e all'infrastruttura, aiutandoli a massimizzare la sicurezza dei dati archiviati nella piattaforma Salesforce. Nel giugno 2021, Doug ha avviato una propria attività di consulenza, Platinum7, concentrandosi esclusivamente su sicurezza, conformità e resilienza di Salesforce.

I principali problemi di sicurezza per i professionisti IT e gli amministratori Salesforce

5 principali problemi di sicurezza

1. Prevenzione dei data breach.
2. Protezione da malware e ransomware.
3. Rilevamento degli attacchi che potrebbero avere eluso altre misure di sicurezza.
4. Sicurezza delle applicazioni di collaborazione basate su cloud, come Office 365 e Salesforce.
5. Prevenzione delle minacce basate su email, quali phishing e Business Email Compromise (BEC).

* Cloud e collaborazione

Le piattaforme cloud come Salesforce sono diventate essenziali per supportare le strategie di lavoro da remoto e ibride che hanno preso piede con la pandemia e per coniugare i vantaggi in termini di aumento dell'efficienza e dell'agilità con la riduzione dei costi e delle risorse. Gli ambienti cloud, tuttavia, creano più gap e componenti mobili, molti dei quali esulano dal controllo diretto.

"Per decenni tutto è rimasto sotto il controllo diretto in locale, con un numero limitato di connessioni esterne a cui prestare attenzione. Oggi tutto è nel cloud e molti sistemi critici non vengono controllati direttamente."

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

Negli ultimi 18 mesi, quali sono stati i tre punti più critici nella gestione della sicurezza dei dati?

(Dal report Salesforce Top Security Trends for 2022)

* **59%** Gestione della sicurezza di terze parti

** **53%** Restare al passo con le normative di conformità

49% Sicurezza dei dispositivi mobili

38% Vincoli di risorse

37% Gestione delle vulnerabilità

28% Gestione delle misure proattive di prevenzione degli attacchi

15% Auditing

5% Comportamento degli utenti

* Gestione della sicurezza di terze parti

Salesforce è pensato per essere estremamente personalizzabile, per trovare e implementare facilmente le nuove funzionalità necessarie. Esistono più di 3.400 applicazioni solo su Salesforce AppExchange e innumerevoli API e plug-in di terze parti prontamente accessibili online. Se da un lato si tratta di un aspetto positivo dal punto di vista dell'integrazione e dell'accessibilità, dall'altro si crea una supply chain di terze parti che può rapidamente diventare incontrollabile. Ogni add-on aumenta la potenziale esposizione agli attacchi alla supply chain.

Gli attacchi alla supply chain hanno dominato il panorama generale della cyber security negli ultimi due anni, quindi non stupisce che si tratti di una problematica chiave per la sicurezza di Salesforce. Per saperne di più, leggi il nostro report sulla gestione di terze parti in Salesforce.

** Normative e conformità

Il panorama normativo si è evoluto costantemente e la conformità alle normative in materia di sicurezza e privacy è diventata sempre più complessa con l'accelerazione della digitalizzazione e della migrazione al cloud.

Nelle varie regioni esistono leggi ed enti normativi specifici e le aziende devono sapere esattamente dove vengono trasferiti, archiviati e trattati i propri dati. Devono anche prestare attenzione alle normative specifiche di settore, ad esempio quelle relative alla sanità e alla finanza.

E con l'introduzione di nuovi regolamenti e l'aggiornamento di altri, i cambiamenti in arrivo sono molti. La Commissione Europea sta per pubblicare la nuova direttiva NIS2 (Network and Information Systems), che dovrebbe entrare in vigore nei prossimi 18 mesi.

Quali sono le tue 3 principali preoccupazioni per la sicurezza IT?

Ransomware e phishing

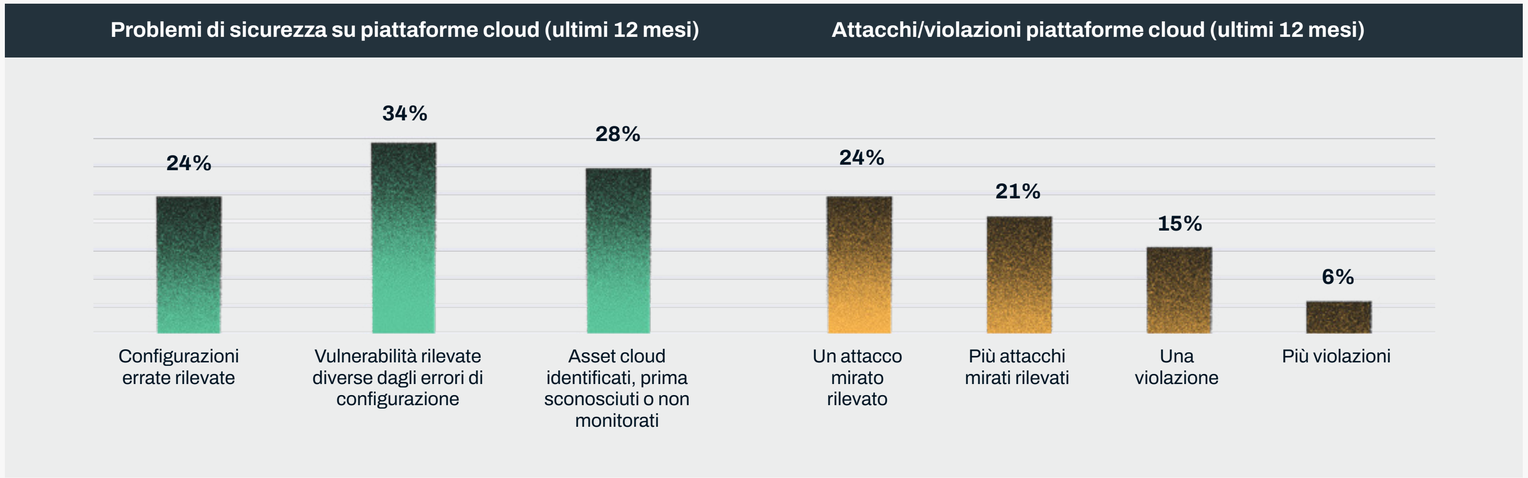
Tradizionalmente, il phishing è considerato una minaccia via email e gli attaccanti continuano effettivamente a usare l'email per questi attacchi. Salesforce non è purtroppo immune agli attacchi di phishing, dato che la piattaforma fornisce diversi flussi basati su email come Email-to-case o Email-to-Chatter. Inoltre, con Slack, Chatter e altre opzioni di terze parti, Salesforce offre numerosi canali di comunicazione e collaborazione che possono essere sfruttati negli attacchi di phishing.

Allo stesso modo, anche se l'ambiente Salesforce è di per sé piuttosto inaccessibile al ransomware standard, può essere sfruttato per inviare file e link malevoli ai sistemi target. È anche importante tenere presente che il ransomware e altri programmi malevoli si evolvono rapidamente. Le funzionalità di comunicazione altamente flessibili di Salesforce potrebbero rappresentare un'opportunità per queste minacce di nuova generazione.

Visibilità e controllo degli accessi

Sulla base della loro esperienza, i nostri esperti hanno evidenziato anche l'importanza della visibilità e del controllo delle connessioni di rete. Le aziende devono comprendere a fondo il modo in cui gli utenti interni ed esterni possono accedere ai dati e ai sistemi critici e il modo in cui la piattaforma Salesforce si connette e interagisce con altri sistemi.

La minaccia rappresentata dagli errori di configurazione e dagli asset non monitorati



Il fatto che un quarto degli intervistati ritenga di avere subito un attacco mirato negli ultimi 12 mesi dimostra che gli attaccanti sono diventati più sofisticati e organizzati. Molte organizzazioni, però, stanno facilitando loro la vita non configurando o monitorando correttamente gli ambienti cloud.

Le configurazioni errate sono particolarmente diffuse perché per un ambiente cloud medio esistono innumerevoli opzioni. Gli errori di configurazione di Salesforce più comuni che abbiamo rilevato riguardano l'accesso. Agli utenti e alle applicazioni viene spesso lasciato il livello di autorizzazioni predefinito che concede un accesso privilegiato di alto livello alla piattaforma. Questo aumenta notevolmente il rischio derivante da threat actor esterni e insider malintenzionati, lasciando anche più spazio per l'errore umano.

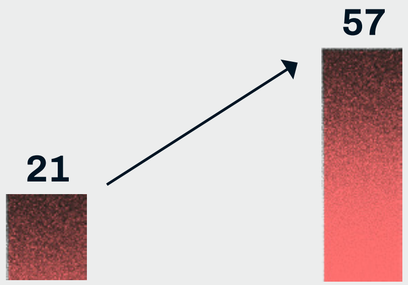
Oltre a questo, le organizzazioni spesso faticano a tenere traccia dei loro sistemi. Il modello Software-as-a Service (SaaS) fa sì che i dipendenti possano acquistare e implementare nuovi componenti e applicazioni in modo estremamente facile, all'insaputa del reparto IT. Di conseguenza, spesso in Salesforce sono presenti moltissimi elementi che non sono stati adeguatamente controllati e non vengono monitorati per rilevare eventuali vulnerabilità o attività sospette.

“La complessità è nemica della sicurezza. Più l'ambiente è complesso, più è probabile che qualcosa venga trascurato e non venga configurato correttamente. Essendo una piattaforma altamente personalizzabile, Salesforce presta il fianco agli errori di configurazione.”

Dmitriy Viktorov, Head of Product and Technology, Cloud Protection, WithSecure™

I file e gli URL malevoli in Salesforce sono in aumento

Rilevamenti di file/URL per cliente al mese



Negli ultimi 6 mesi, il volume di file e URL malevoli rilevati è cresciuto del 250%

Primi 5 rilevamenti e tipi di file dannosi

1. File HTML 49 %
2. Archivi RAR/ZIP 23 %
3. File Microsoft Office 10%
4. File exe/com 4 %
5. File PDF 3%

*ultimi 6 mesi

Primi 5 tipi di malware:

1. Trojan 54%
2. Adware 15%
3. Exploit 12%
4. Altro 12%
5. Downloader 2%

*ultimi 6 mesi

È risaputo che il numero di tentativi di attacco è in costante aumento e questa tendenza è chiaramente suffragata dai dati di WithSecure™ sul monitoraggio degli ambienti Salesforce. Negli ultimi sei mesi abbiamo rilevato una media di 57 file o URL malevoli per cliente al mese. Si tratta di un aumento del 274% rispetto alla media del semestre precedente.

I file HTML malevoli sono il metodo di attacco più diffuso e rappresentano più della metà dei file che abbiamo rilevato. Tra gli attacchi basati su malware che abbiamo identificato, la maggior parte riguardava malware di tipo Trojan.

Sono anche emerse diverse tendenze che sembrano indicare che i threat actor concentrano l'attenzione sugli asset Salesforce da attaccare. Ad esempio, se un cliente implementa Salesforce Experience Cloud e crea un portale per il caricamento di contenuti, subito dopo si verifica un rapido aumento del numero di file e URL rilevati.

Degno di nota è anche il fatto che vengono rilevati più URL malevoli che file. Gli attaccanti sanno che un numero maggiore di aziende ha implementato solide strategie incentrate sulla scansione dei file e hanno adottato l'approccio più versatile e più difficile da rilevare degli URL.

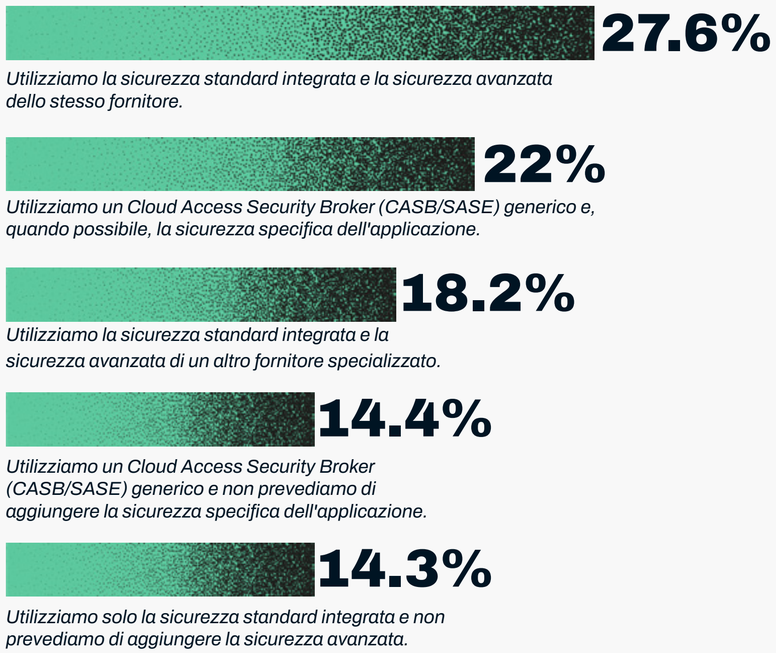
“Tutti sanno esaminare i sistemi alla ricerca di file malevoli, ma la scansione degli URL non è ancora una pratica standard, soprattutto al di fuori dell'email.”

Doug Merrett, specialista in sicurezza, conformità, privacy e resilienza di Salesforce, Platinum7

Trovare i giusti controlli di sicurezza

Quali delle seguenti affermazioni sulla sicurezza delle applicazioni cloud si adattano meglio alla tua azienda/organizzazione?

(es. Office 365, Google Workspace, Salesforce)



La nostra ricerca ha messo in luce una situazione eterogenea per quanto riguarda le funzionalità di sicurezza del cloud. La maggior parte degli intervistati usa un mix di applicazioni di sicurezza specializzate, ma moltissimi fanno affidamento solo sulle funzionalità di sicurezza native dell'applicazione o piattaforma.

Questi strumenti integrati sono un buon punto di partenza e spesso offrono il vantaggio di essere costruiti dal fornitore dell'applicazione. Di solito, però, lasciano alcuni gap rilevanti. Ad esempio, Salesforce non offre sicurezza per i dati non strutturati e non dispone di una funzionalità nativa per la scansione dei contenuti caricati e scaricati.

Le aziende dovrebbero combinare le funzionalità di sicurezza native e i servizi Salesforce interni con strumenti di sicurezza specializzati di almeno un fornitore per colmare le lacune. Inoltre, dovrebbero cercare di coprire tutte le risorse con soluzioni di un unico fornitore, laddove possibile. L'impiego di soluzioni di fornitori diversi può essere difficile da gestire perché costringe i team a confrontarsi con più flussi di dati e avvisi di minacce scollegati.

Se si sceglie un Cloud Access Security Broker (CASB), quelli che agiscono da proxy possono essere più difficili da implementare in quanto devono essere configurati specificamente per ogni prodotto SaaS. I CASB basati su API o le soluzioni integrate in modo nativo si rivelano più versatili e utili.

"Gli strumenti integrati dei fornitori raramente coprono tutto, ma possono essere molto efficaci, dato che gli sviluppatori conoscono a fondo il sistema. L'inserimento di un altro strumento specializzato aggiungerà equilibrio e colmerà le eventuali lacune."

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

Le nostre otto raccomandazioni per la protezione di Salesforce nel 2023

L'analisi dei dati chiave del 2022 aiuta a delineare le massime priorità di sicurezza per l'anno prossimo. Ecco cosa raccomandano i nostri esperti in vista del 2023 e oltre.

1. Gestire le identità e gli accessi

Concentrarsi sulla gestione degli accessi al sistema è una delle soluzioni più affidabili e rapide. L'autenticazione a più fattori (MFA) ridurrà il rischio di violazioni in modo immediato e significativo e, facendo ora parte della dotazione standard di Salesforce, può essere implementata rapidamente e senza costi aggiuntivi.

Al contempo, una strategia di accesso al sistema basata sui privilegi minimi sia per gli utenti che per l'integrazione delle API ridurrà notevolmente la superficie di attacco. È un processo più lento, ma è estremamente importante.

2. Monitorare le minacce in ingresso in Salesforce

I threat actor stanno espandendo le loro strategie di attacco oltre l'email. La funzione di caricamento dei contenuti di Salesforce e i canali di comunicazione integrati come Chatter possono essere sfruttati per attacchi di tipo malware e phishing, ma la piattaforma non include funzionalità native per il monitoraggio dei contenuti. WithSecure™ Cloud Protection for Salesforce è stato progettato in collaborazione con Salesforce per esaminare tutti i contenuti in ingresso e in uscita in tempo reale e identificare e bloccare i file e gli URL malevoli.

3. Restare al passo con le normative in materia di privacy e conformità

Il panorama normativo è in continua trasformazione e, dato il numero così elevato di componenti mobili nell'ambiente Salesforce, tenere traccia della conformità può essere un compito complesso. L'adozione del principio del privilegio minimo, che prevede un accesso minimo per impostazione predefinita, sarà estremamente funzionale a garantire la conformità. Per quanto riguarda le normative che si estendono a terze parti, è necessario implementare un controllo rigoroso per coprire le connessioni e le responsabilità.

4. Non sprecare gli strumenti integrati

Salesforce include tutta una serie di utilissimi strumenti integrati, che è bene sfruttare al meglio prima di iniziare a investire in soluzioni di terze parti. Due di questi strumenti, Health Check e Optimizer, possono essere particolarmente utili per evidenziare rapidamente eventuali configurazioni errate o controlli di accesso troppo blandi.

“Salesforce si adopera per tenere al sicuro la propria infrastruttura, ma gli utenti devono riconoscere le proprie responsabilità riguardo la protezione delle proprie istanze. I giorni in cui Salesforce non è oggetto di attacchi sono agli sgoccioli, non c'è tempo da perdere.”

Doug Merrett, specialista in sicurezza, conformità, privacy e resilienza di Salesforce, Platinum7

“Il monitoraggio efficace degli utenti è imprescindibile. Non solo aiuterà a scovare i threat actor e gli insider malintenzionati, ma anche a rilevare incidenti e configurazioni errate.”

Doug Merrett, specialista in sicurezza, conformità, privacy e resilienza di Salesforce, Platinum7

5. Eseguire il backup dei backup

I backup affidabili sono una delle risorse più preziose per migliorare la resilienza. La possibilità di ripristinare un'istanza di Salesforce riduce drasticamente l'impatto degli attacchi come il ransomware che mirano a danneggiare o distruggere i dati del CRM. I backup aggiungono anche un ulteriore livello di protezione dall'errore umano, permettendo di effettuare un reset nel momento in cui gli errori di configurazione o un'integrazione di app non corretta iniziano a causare problemi.

6. Procedere con due diligence

Man mano che l'ambiente Salesforce si espande, diventa essenziale attuare i processi di due diligence in modo scrupoloso. Quando si decide di implementare una nuova applicazione o un plug-in di terze parti, è importante indagare sul fornitore e verificare se è affidabile e credibile. Un buon punto di partenza è rappresentato dai report accurati che la solerte community lascia sullo store AppExchange. Le recensioni sono aggiornabili, quindi è bene verificare se ci sono state delle modifiche nel tempo.

7. Abilitare il monitoraggio degli eventi

Il monitoraggio degli eventi è fondamentale per comprendere ciò che accade all'interno dell'ambiente Salesforce e scoprire in che modo gli utenti e le applicazioni accedono e interagiscono con i dati critici. Questa visibilità è fondamentale per proteggere la piattaforma Salesforce dai tentativi di attacco dall'esterno e dai rischi interni, siano essi intenzionali o meno.

Questi dati di indagine forense, però, sono utili solo se vengono adeguatamente assimilati e compresi; esistono strumenti che consentono di tenere tutto sotto controllo, ad esempio Splunk e Imprivata FairWarning.

8. Mettere al sicuro i dati sensibili

I dati di business sono di vitale importanza e vanno protetti. Occorre però prestare particolare attenzione ai dati sensibili e alle informazioni dei clienti. Salesforce Shield o altre soluzioni di terze parti consentono di trovare, crittografare, monitorare e conservare i dati sensibili.

“Salesforce migliora costantemente la sua capacità di contrastare le minacce come il phishing incorporando nuove funzioni integrate, ma gli utenti devono fare la loro parte, implementando e utilizzando correttamente questi strumenti.”

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

“Gli attacchi alla supply chain sono un grande problema da due anni a questa parte e lo rimarranno anche il prossimo anno. È di primaria importanza che le organizzazioni comprendano e proteggano gli ambienti digitali estesi.”

Dmitriy Viktorov, Head of Product and Technology, Cloud Protection, WithSecure™

WithSecure™ Cloud Protection for Salesforce completa le funzionalità di sicurezza native di Salesforce mitigando i rischi associati ai file e agli URL caricati.

Contattaci

salesforce PARTNER SINCE 2016

Fonti dei dati

Lo studio WithSecure™ 2022 B2B Market Research ha coinvolto 3072 persone in un sondaggio online realizzato nel mese di maggio 2022 in 12 paesi, 9 dei quali in Europa (Regno Unito, Francia, Germania, Belgio, Paesi Bassi, Danimarca, Finlandia, Norvegia, Svezia), 2 in Nord America (Stati Uniti e Canada) e in Giappone. Tutti gli intervistati sono decision maker e influencer in ambito sicurezza IT/Reti/Cloud per l'acquisto di prodotti e servizi di sicurezza IT/Network/Cloud nelle rispettive organizzazioni.

I numeri e i trend sui rilevamenti di file e URL malevoli sono stati raccolti da WithSecure™ sulla base di dati interni anonimizzati relativi alle richieste di analisi delle minacce ricevute da ambienti Salesforce protetti.

Top Security Data Trends for 2022 di Salesforce: in base a un sondaggio su 300 dirigenti InfoSec e IT condotto da Salesforce e Pulse.

Chi siamo

WithSecure™, precedentemente F-Secure Business, è il partner di riferimento per la cyber security. Provider di servizi IT, MSSP e aziende, insieme alle più importanti istituzioni finanziarie, imprese manifatturiere e migliaia di fornitori dei più avanzati sistemi di comunicazione e tecnologie nel mondo si affidano a noi per conseguire una sicurezza informatica basata sui risultati, che protegge e consente le loro operazioni. La nostra protezione guidata dall'IA protegge gli endpoint e la collaborazione nel cloud e il nostro sistema di intelligent detection and response è alimentato da esperti che identificano i rischi aziendali tramite threat hunting proattivo e affrontano gli attacchi in tempo reale. I nostri consulenti collaborano con imprese e tech challenger per costruire la resilienza attraverso una consulenza sulla sicurezza basata su prove concrete. Con oltre 30 anni di esperienza nella costruzione di tecnologie che soddisfano gli obiettivi aziendali, abbiamo costruito il nostro portfolio per crescere insieme ai nostri partner attraverso modelli commerciali flessibili.

WithSecure™ Corporation è stata fondata nel 1988 ed è quotata sul listino NASDAQ OMX Helsinki Ltd.

W / T H®
secure