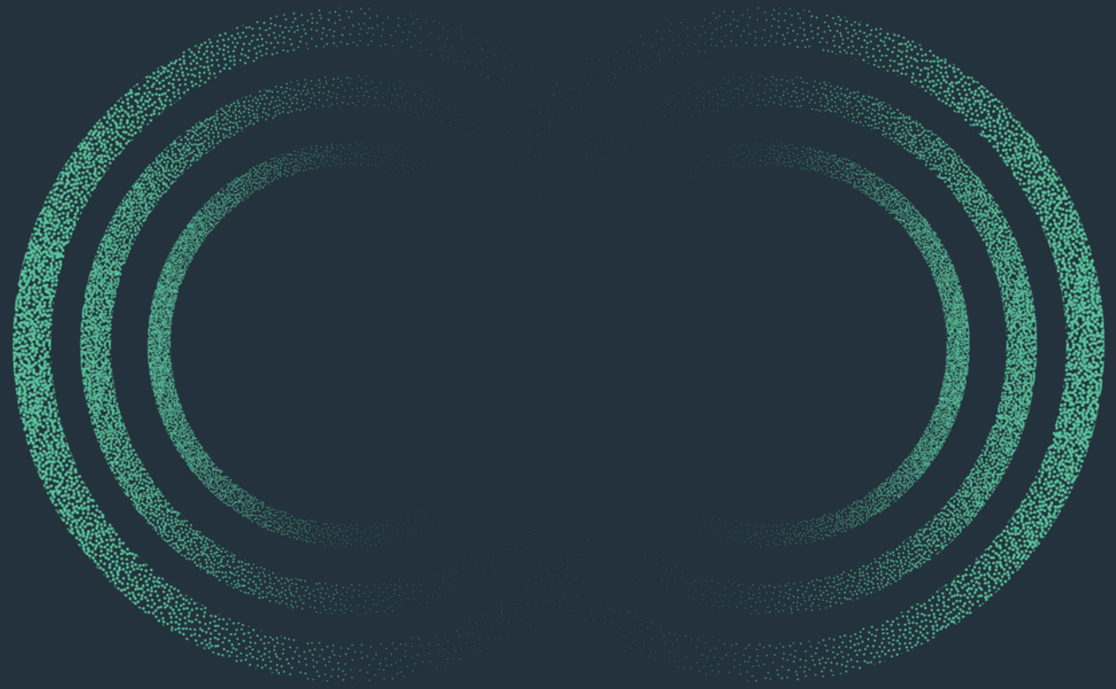
WithSecure™ Pulse 2023

Tutto ciò che c'è da sapere sulle ultime tendenze in ambito IT e cyber security

W / T H®
secure

Indice



Sintesi

Introduzione

Per la nostra ricerca di mercato globale abbiamo posto a migliaia di professionisti dell'IT una serie di domande riguardo il loro lavoro, le organizzazioni e le priorità per l'anno a venire. I dati così raccolti possono essere usati per dare forma alle tue strategie di sicurezza per il 2023 e oltre.

Pulse 2023 ha intervistato 3072 persone in 12 paesi: Regno Unito, Francia, Germania, Belgio, Paesi Bassi, Danimarca, Finlandia, Norvegia, Svezia, Stati Uniti, Canada e Giappone. Tutti gli intervistati erano decision maker nel campo della sicurezza ed influencer nei settori IT, network e cloud, responsabili dell'acquisto di prodotti e servizi di sicurezza IT per le loro organizzazioni.

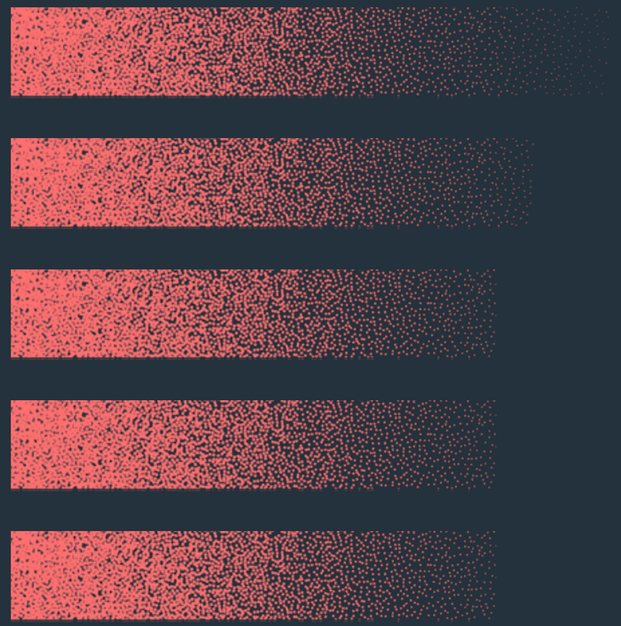
Per ottenere le informazioni più utili per te, usa le nostre funzionalità di personalizzazione per vedere i dati che riguardano il tuo settore, la tua regione e il tuo ruolo.

Priorità di sicurezza per il 2023

I partecipanti al nostro sondaggio ci hanno riferito quali sono le loro principali priorità commerciali e tecniche per i prossimi 12 mesi. Le prime cinque priorità per i leader della cyber security sono:

Il nostro articolo di approfondimento sulle priorità di sicurezza (a partire da pagina 10) delinea le tendenze che abbiamo osservato nel nostro sondaggio Pulse 2023.

Principali sfide tecniche di sicurezza (Prime 5 risposte)



34% Prevenire i data breach

29% Garantire protezione da malware e ransomware

27% Garantire la sicurezza delle applicazioni di collaborazione basate su cloud, come Office 365 e Salesforce

27% Prevenire le minacce avanzate basate su email, come phishing o business email compromise (BEC)

26% Garantire la sicurezza di un pool di dispositivi, servizi e software sempre più vario

“L’aspetto interessante è che le opzioni che nessuno sceglie tra le sue priorità sono quelle che fanno maggiormente la differenza quando si parla di profilo di sicurezza; per esperienza, queste sono le competenze e le pratiche che mancano a molte organizzazioni.”

Peter Page, Head of Solution Consulting presso WithSecure™

Spesa per la sicurezza

In tutti i discorsi sulla cyber security, forse la questione più importante per le aziende è la riga finale del bilancio. Quanto dobbiamo spendere per la sicurezza? È mai abbastanza? Dipende da quante postazioni abbiamo, dalla posizione geografica o dal mercato in cui operiamo? Anche i miei colleghi si preoccupano di quanto spendono? E quanto del loro budget è destinato a questo aspetto?

La nostra ricerca ha fornito informazioni interessanti su come le organizzazioni spendono per la cyber security. I dati suggeriscono che man mano che le aziende sviluppano la propria strategia, il costo diventa un fattore meno critico.

L' 86% degli intervistati afferma che il budget che intende destinare alla sicurezza aumenterà nei prossimi 12 mesi.

"Dico sempre che si dovrebbe iniziare con un minimo del 5%. Ma ovviamente quanto più importante è la sicurezza per il cliente, tanto maggiore sarà la percentuale. E viceversa."

Teemu Myllykangas, Director, B2B Product Management presso WithSecure™

"Le aziende devono decidere il livello di sicurezza desiderato. Devono concordare su quanto rischio siano disposte ad accettare, sul livello di interruzione di business che possono tollerare e quale sia la loro propensione al rischio. Sulla base di questi parametri, si possono prendere decisioni razionali sulla spesa di sicurezza."

Paul Brucciani, Head of Product Marketing presso WithSecure™

Residenza dei dati

Il nostro sondaggio Pulse del 2023 ha dimostrato che gli addetti IT hanno opinioni precise riguardo a dove i dati delle loro organizzazioni sono conservati e trattati. Questo non sorprende visto che le norme e i regolamenti sui dati, nonché moltissimi esempi di uso improprio o abuso di dati, rendono infatti tale argomento importante per molti.

Le opinioni tendono a differire tra persone di organizzazioni di dimensioni diverse o che lavorano in regioni o settori diversi.

Quando ci sono opinioni così diverse su quale sia il modo giusto di gestire i dati, come si può raggiungere un consenso? Può la politica di residenza dei dati di un'organizzazione influenzare il suo rapporto con i clienti? Molto spesso i responsabili della privacy esercitano una notevole influenza.

Forse la questione più importante è perché esistono differenze di opinione. Il disaccordo e le incomprensioni possono essere causa di problemi, in particolare tra gli influencer IT e i responsabili delle decisioni all'interno della stessa organizzazione. Quando si parla di privacy e protezione, non esiste alcun margine di errore.

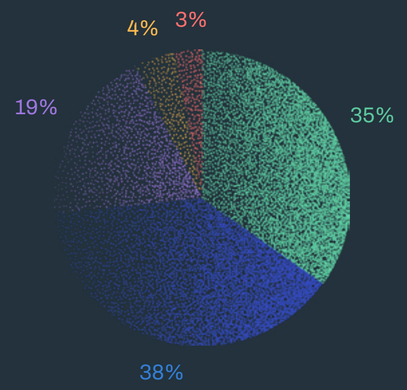
"La residenza dei dati è un aspetto che al giorno d'oggi, come azienda, devi prendere in considerazione. Il motivo è che potresti avere clienti che si preoccupano delle questioni di sicurezza nazionale e tu, in quanto start-up, per esempio, potresti aver fornito il tuo software "as a service" utilizzando provider di servizi cloud americani. Puoi continuare a farlo, puoi continuare a innovare con lo stesso ritmo di prima, o devi trovare una soluzione alternativa? È un aspetto che devi prendere in considerazione."

Albert Koubov Gonzalez, Consultant, WithSecure™

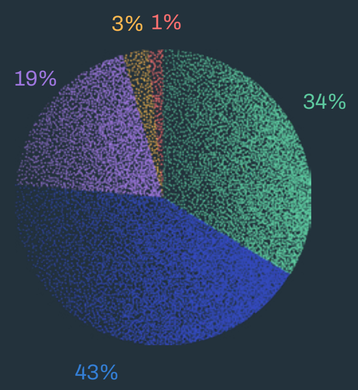
Dove conservi i dati

Quanto è importante il luogo geografico per l'elaborazione dei dati nel tuo ruolo?

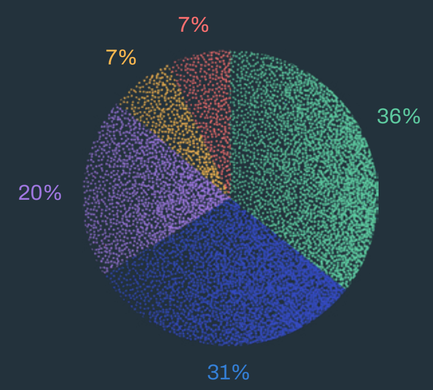
Totale



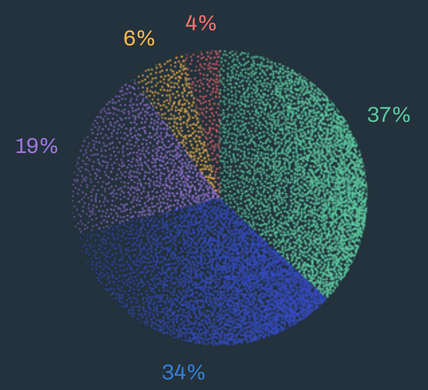
Decision maker IT



Influencer IT



Top management



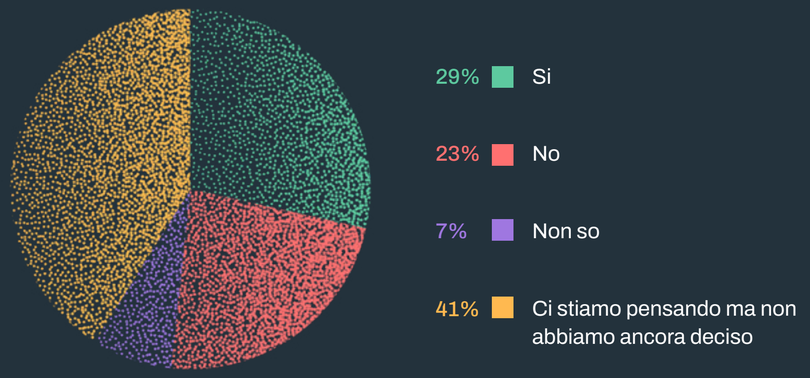
- I dati devono essere elaborati nello stesso paese delle attività operative
- I dati devono essere elaborati nella stessa regione (ad es. UE, Nord America, APAC) delle attività operative
- Non ha importanza dove elaboriamo i dati dei clienti finali a condizione che siano rispettati tutti i requisiti legali e di conformità
- Non elaboriamo dati per i consumatori finali
- Non so

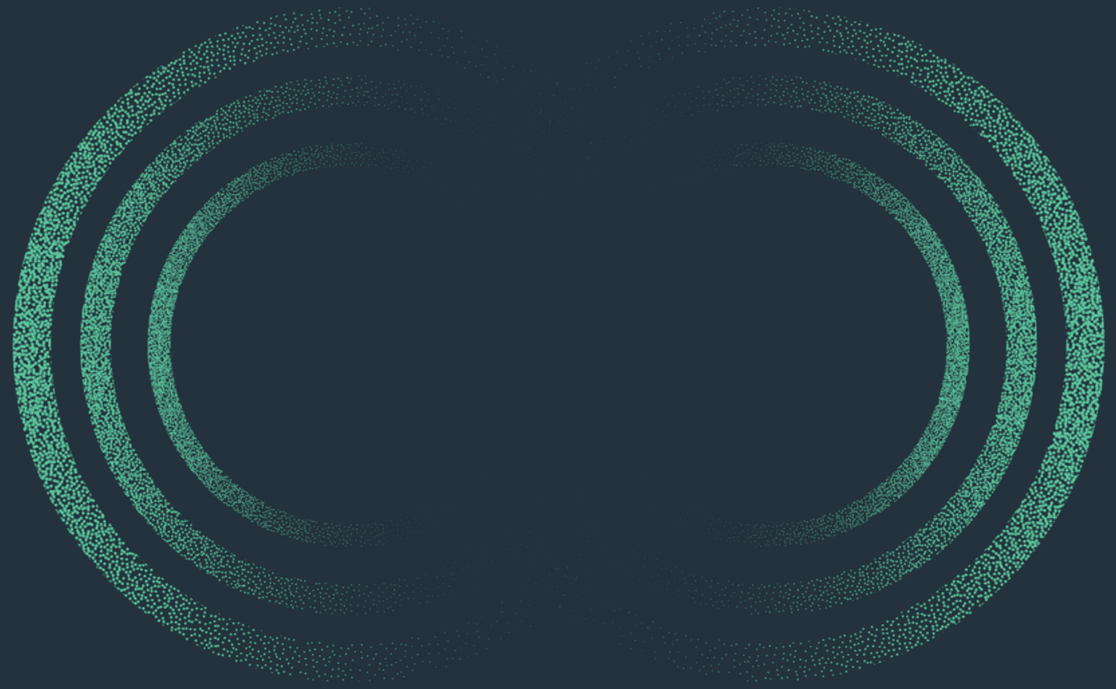
Migrazione dei vendor

Cambiare il vendor della sicurezza è un'impresa molto impegnativa. È un grandissimo investimento di tempo e risorse. Nonostante ciò, il nostro sondaggio Pulse 2023 indica che oltre il 30% degli intervistati ha cambiato vendor negli ultimi sei mesi, mentre la stessa percentuale ha in programma di cambiare vendor nei prossimi sei mesi.

Ciò indica che è in atto un'enorme ondata di migrazione dei vendor. Perché e quale sarà il costo?

La tua azienda/organizzazione ha in programma di cambiare la soluzione di sicurezza IT o il vendor nei prossimi sei mesi?

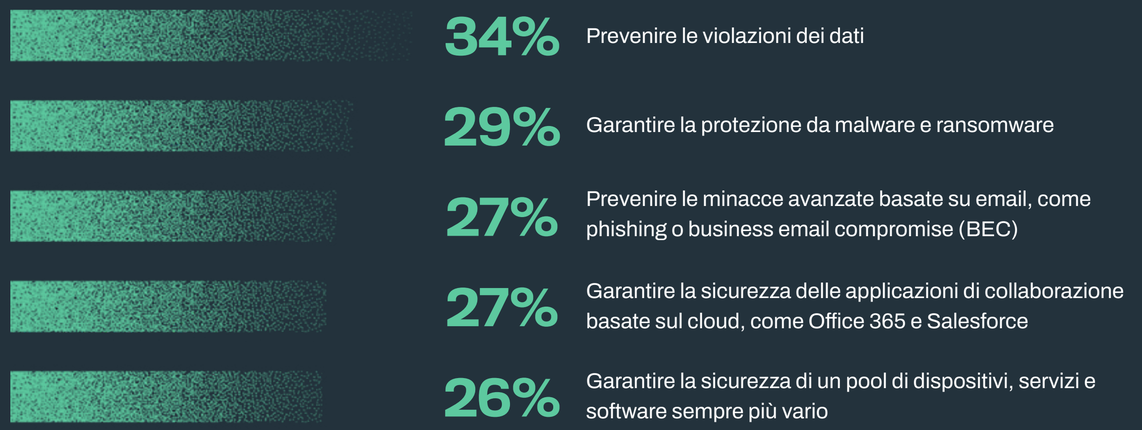




1.Priorità di sicurezza per il 2023

Priorità tecniche di sicurezza

Principali priorità tecniche di sicurezza



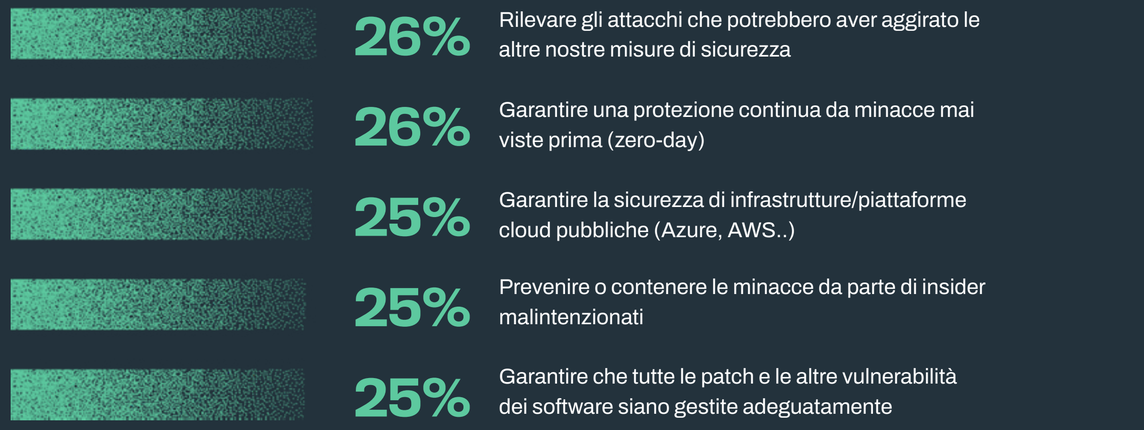
34% Prevenire le violazioni dei dati

29% Garantire la protezione da malware e ransomware

27% Prevenire le minacce avanzate basate su email, come phishing o business email compromise (BEC)

27% Garantire la sicurezza delle applicazioni di collaborazione basate sul cloud, come Office 365 e Salesforce

26% Garantire la sicurezza di un pool di dispositivi, servizi e software sempre più vario



26% Rilevare gli attacchi che potrebbero aver aggirato le altre nostre misure di sicurezza

26% Garantire una protezione continua da minacce mai viste prima (zero-day)

25% Garantire la sicurezza di infrastrutture/piattaforme cloud pubbliche (Azure, AWS..)

25% Prevenire o contenere le minacce da parte di insider malintenzionati

25% Garantire che tutte le patch e le altre vulnerabilità dei software siano gestite adeguatamente

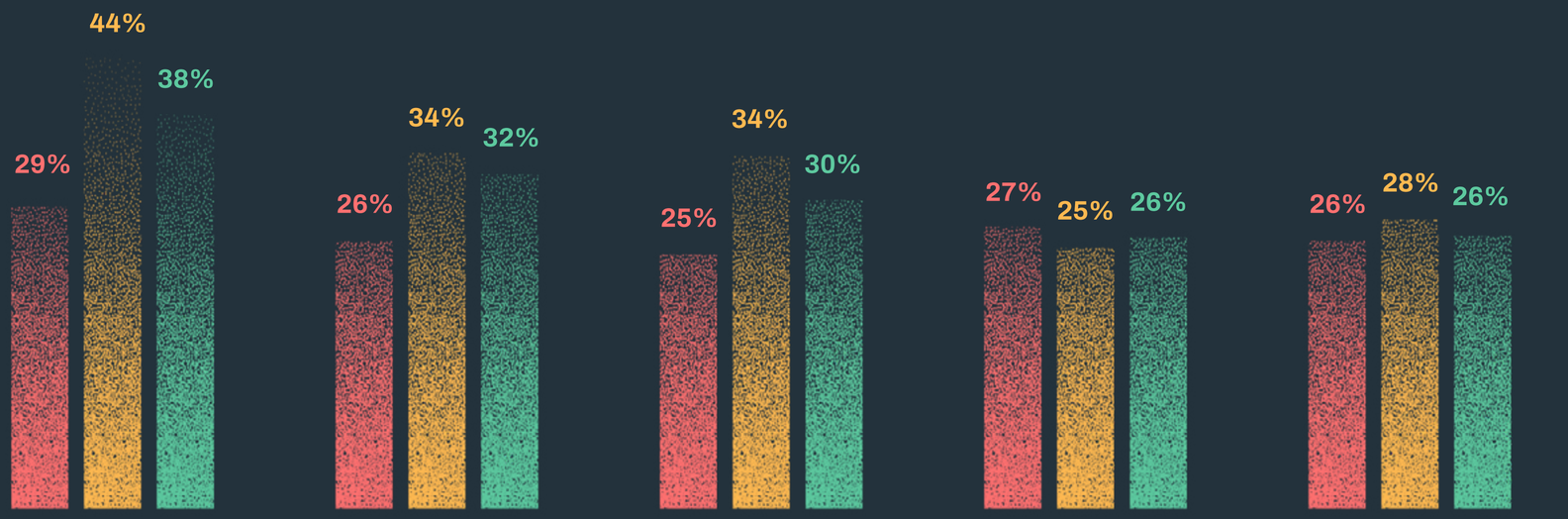
I risultati mostrano un ampio consenso su quali siano le priorità tecniche più urgenti. La sfida principale è, come era prevedibile, "prevenire le violazioni dei dati" (33,7 %). Anche prevenire minacce basate su email e garantire la sicurezza delle applicazioni di collaborazione basate sul cloud, come Office 365 e Salesforce, è in cima alla lista. Le altre priorità scelte in genere riguardano il rilevamento e la risposta alle minacce.

"L'aspetto interessante è che le cose che fanno maggiormente la differenza per quanto riguarda il profilo di sicurezza non compaiono nella lista e queste sono, secondo la nostra esperienza, competenze e pratiche che mancano a molte organizzazioni. Tutti si preoccupano di prevenire gli attacchi usando soluzioni come EDR e consulenza, ma entrambe sono cruciali. L'EDR deve essere implementata accanto all'EPP per creare una soluzione inoppugnabile. Inoltre, le attività "business as usual" che hanno un impatto duraturo sono trascurate perché spesso devono essere seguite internamente e comportano un lavoro veramente difficile: la creazione di una cultura della sicurezza non si può delegare ad altri."

— Peter Page, Head of Solution Consulting presso WithSecure™

Prime 5 sfide tecniche 2022/3 divise per tipo di ruolo

Questi dati mostrano le percentuali attribuite alle prime cinque priorità tecniche da parte di decision maker IT, influencer IT e top management nel 2023. Ancora una volta sembra esserci un accordo generale tra i nostri intervistati su quali siano le principali priorità in questo momento. Le discrepanze invece (per esempio tra decisori IT e influencer IT sulla “prevenzione dei data breach”), meriterebbero un’analisi più approfondita per assicurarsi che tutti i componenti del team di sicurezza siano sulla stessa linea.



Prevenire i data breach

Garantire la protezione da malware e ransomware

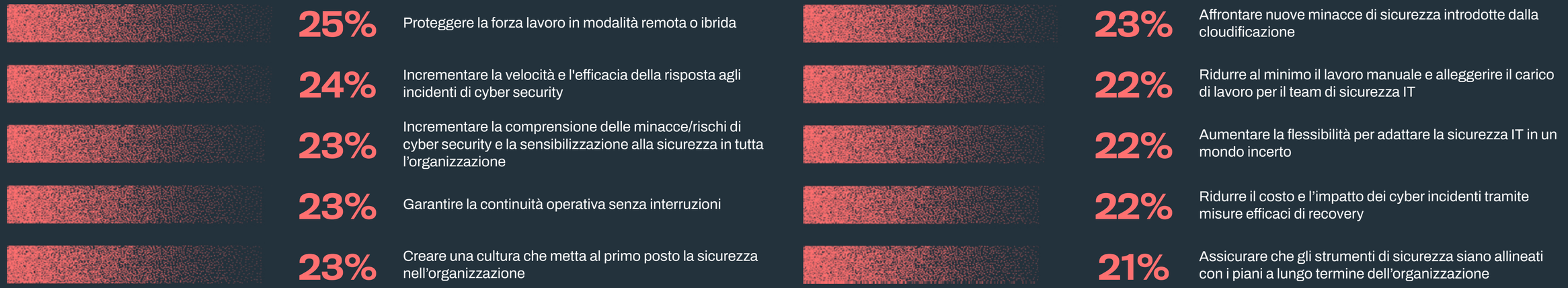
Prevenire le minacce avanzate basate su email, come phishing o business email compromise (BEC)

Garantire la sicurezza delle applicazioni di collaborazione basate sul cloud, come Office 365 e Salesforce

Garantire la sicurezza di un pool di dispositivi, servizi e software sempre più vario

Risultati della sicurezza aziendale

Principali sfide aziendali



25% Proteggere la forza lavoro in modalità remota o ibrida

24% Incrementare la velocità e l'efficacia della risposta agli incidenti di cyber security

23% Incrementare la comprensione delle minacce/rischi di cyber security e la sensibilizzazione alla sicurezza in tutta l'organizzazione

23% Garantire la continuità operativa senza interruzioni

23% Creare una cultura che metta al primo posto la sicurezza nell'organizzazione

23% Affrontare nuove minacce di sicurezza introdotte dalla cloudificazione

22% Ridurre al minimo il lavoro manuale e alleggerire il carico di lavoro per il team di sicurezza IT

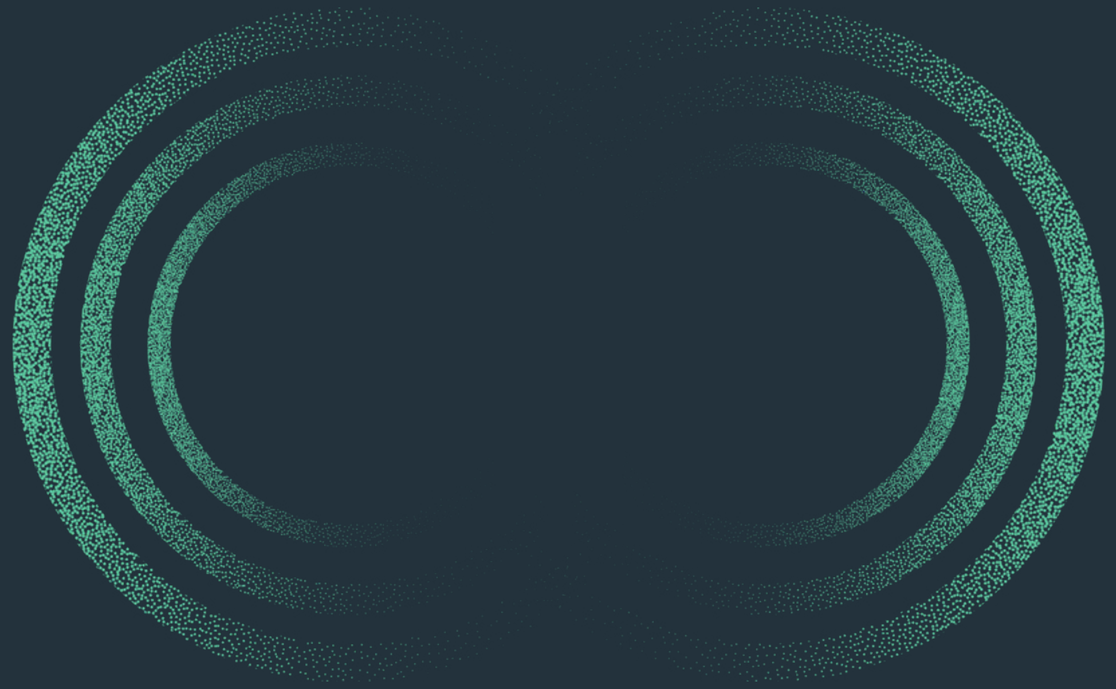
22% Aumentare la flessibilità per adattare la sicurezza IT in un mondo incerto

22% Ridurre il costo e l'impatto dei cyber incidenti tramite misure efficaci di recovery

21% Assicurare che gli strumenti di sicurezza siano allineati con i piani a lungo termine dell'organizzazione

"Non sorprende che ci si preoccupi soprattutto di proteggere i lavoratori in remoto. Nel 2020 si è verificato un cambiamento epocale delle modalità di lavoro e abbiamo visto una grande quantità di linee guida e consigli in questo settore per aiutare le organizzazioni ad adattarsi. Per molte persone tutto ciò ha comportato progetti su larga scala, che riguardavano un cambiamento dell'architettura IT (per esempio la migrazione su cloud) e la formazione degli impiegati. Ma anche se al momento questa è una delle preoccupazioni prevalenti, spero e prevedo che quando questo sondaggio sarà ripetuto, nel 2024/5, la maggior parte delle organizzazioni avrà raggiunto una fase stabile in cui si sarà adattata e in cui tutti si saranno abituati a questo nuovo modo di lavorare."

— Peter Page, Head of Solution Consulting presso WithSecure™



2. Spesa per la sicurezza

Quanto dovrei spendere per la sicurezza?

È una domanda che migliaia di aziende si pongono in tutto il mondo; ma quanto del budget IT dovrebbe essere destinato alla cyber security?

Secondo le previsioni il valore del mercato globale della sicurezza informatica sarà di 174,7 miliardi di dollari entro il 2024. È un dato statistico sbalorditivo che mostra quanto sia aumentata l'importanza della cyber security in un mondo in continua evoluzione e suggerisce che le aziende stanno reagendo all'aumento delle minacce investendo di più nella sicurezza.

Considerati diversi fattori, quali attaccanti più sofisticati, la prosecuzione del lavoro da remoto e la situazione geopolitica globale, quanta sicurezza può ritenersi sufficiente e quanto dovrebbero pagare le aziende per ottenerla?

La ricerca condotta da WithSecure™ ha rivelato che l'87,9% delle aziende con sede nell'UE ha in programma di aumentare il budget per la sicurezza nei prossimi 12 mesi. La cosa forse più sorprendente è che l'8,3% si sente adeguatamente coperto o cercherà attivamente di ridurre la spesa per la cyber security.

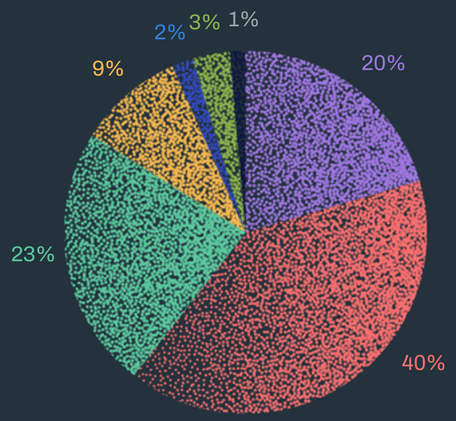
Sembra inoltre esserci un disaccordo tra i gruppi per quanto riguarda il budget per il prossimo anno: mentre infatti i decision maker IT e il top management sembrano essere sulla stessa linea, gli Influencer IT hanno a volte aspettative significativamente diverse. Una comunicazione tempestiva e chiara verso i propri stakeholder su questo argomento è fondamentale per evitare confusione e decisioni dell'ultimo minuto.

Teemu Myllykangas, Director, B2B Product Management presso WithSecure™, è molto esperto in questo campo. "*Quando chiedi a un'azienda se sta spendendo abbastanza, ha difficoltà a rispondere. Se la risposta è sì, nel caso di una violazione le conseguenze saranno gravi perché le persone vorranno sapere come sia successo nonostante gli investimenti che avrebbero dovuto proteggerli. Se la risposta è no, allora le stesse persone dovrebbero chiedersi se stanno facendo bene il loro lavoro e se stanno proteggendo l'azienda. Non è facile rispondere a questa domanda, chiunque dica il contrario non dice la verità o sta cercando di vendervi un rimedio inesistente.*"

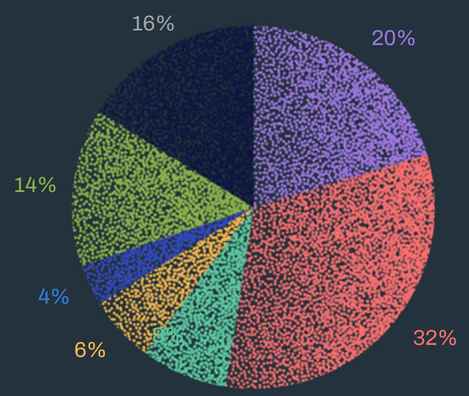
Nel settore, si ritiene in generale che le aziende spendano ogni anno per la sicurezza tra il 3% e il 15% del proprio budget. Quando i clienti vogliono sapere dove dovrebbero collocarsi in questa categoria, Myllykangas è cauto. "*Io dico sempre che bisogna iniziare da un minimo assoluto del 5%. Ma ovviamente quanto più importante è la sicurezza per il cliente, tanto maggiore sarà la percentuale. E viceversa. Generalmente suggerisco di dividere il processo in tre passaggi: si inizia con una valutazione del rischio e la determinazione di un modello di minaccia per definire il ROI, quindi si decide come usare tale somma in modo adeguato usando un framework di sicurezza noto e di base, infine si riesaminano i primi due passaggi ogni anno per identificare il punto di rendimento decrescente e gestire il proprio budget.*"

Intenzioni riguardo al budget per ruolo

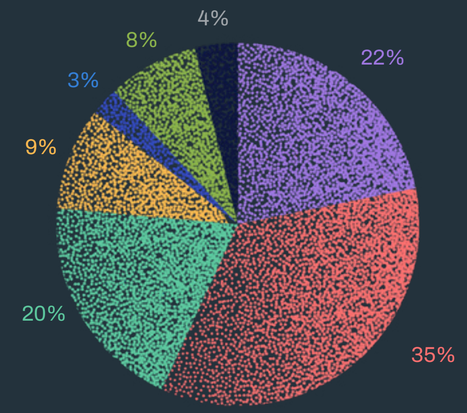
Decision maker IT



Influencer IT



Top management



- Nei prossimi 12 mesi il nostro budget aumenterà dell'1-5%
- Nei prossimi 12 mesi il nostro budget aumenterà del 6-10%
- Nei prossimi 12 mesi il nostro budget aumenterà del 11-15%
- Nei prossimi 12 mesi il nostro budget aumenterà di oltre il 15%
- Nei prossimi 12 mesi il nostro budget diminuirà
- Nei prossimi 12 mesi il nostro budget non aumenterà né diminuirà
- Non so

La valutazione del rischio è essenziale

“*Penso ci siano troppe variabili per poter stabilire una regola generale. I fattori variano enormemente e potrebbero rappresentare una differenza di dieci volte, a seconda delle circostanze. Circa cinque anni fa, la percentuale di spesa per la sicurezza era di circa il 10% del budget IT di un'azienda, ma da allora è aumentata. Le aziende per le quali la sicurezza ha un’importanza critica spendono circa il 12-15% del budget IT per la sicurezza,*” afferma Paul Brucciani, Head of Product Marketing presso WithSecure™.

La prima domanda da porsi è: cosa ti minaccia? E quindi, se dovesse verificarsi l’ipotesi peggiore, quali sarebbero le conseguenze? È necessario calcolare quale sarebbe la perdita annuale prevista (Annual Loss Expectancy o ALE) e la probabilità che si verifichi.

È qui che entra in campo WithSecure™, perché generalmente un'azienda non saprà rispondere a questa domanda. Avendo un'esperienza significativa nella risposta agli incidenti, siamo in grado di delineare l’ALE rispetto ai fattori di rischio e calcolare quanto un'azienda dovrebbe spendere per la sicurezza.

“*Una volta identificato il rischio, è necessario determinare cosa fare con i rischi e in questo senso ci sono tre opzioni. Primo, si possono trasferire i rischi, il che potrebbe, ad esempio, comportare una cyber assicurazione. Secondo, si possono ridurre i rischi, usando controlli, tecnologie e servizi di sicurezza adeguati. Terzo, si possono semplicemente accettare i rischi, conviverci e affrontare le cose quando succedono,*” continua Brucciani.

“*Essenzialmente, si cerca di determinare quanto si può ridurre il rischio e di valutare di conseguenza che parte del budget deve essere accantonata per la sicurezza. Bisogna decidere che rischio si è disposti ad accettare, il proprio livello di tolleranza del rischio e se la propria azienda ha la capacità di assorbirlo,*” secondo Brucciani.

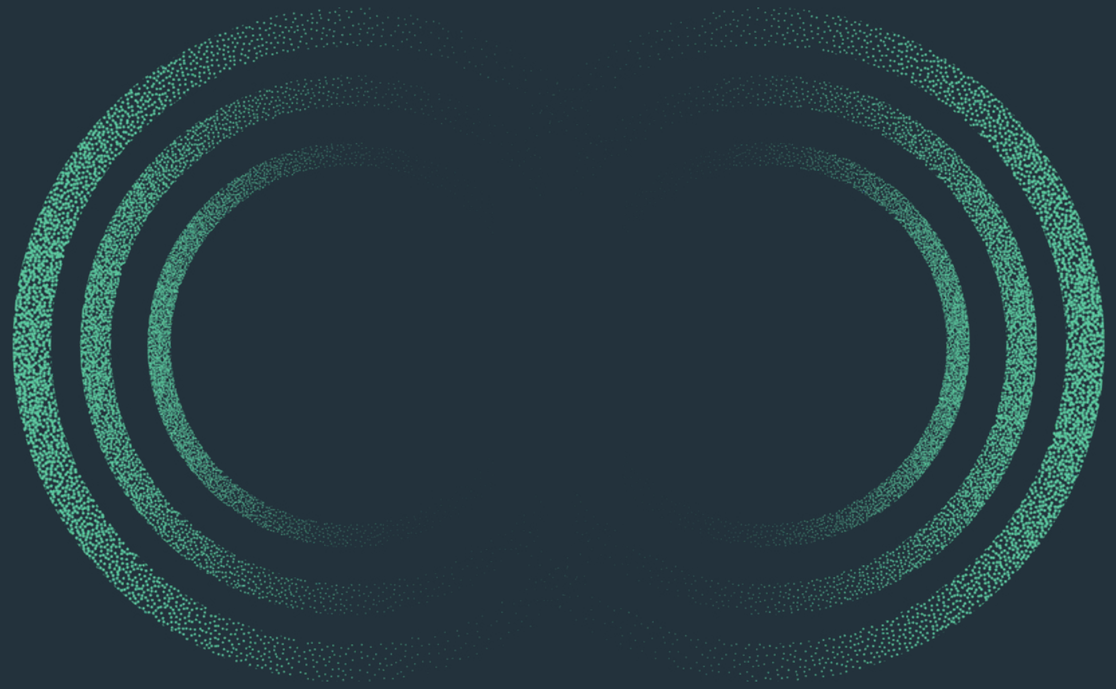
Sono questioni sulle quali è il CFO a dover prendere una decisione. Solo dopo si possono determinare budget, accantonamenti per gli imprevisti e modo di gestire i rischi.

Non è una semplice questione di costo

È importante sottolineare che la protezione della tua azienda è un aspetto che va molto oltre il costo. Ci sono molti altri fattori e la ricerca condotta da WithSecure™ ha dimostrato proprio questo punto. Solo il 13,2% degli intervistati nel sondaggio di WithSecure™ ha dichiarato che il prezzo più basso è l'aspetto più importante quando si sceglie un vendor. Al contrario, più di un quinto (21,8%) pensa che il supporto 24/7 sia l'aspetto più importante, con un ulteriore 16,7% per il quale anche la fiducia nel vendor è importante.

Anche se non c'è una soluzione perfetta quando si tratta di decidere quanto bisognerebbe spendere per la sicurezza, WithSecure™ ti può indicare un percorso logico e sostenibile per assicurare che la tua azienda sia il più protetta possibile. Inoltre, anche se il prezzo è e sarà sempre una questione centrale, la sicurezza va ben oltre questo limite.

WithSecure™ Elements può aiutarti a ridurre rischio, complessità e inefficienza. Associa solide funzionalità di previsione, prevenzione e risposta, tutte gestite e monitorate attraverso una singola console.



3. Residenza dei dati

Sai dove si trovano i tuoi dati?

Per le persone è importante il luogo dove sono conservati ed elaborati i loro dati.

I risultati del nostro sondaggio Pulse 2023 evidenziano un sentito interesse riguardo il luogo in cui i dati sono conservati ed elaborati. Quasi il 73% degli intervistati ha detto che i dati devono essere elaborati nello stesso paese o regione in cui si svolgono le proprie attività operative. Meno di un quinto ha risposto che non era importante.

Quando è importante il luogo geografico per l'elaborazione dei dati nel tuo ruolo?

- I dati devono essere elaborati nello stesso paese delle nostre attività operative
- I dati devono essere elaborati nella stessa regione (ad es. UE, Nord America, APAC) delle nostre attività operative
- Non ha importanza dove elaboriamo i dati dei clienti finali a condizione che siano rispettati tutti i requisiti legali e di conformità
- Non elaboriamo dati per i consumatori finali
- Non so

Dove si conservano i dati

Analizzando queste risposte emerge un disaccordo. Il 42,8% dei decision maker IT considera l'elaborazione dei dati a livello regionale una necessità, rispetto ad appena il 30,9% degli influencer IT. Questa risposta fa comprendere che la questione dell'elaborazione dei dati a livello regionale o nazionale non è semplice o che gruppi diversi hanno priorità diverse.

Aziende di dimensioni specifiche (500-999 e oltre i 5.000 dipendenti) preferiscono l'elaborazione a livello regionale, con più intervistati che concordano sul fatto che non sia importante dove vadano a finire i dati dei clienti.

Tale opinione varia a seconda delle dimensioni dell'azienda: gli intervistati di organizzazioni più grandi hanno risposto più spesso che i dati devono essere elaborati a livello regionale e meno spesso che non è importante.

La preferenza per una solida residenza dei dati potrebbe essere il risultato di cambiamenti radicali, sia in termini di regole che in termini di eventi fisici. La sovranità dei dati, cioè le regole secondo le quali i singoli paesi gestiscono i dati all'interno dei loro confini, è stata al centro di forze contrastanti come la globalizzazione dell'elaborazione e del trattamento dei dati, le normative regionali, la geopolitica, la guerra e gli sconvolgimenti politici e un conseguente desiderio di ridurre il rischio. Tutto ciò mette al centro dell'attenzione il luogo dove si trovano i dati e verso o attraverso il quale si muovono.

Dove si elaborano i dati

Qui le cose si complicano un po': continuano a ripeterci che il cloud cambia ogni cosa (Cloud Changes Everything™), eppure non sembra avere alcun effetto sulle opinioni dei nostri intervistati.

A prescindere dal fatto che le app di un'organizzazione siano ospitate internamente o sul cloud, i punti di vista rimangono invariati. Le organizzazioni con oltre 2.500 dipendenti (e le organizzazioni del Nord America) hanno una tendenza leggermente maggiore a ospitare le applicazioni sul posto, mentre danesi, svedesi, tedeschi e intervistati nel Regno Unito tendono a preferire il cloud. In fondo alla lista, tra il 12,1% e il 6,2% si trovano le persone particolarmente progressiste che fanno tutto sul cloud.

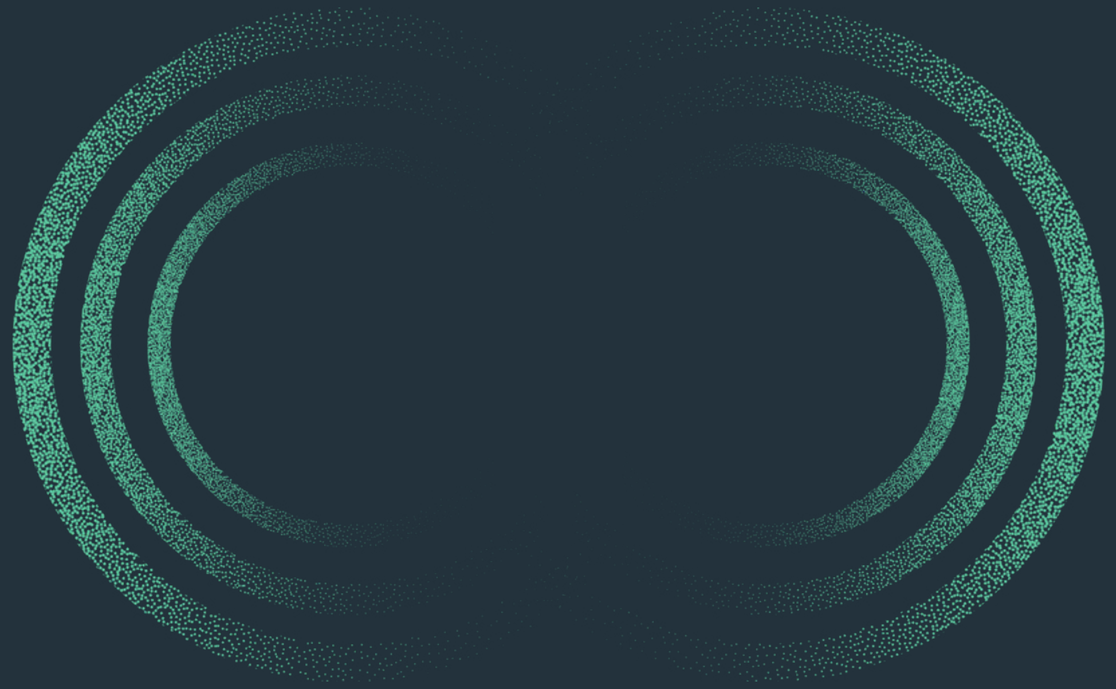
Ambiente IT per dimensioni aziendali

Conclusioni e raccomandazioni

La residenza è importante, come hanno ribadito chiaramente i clienti del nostro Countercept MDR l'anno scorso, tanto da indurci a introdurre una versione del Countercept solo per l'Europa che si addicesse alle loro esigenze. Le motivazioni e le forze motrici di tale desiderio sono complesse, ma è interessante che ci sia un ampio consenso tra gli intervistati di tutte le fasce.

In definitiva, sono le singole organizzazioni a dover allo stesso tempo rispettare le disposizioni di legge e assicurarsi che i propri clienti siano serviti bene. Nella pratica questo può risultare quanto meno complesso. Abbandonare il cloud per passare alla conservazione e all'elaborazione dei dati on-premise comporta una serie di spese di compliance, di sicurezza e tecniche. Il consiglio dei nostri consulenti è di seguire le disposizioni normative nazionali per la protezione dei dati innanzitutto e poi aggiungere a questo le richieste e le esigenze dei clienti.

L'unico campo che potrebbe richiedere un'azione significativa è la comunicazione interna: tra i decisori IT, gli influencer più strategici e il top management c'è un po' di disaccordo riguardo l'elaborazione regionale dei dati. Capire le differenze tra le esigenze nazionali e regionali, e perché tali differenze di opinione esistano nelle organizzazioni, dovrebbe essere un campo da esplorare per i lettori.



4. Cambiare i vendor di cyber security

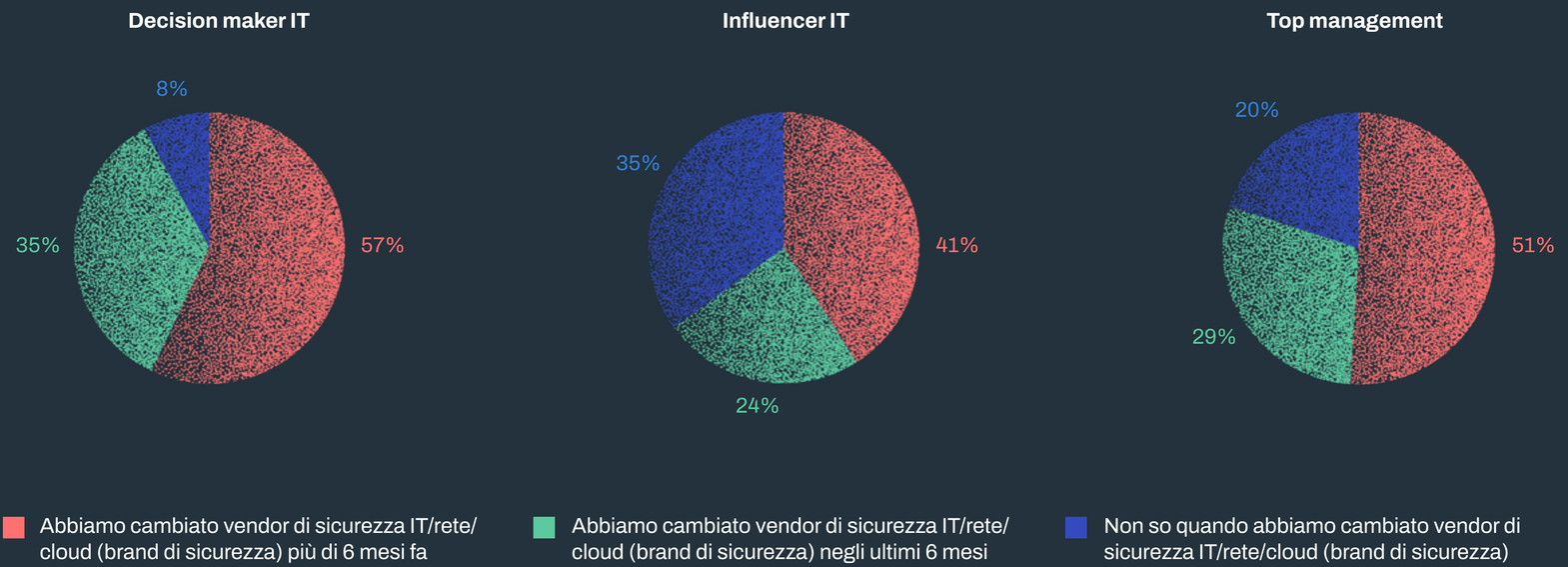
Il cambiamento dei vendor è la costante

Il cambiamento in ambito sicurezza è continuo per le organizzazioni, o piuttosto in termini di fornitori.

Il nostro sondaggio mostra che quasi un terzo (31,9%) delle organizzazioni ha cambiato vendor di sicurezza negli ultimi sei mesi, mentre il 32% si appresta a cambiare soluzione di sicurezza IT o vendor nei prossimi sei mesi.

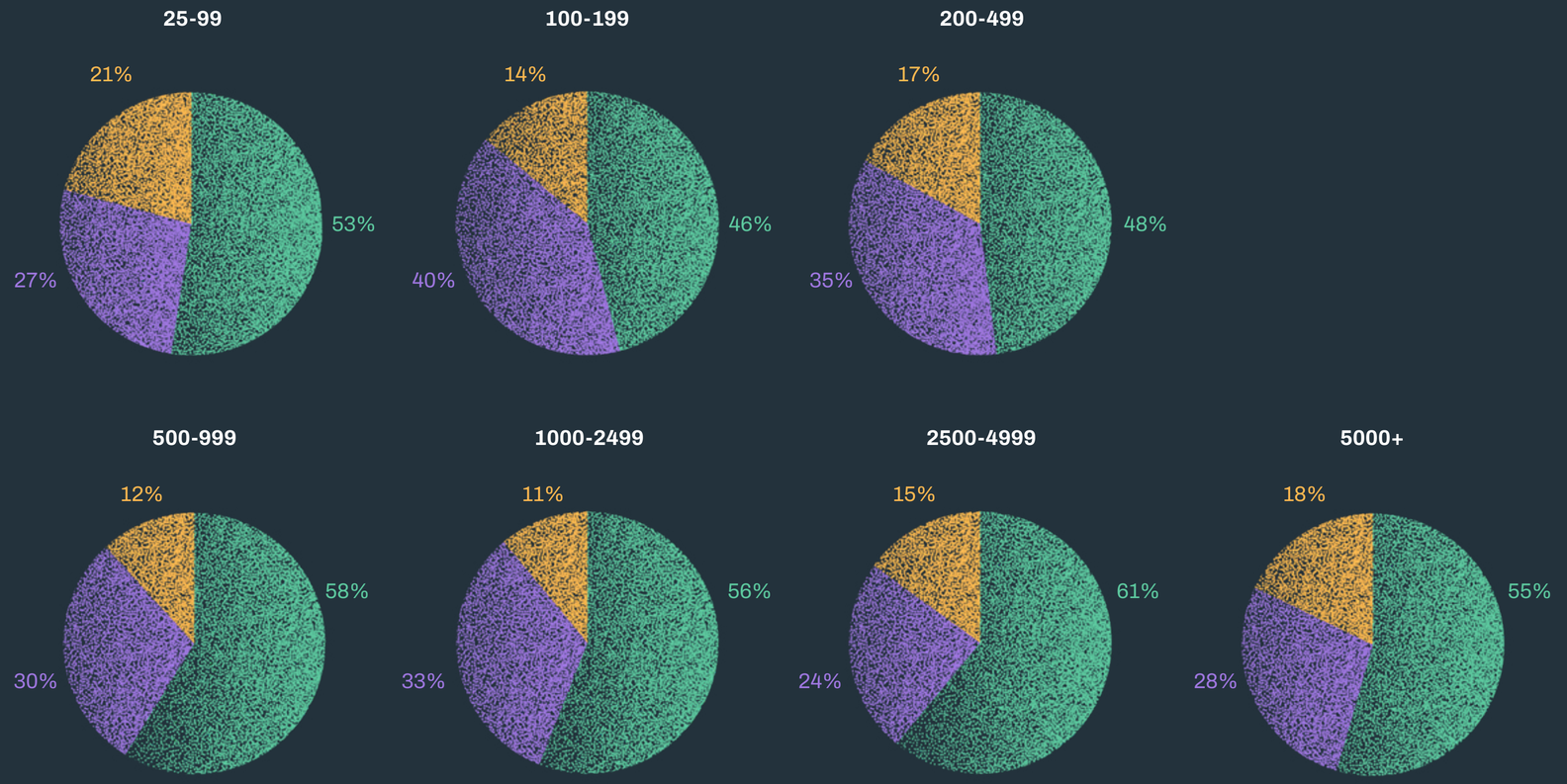
Gli intervistati del settore finanziario e assicurativo e dei servizi IT e tecnologia avevano più spesso cambiato vendor più di sei mesi prima (59,4% e 58,4% rispettivamente) ed erano più propensi a cambiare nei prossimi sei mesi, con una percentuale del 45% e 41,1% rispettivamente.

Opinioni e criteri riguardo al cambiamento di vendor per tipo di ruolo



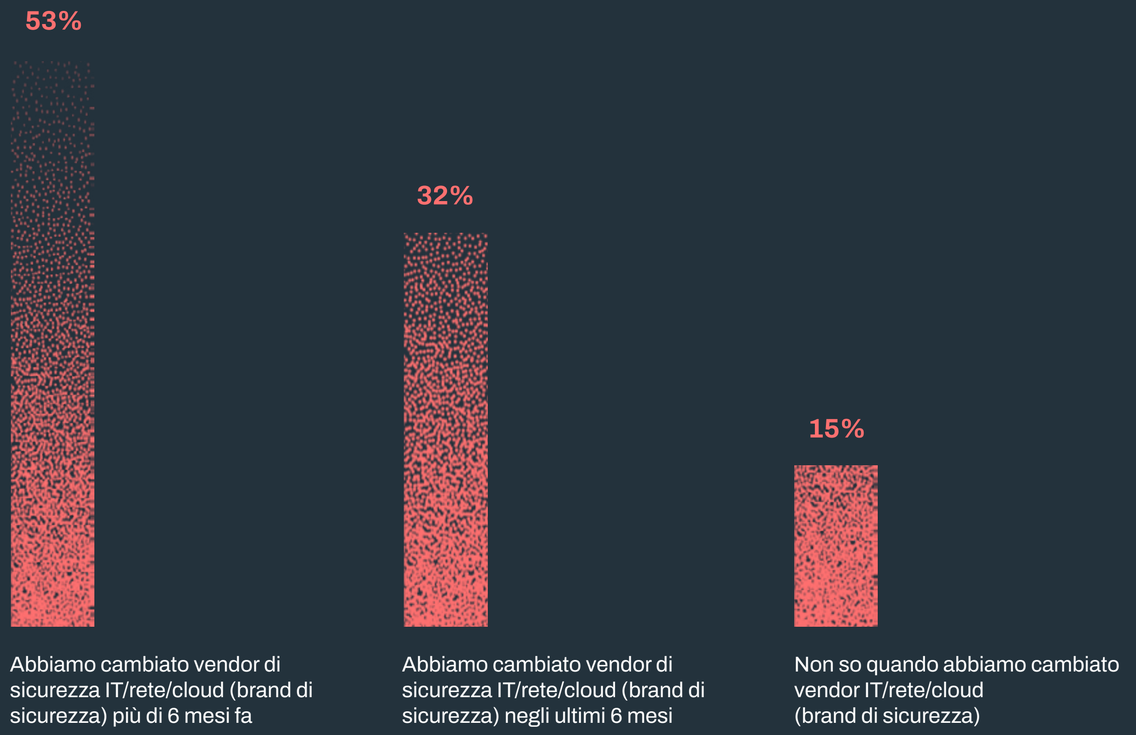
Guardando i dati dalla prospettiva delle dimensioni dell'azienda (n=1.800) si osserva molto più movimento nelle aziende medio-piccole rispetto ad aziende più grandi.

Intenzioni e criteri riguardo il cambiamento di vendor per dimensioni aziendali

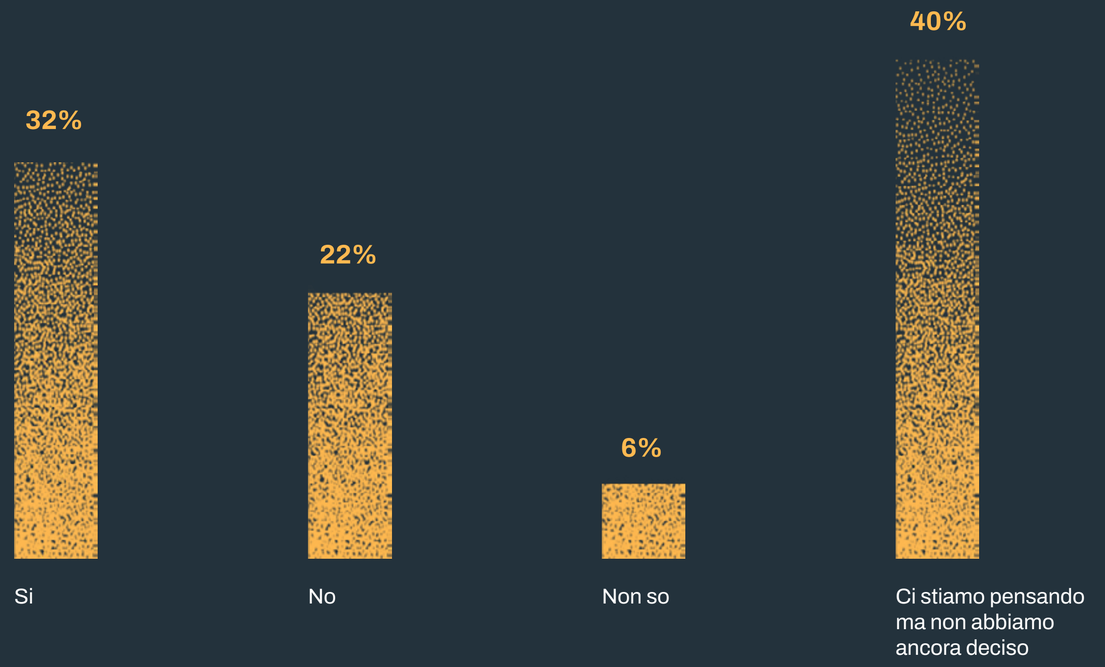


Anche se “cambiare tutto” potrebbe essere la norma per molte organizzazioni, che passano regolarmente da un provider all’altro, questo processo può rivelarsi complicato e richiedere molto tempo. Abbiamo chiesto al Direttore della consulenza per le soluzioni di WithSecure™, Peter Page, di dirci cosa pensa del modo in cui le aziende gestiscono il cambiamento di fornitori. Abbiamo anche esaminato la chiave per creare e mantenere la fiducia tra i vendor e i loro clienti.

Riguardo un cambiamento del vendor di sicurezza IT/rete/cloud (brand di sicurezza)



La tua azienda ha in programma di cambiare il vendor di sicurezza IT/rete/cloud nei prossimi 6 mesi?



Cosa temono di più i clienti nei progetti di transizione?

Le risorse limitate sono certamente un ostacolo e rendono il passaggio da un vendor ad un altro un'impresa ardua per molte organizzazioni. È semplice: a volte cambiare un fornitore con un rendimento scarso richiede troppo lavoro. Non è più così, a giudicare da quanto ci hanno detto i partecipanti al nostro sondaggio.

"I team di sicurezza spesso non sono le persone che implementano i nuovi servizi," afferma Page. "Devono chiedere ai project manager (e) ai team IT di installare il software, devono affidarsi al team delle reti perché il cambiamento che stanno effettuando interessa più parti dell'azienda di quelle di cui sono responsabili e devono ottenere l'approvazione da tutte le diverse parti interessate."

L'avvento dei servizi cloud rende il passaggio più facile?

Abbiamo parlato prima del cloud che cambia le esigenze e le sfide in ambito sicurezza. Cambiare fornitori sta diventando più facile, ma non a causa della natura del cloud: per gli utenti è più facile cambiare servizi cloud, rispetto ai servizi on-premise.

Per Page, è una questione di persone: "*In questo momento ci sono molte persone di talento con competenze nello sviluppo, nell'implementazione e nella sicurezza del cloud. I fornitori di soluzioni di sicurezza devono avere le stesse capacità. Ma con il cambiare del perimetro, cambia il servizio di sicurezza e questo sta aiutando i clienti a capire tale rischio ed è qui che entra in gioco per esempio il Cloud Security Posture Management*."

Perché i contratti hanno una durata sempre minore?

I contratti più brevi sono probabilmente il risultato di due fattori: lo stato dei prodotti e servizi nel mercato della cyber security e mandati più brevi per i CISO (Chief Information Security Officer). Questi manager in genere restano meno di due anni presso un'organizzazione prima di passare a un'altra.

Con il continuo cambiamento dei CISO può crearsi la tendenza a un continuo cambiamento di requisiti e decisioni che probabilmente contribuisce in parte all'instabilità del mercato e al conseguente cambiamento regolare dei vendor.

"*Esiste anche una costante tendenza a preferire la "novità" o l'alternativa migliore ed è in questo modo che il mercato influenza i comportamenti," dice Page. "A volte le risorse impiegate per acquistare l'ultima e la migliore novità potrebbero essere spese meglio per gli elementi fondamentali o per la messa a punto di quello che si ha già.*"

"*A causa della confusione presente sul mercato, è difficile capire quale sia l'approccio migliore. Un CISO che si impegna con un tipo di assistenza pluriennale costosa deve essere sicuro che il fornitore offrirà i risultati di cui ha bisogno e che i dirigenti si aspettano.*"

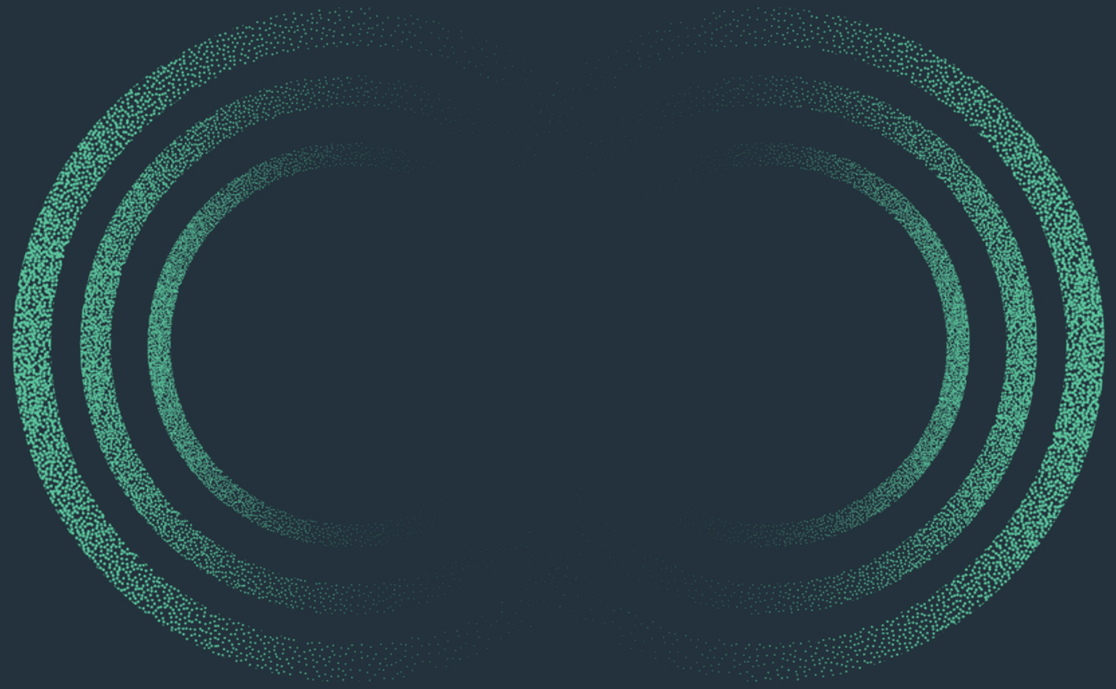
Sta diventando più facile o più difficile per i CISO decidere una transizione?

“In precedenza era difficile per un CISO far approvare dal consiglio di amministrazione una spesa ingente per la cyber security. Adesso è più facile: il consiglio di amministrazione, il CFO e il CEO sono testimoni di violazioni ed infezioni da ransomware nelle organizzazioni e ne comprendono l’impatto finanziario e generale.

“Ma, a causa della situazione del mercato, ci sono molti modi diversi in cui i CISO possono affrontare il problema: Per cosa spendono il denaro? Usano le risorse interne o appaltano a terzi? Cosa scegliere tra MDR, EDR, SIEM o altro? È quasi un’“analisi-paralisi”. Ci sono troppe possibilità e questo significa che passano gran parte del loro tempo chiedendo informazioni e parlando con i vendor, tanto che questo aspetto diventa un lavoro a tempo pieno.”

Il tempo è un fattore determinante

Nonostante la confusione dell'attuale mercato della cyber security, Page afferma che per quanto riguarda la sicurezza, qualsiasi decisione è meglio di niente: *“Se si passa dal niente a qualcosa, prendere una decisione è importante perché non si ha visibilità o copertura della propria proprietà. Ma nei servizi gestiti, la fine del contratto è la scadenza. La questione diventa: quanto tempo prima si dovrebbe iniziare a parlare con altri vendor? I CISO fanno bene a cominciare a cercare 12 mesi prima della fine del contratto e a riflettere sulle opzioni che hanno: è in questo modo che si ottengono i risultati migliori.”*



5. Conclusioni

Il sondaggio di quest'anno invita alla riflessione. È chiaro che coloro che prendono le decisioni sulla cyber security hanno opinioni e aspettative diverse. Analizzare i dati per trovare cosa è fattibile, piuttosto che cosa è soltanto interessante, è difficile. Detto questo, queste sono, secondo noi, le conclusioni più rilevanti. Alcune sono, inevitabilmente, già chiare per i lettori ben informati, ma è utile ripeterle e i nostri dati sostengono anche tali conclusioni.

1) Le priorità percepite possono non essere quelle che fanno veramente la differenza per il profilo di sicurezza. Controlla quali pratiche e competenze mancano alla tua organizzazione e confrontale con le priorità percepite. Cerca le discrepanze.

2) La spesa per la sicurezza è una questione di opinioni. Il nostro sondaggio ha mostrato una grande differenza di percezione dei budget per la sicurezza per l'anno a venire e le aspettative disallineate possono portare a confusione, conflitti e decisioni affrettate. Garantire che ci sia chiarezza e, se il budget non è già confermato o indicato, che ciascun stakeholder si renda conto di cosa un certo livello di budget permetta loro di cambiare, acquistare o ottenere, porta a decisioni serene e controllate.

3) La residenza dei dati è una questione scottante ed è assolutamente imperativa per oltre il 70% degli intervistati. Ma è altrettanto importante prendere in considerazione le implicazioni di abbandonare un'app basata sul cloud che non può garantire la residenza per un'alternativa. Una soluzione locale o in-house sarà altrettanto sicura e offrirà le funzionalità di cui hai bisogno?

4) Quando devi cambiare vendor, decidi per tempo. Le transizioni più riuscite sembrano essere quelle che iniziano 12 mesi prima della scadenza o del rinnovo del contratto e decidere di decidere è probabilmente la migliore decisione da prendere per prima. Non cadere nell'analisi-paralisi.

In definitiva, i nostri dati hanno mostrato un accordo e un consenso notevole tra i gruppi intervistati, il che fa pensare a una buona armonia organizzativa. Ci sono però anche alcuni punti su cui le opinioni di decisori, influencer e management divergono significativamente. Sono questi settori che dovrebbero preoccuparci e quelli in cui una comunicazione chiara e aperta sarà lo strumento più efficace per l'anno a venire.

Metodologia

Lo studio B2B Market Research per il 2022 di WithSecure™ ha intervistato 3.072 persone (2.098 in Europa) per mezzo di un sondaggio online a maggio 2022 in 12 paesi, tra cui nove paesi europei: Regno Unito, Francia, Germania, Belgio, Paesi Bassi, Danimarca, Finlandia, Norvegia e Svezia, oltre a Stati Uniti, Canada e Giappone. Tutti gli intervistati sono responsabili delle decisioni per la sicurezza IT, delle reti o del cloud ed influencer per l'acquisto di prodotti e servizi di sicurezza IT, delle reti o del cloud nelle proprie organizzazioni.

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