Lo stato delle architetture SD-WAN, SASE e Zero Trust

Sponsorizzato da Aruba

Ricerca condotta in maniera indipendente da Ponemon Institute LLC

Data di pubblicazione: Aprile 2021

Lo stato delle architetture SD-WAN, SASE e Zero Trust

Presentato da Ponemon Institute, aprile 2021

Parte 1. Introduzione

Questa ricerca mira ad apprendere importanti informazioni sull'utilizzo delle architetture SD-WAN (Software-Defined Wide Area Network), SASE (Secure Access Service Edge) e Zero Trust. Il Ponemon Institute ha condotto un sondaggio, sponsorizzato da Aruba, tra 1.826 professionisti della sicurezza e del networking delle regioni Nord America, EMEA, Asia-Pacifico e LATAM. Nel contesto della presente ricerca, queste tecnologie sono definite come segue.

- L'**SD-WAN** semplifica la gestione e l'operatività di una Wide Area Network (WAN) separando l'hardware di rete dal suo meccanismo di controllo e virtualizzando i servizi di trasmissione.

- **SASE e Zero Trust** sono architetture di sicurezza utilizzate per implementare controlli di sicurezza.

Di seguito sono riportati i risultati in merito allo stato di adozione e di implementazione di tali tecnologie.

- **Per l'architettura SASE, si preferisce puntare sulle soluzioni migliori.** Per l'implementazione di una SD-WAN e di una soluzione di sicurezza basata sul cloud per un'architettura SASE, il 71% degli intervistati selezionerebbe uno dei fornitori leader.

- **Le organizzazioni molto fiduciose nell'efficacia della propria architettura di sicurezza e nella sua implementazione sono quelle che più hanno implementato soluzioni Zero Trust, SASE e SD-WAN.** Quasi la metà delle organizzazioni altamente performanti (il 48% degli intervistati) ha implementato o implementerà una soluzione Zero Trust, contro il 35% del campione totale. Il 43% degli intervistati appartenenti a organizzazioni altamente performanti ha implementato o implementerà una soluzione SASE, contro il 24% del campione totale.

- **Il Nord America guida l'implementazione di Zero Trust, SD-WAN e SASE.** Il 43% degli intervistati nel Nord America ha implementato una soluzione Zero Trust, contro il 33% degli intervistati nella regione EMEA, il 31% di quelli nella regione Asia-Pacifico e il 26% di quelli nella regione LATAM. Risultati simili si hanno per l'implementazione di soluzioni SD-WAN e SASE, come si può vedere dal report.

- **C'è una familiarità maggiore con l'architettura di sicurezza Zero Trust che con l'SD-WAN e il SASE.** Il 62% degli intervistati dichiara di avere familiarità o una grande familiarità con l'architettura Zero Trust. Segue l'architettura di sicurezza SASE, con il 45% degli intervistati che dichiarano di avere familiarità con essa.

- **Ci si aspetta una crescita dell'adozione di architetture Zero Trust e SASE.** Il 57% degli intervistati dichiara che la propria organizzazione ha implementato o implementerà una soluzione Zero Trust, mentre il 49% dichiara lo stesso con riguardo alle architetture SASE.

- **Il team di rete è quello che ha la maggior influenza sulle implementazioni di soluzioni SD-WAN.** Il 46% degli intervistati dichiara che il team di rete è quello che ha la maggior influenza sulle implementazioni di soluzioni SD-WAN, con la consulenza del team della sicurezza. Il 37% dichiara invece che è il team della sicurezza a guidare l'implementazione, con la consulenza del team di rete.

- **Verso che tipo di fornitori si orientano le organizzazioni con riguardo all'implementazione di servizi di sicurezza basati sul cloud come un Firewall-as-a-**

Service basato sul cloud o un CASB? Il 44% degli intervistati dichiara che la propria organizzazione si rivolgerebbe a fornitori leader del settore specializzati in servizi di sicurezza basati sul cloud.

Parte 2. Risultati principali

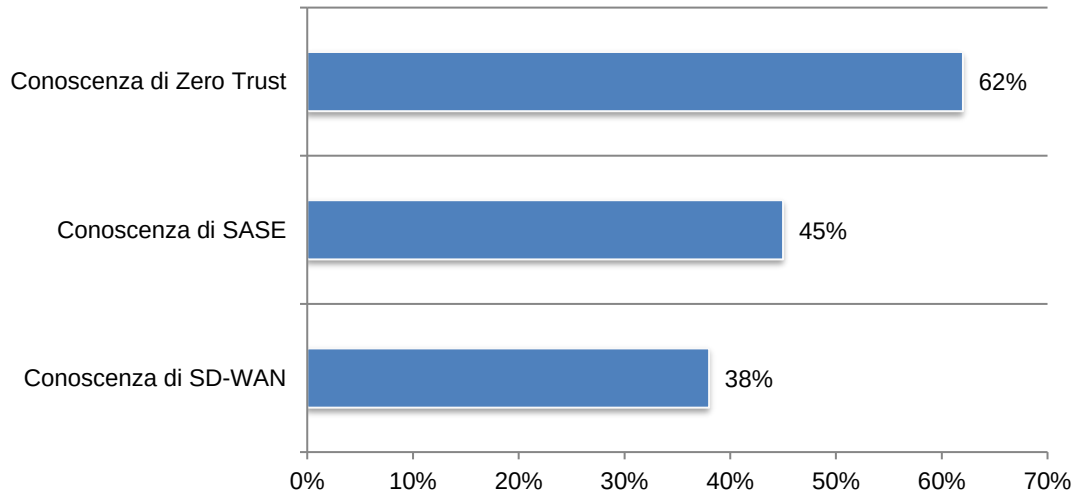
Questa sezione contiene un'analisi dei risultati della ricerca. I risultati integrali e verificati si trovano nell'appendice al report. Nel presente report sono trattate le seguenti tematiche:

- Familiarità e implementazione di soluzioni SD-WAN, di soluzioni di sicurezza basate sul cloud, di soluzioni con architettura SASE e con architettura Zero Trust
- Differenze tra le regioni
- pratiche delle organizzazioni con architetture e implementazioni di sicurezza altamente efficaci

Familiarità e implementazione di soluzioni SD-WAN, di soluzioni di sicurezza basate sul cloud, di soluzioni con architettura SASE e con architettura Zero Trust

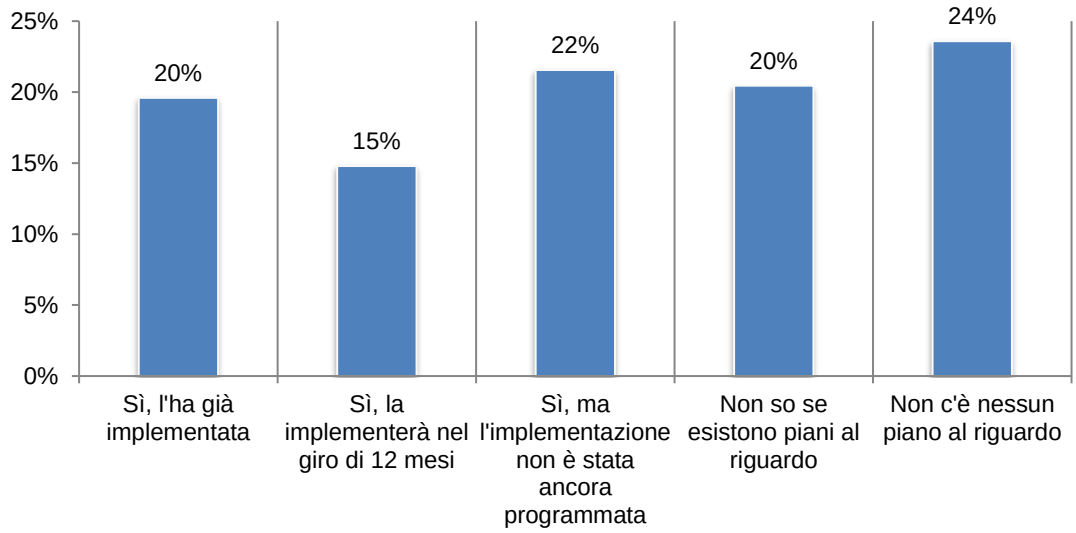
C'è una familiarità maggiore con l'architettura di sicurezza Zero Trust che con l'SD-WAN e il SASE. Come mostrato in figura 1, il 62% degli intervistati dichiara di avere familiarità o una grande familiarità con l'architettura Zero Trust. Segue l'architettura di sicurezza SASE, con il 45% degli intervistati che dichiarano di avere familiarità con essa. Solo il 38% degli intervistati dichiara di avere familiarità o una grande familiarità con le soluzioni SD-WAN.

Figura 1. Conoscenza di Zero Trust, SD-WAN e SASE
Le risposte "Familiarità" e "Grande familiarità" sono state qui riunite in un'unica voce



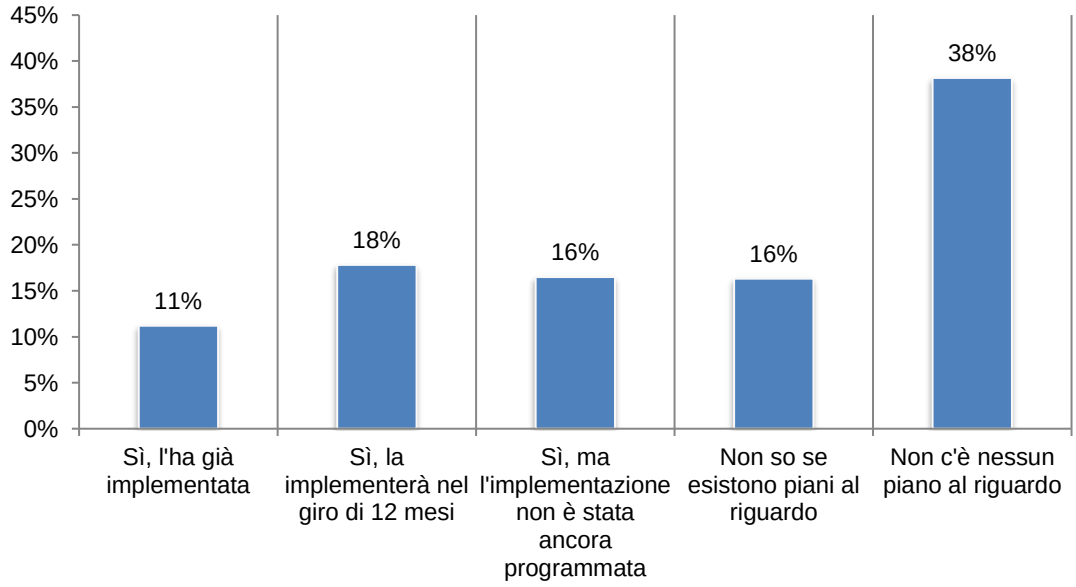
La maggior parte delle organizzazioni ha implementato o intende implementare un'architettura di sicurezza Zero Trust. Come si evince dalla figura 2, il 57% degli intervistati dichiara di aver implementato una soluzione Zero Trust (20%) o che lo farà nei prossimi 12 mesi (15%) o comunque in futuro (22%).

Figura 2. La tua organizzazione ha implementato o intende implementare un'architettura di sicurezza Zero Trust?



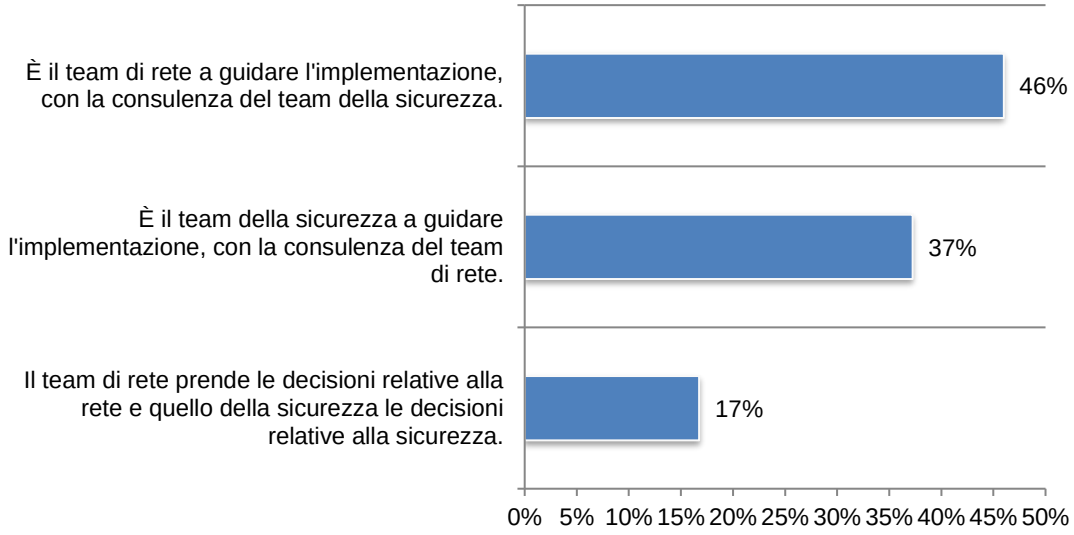
Il 45% degli intervistati dichiara che la propria organizzazione ha implementato o intende implementare una soluzione SD-WAN. Come si evince dalla figura 3, l'11% degli intervistati dichiara di averla già implementata, il 18% che lo farà nei prossimi 12 mesi e il 16% che intende comunque farlo in futuro.

Figura 3. La tua organizzazione ha implementato o intende implementare soluzioni SD-WAN?



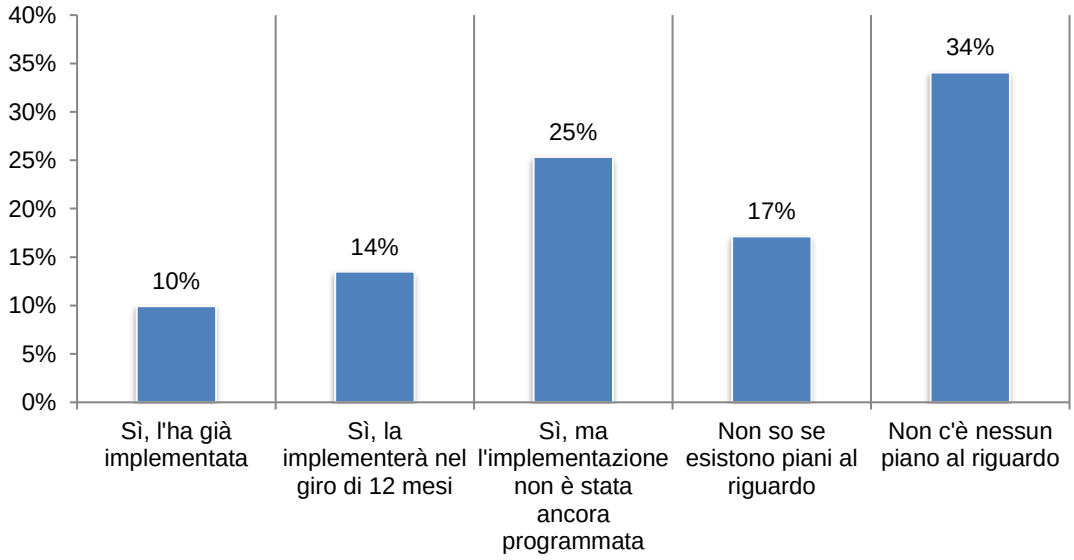
Il team di rete è quello che ha la maggior influenza sulle implementazioni di soluzioni SD-WAN Come mostrato in figura 4, il 46% degli intervistati dichiara che il team di rete è quello che ha la maggior influenza, avvalendosi della consulenza del team della sicurezza. Solo il 17% dichiara invece che il team di rete prende le decisioni relative alla rete e quello della sicurezza le decisioni relative alla sicurezza.

Figura 4. Chi ha la maggior influenza sull'implementazione di soluzioni SD-WAN?



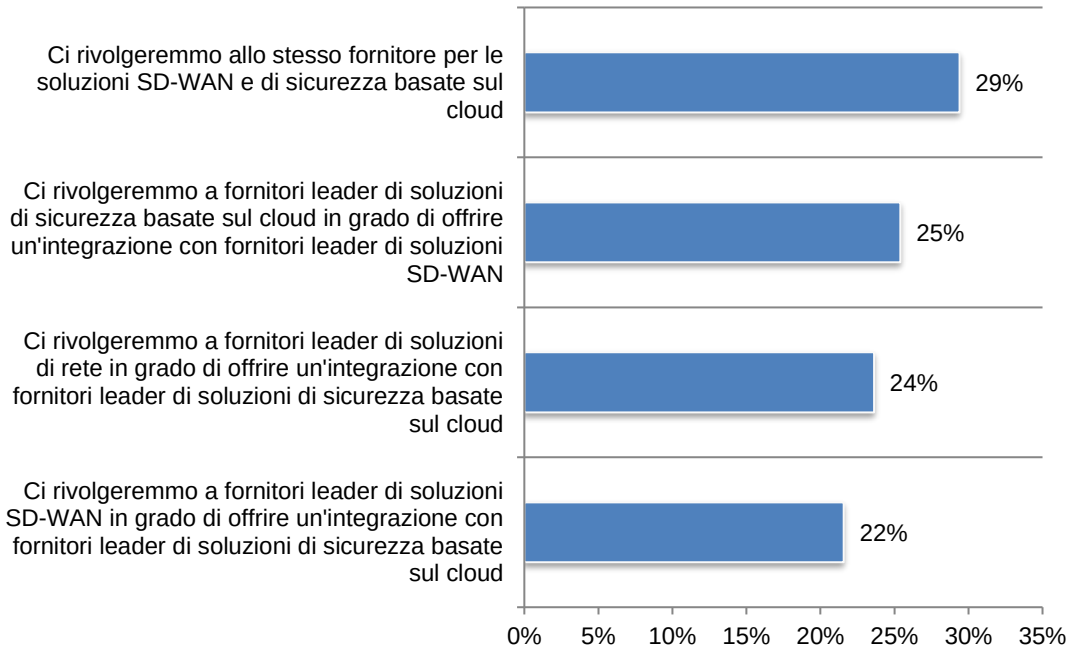
Quasi la metà degli intervistati dichiara che la propria organizzazione ha implementato o intende implementare un'architettura di sicurezza SASE. Come si evince dalla figura 5, il 49% degli intervistati dichiara di aver implementato una soluzione SASE (10%) o che lo farà nei prossimi 12 mesi (14%) o comunque in futuro (25%).

Figura 5. La tua organizzazione ha implementato o intende implementare un'architettura di sicurezza SASE?



Per l'implementazione di una SD-WAN e di una soluzione di sicurezza basata sul cloud per un'architettura SASE si preferisce rivolgersi a un fornitore leader Come mostrato, il 71% degli intervistati dichiara che la propria organizzazione si rivolgerebbe a fornitori leader di soluzioni di sicurezza basate sul cloud in grado di offrire un'integrazione con fornitori SD-WAN (25%), a fornitori leader di soluzioni di rete in grado di offrire un'integrazione con fornitori leader di soluzioni di sicurezza basate sul cloud (24%) o a fornitori leader di soluzioni SD-WAN in grado di offrire un'integrazione con fornitori di soluzioni di sicurezza basate sul cloud (22%).

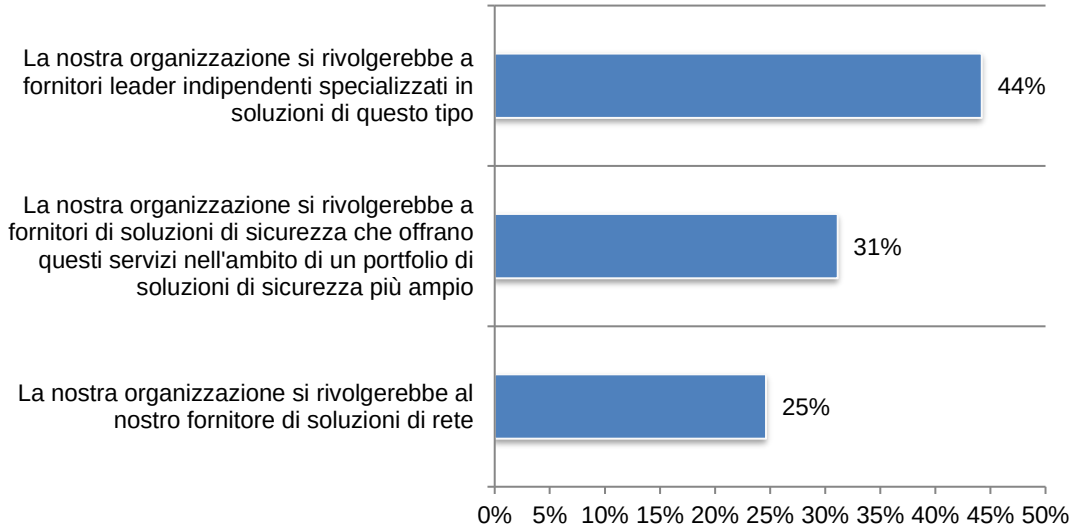
Figura 6. Se la tua organizzazione dovesse implementare una SD-WAN e una soluzione di sicurezza basata sul cloud per un'architettura SASE, come verrebbero scelti i fornitori?
(Una sola risposta ammessa)



Il team di rete è quello che ha la maggior probabilità di prendere decisioni su prodotti/architetture di soluzioni di sicurezza. Il 42% degli intervistati dichiara che nella propria organizzazione è il team di rete a prendere decisioni su prodotti/architetture di soluzioni di sicurezza, seguito dal 31% che dichiara che queste decisioni sono prese dal team della sicurezza e dal 27% che dichiara che a essere coinvolti sono entrambi i team.

Come si vede in figura 7, sulla scelta del fornitore con riguardo all'implementazione di servizi di sicurezza basati sul cloud (per es. Firewall-as-a-Service basati sul cloud, CASB, ecc.), nel 44% dei casi pesa la volontà di servirsi di fornitori leader indipendenti e specializzati in quel tipo di soluzioni, nel 31% dei casi si preferiscono fornitori di soluzioni di sicurezza che offrono tali servizi nell'ambito di un portfolio di soluzioni più ampio, mentre nel 25% si preferisce utilizzare lo stesso fornitore della soluzione di rete.

Figura 7. Come verrebbe scelto il fornitore con riguardo all'implementazione di servizi di sicurezza basati sul cloud?

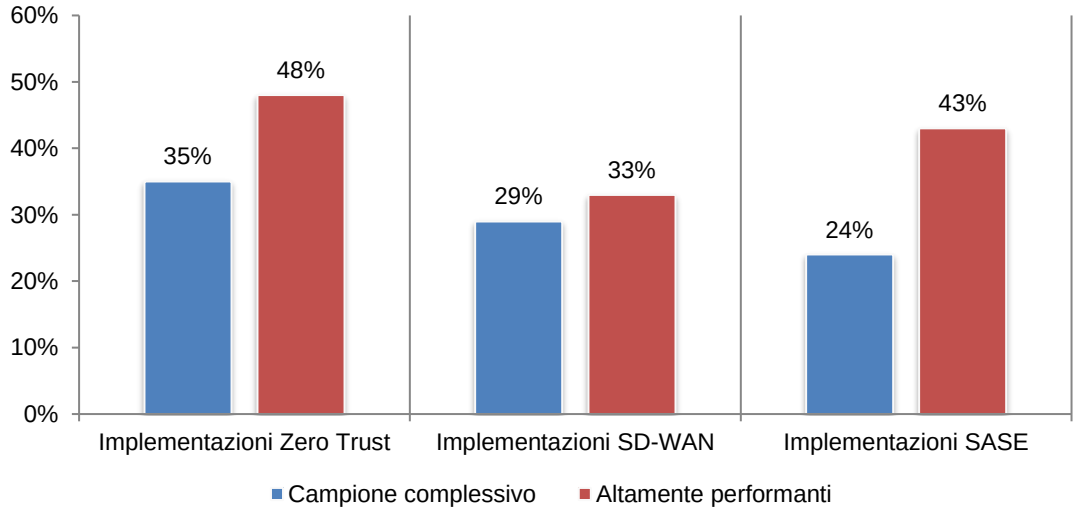


pratiche delle organizzazioni con architetture e implementazioni di sicurezza altamente efficaci

In questa sezione analizziamo le risposte degli intervistati che hanno dichiarato un elevato livello di fiducia da parte delle loro organizzazioni in merito all'efficacia della propria architettura di sicurezza e della sua implementazione (22% degli intervistati). Definiremo le loro organizzazioni come "altamente performanti".

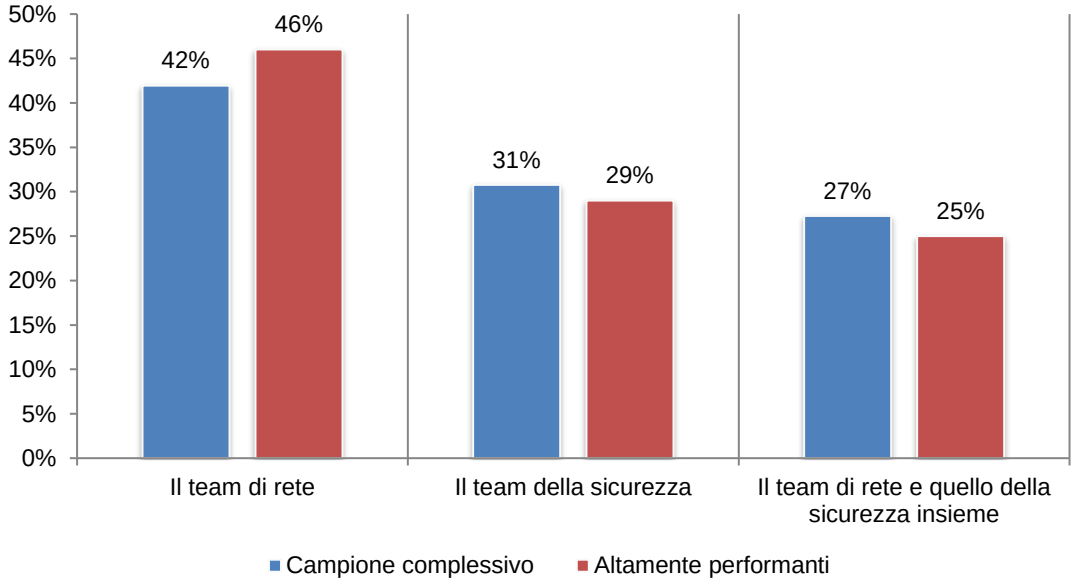
La probabilità che un'organizzazione abbia implementato soluzioni Zero Trust, SD-WAN e/o SASE è molto maggiore nel caso delle organizzazioni altamente performanti. Come mostrato in figura 8, quasi la metà delle organizzazioni altamente performanti (il 48%) ha implementato una soluzione Zero Trust, contro il 35% del campione totale degli intervistati. Il 43% degli intervistati appartenenti a organizzazioni altamente performanti ha implementato una soluzione SASE, contro il 24% del campione totale.

Figura 8. Implementazione di soluzioni Zero Trust, SD-WAN e SASE
Le risposte "Ha implementato" e "Implementerà nei prossimi 12 mesi" sono state qui riunite in un'unica voce



Come si vede nella figura 9, nelle organizzazioni altamente performanti è leggermente più probabile che sia il team di rete a prendere decisioni su prodotti/architetture di soluzioni di sicurezza.

Figura 9. Chi prende le decisioni su prodotti/architetture di soluzioni di sicurezza?

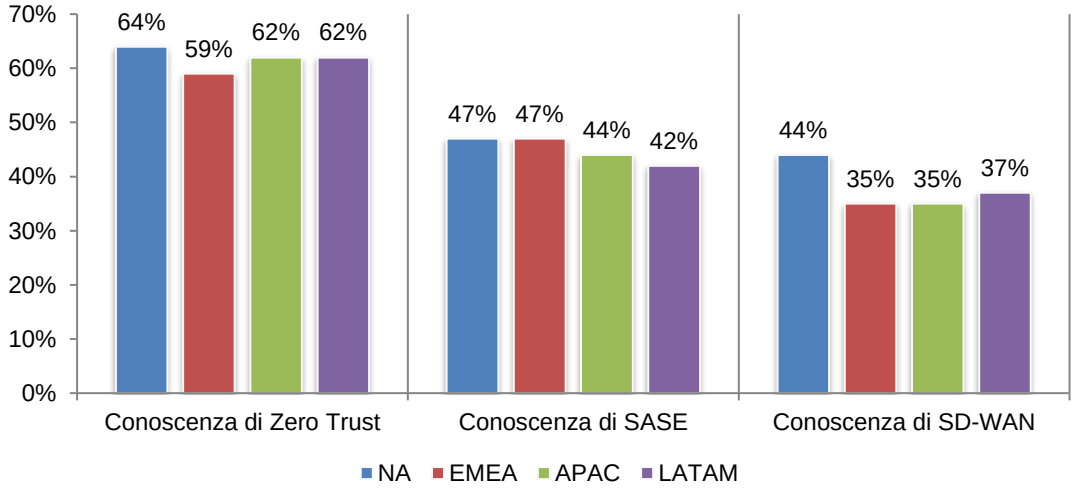


Differenze tra le regioni

In questa sezione confrontiamo le quattro regioni rappresentate nella ricerca: Nord America (598 intervistati), EMEA (454 intervistati), Asia-Pacifico (402 intervistati) e LATAM (372 intervistati).

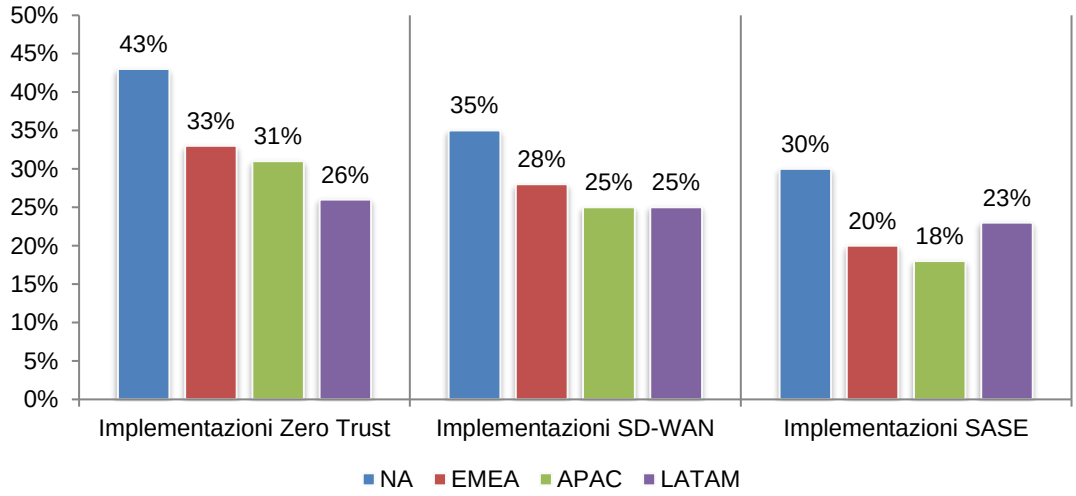
In tutte le regioni si rileva una familiarità maggiore con l'architettura di sicurezza Zero Trust che con l'SD-WAN e il SASE. Come si vede in figura 10, in tutte le regioni la maggior parte degli intervistati dichiara di avere familiarità o una grande familiarità con l'architettura Zero Trust. Riguardo alle soluzioni SASE, gli intervistati di Nord America ed EMEA presentano una familiarità leggermente maggiore rispetto ai colleghi di Asia-Pacifico e LATAM. Gli intervistati nord americani sono coloro che vantano una familiarità maggiore con le soluzioni SD-WAN, con il 44% di risposte positive.

Figura 10. Conoscenza di Zero Trust, SD-WAN e SASE
Le risposte "Familiarità" e "Grande familiarità" sono state qui riunite in un'unica voce



Come mostrato in figura 11, l'implementazione di soluzioni Zero Trust, SD-WAN e SASE è più frequente nel Nord America.

Figura 11. Implementazione di soluzioni Zero Trust, SD-WAN e SASE
Le risposte "Ha implementato" e "Implementerà nei prossimi 12 mesi" sono state qui riunite in un'unica voce



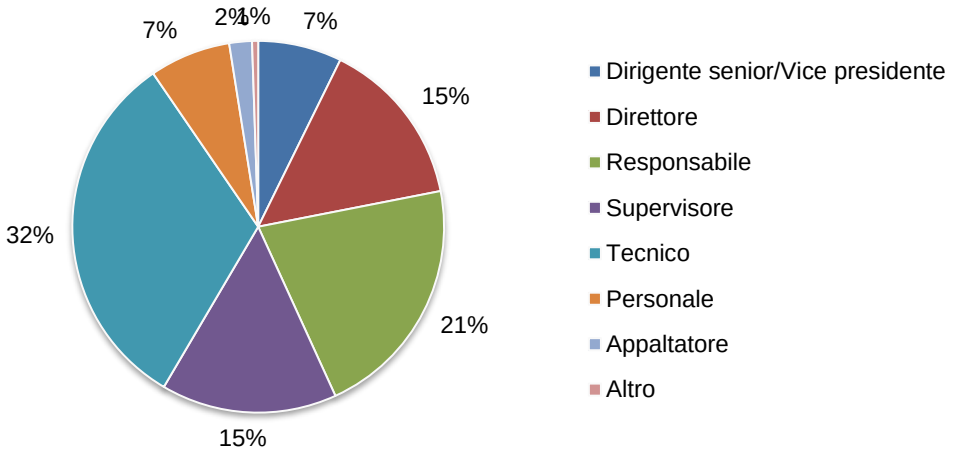
Parte 3. Metodologia

Il frame di campionamento è composto da 51.248 professionisti IT e di sicurezza IT nelle seguenti regioni: Asia-Pacifico, EMEA, Nord America e LATAM. Come mostrato in tabella 1, hanno completato il sondaggio 2.040 intervistati. Lo screening ha escluso le risposte di 214 intervistati. Il campione finale è stato dunque di 1.826 sondaggi, con un tasso di risposta del 3,6%.

Tabella 1. Risposta del campione	Freq	Perc
Frame di campionamento complessivo	51.248	100.0%
Sondaggi completati	2.040	3.9%
Sondaggi esclusi	214	0.4%
Campione finale	1.826	3.6%

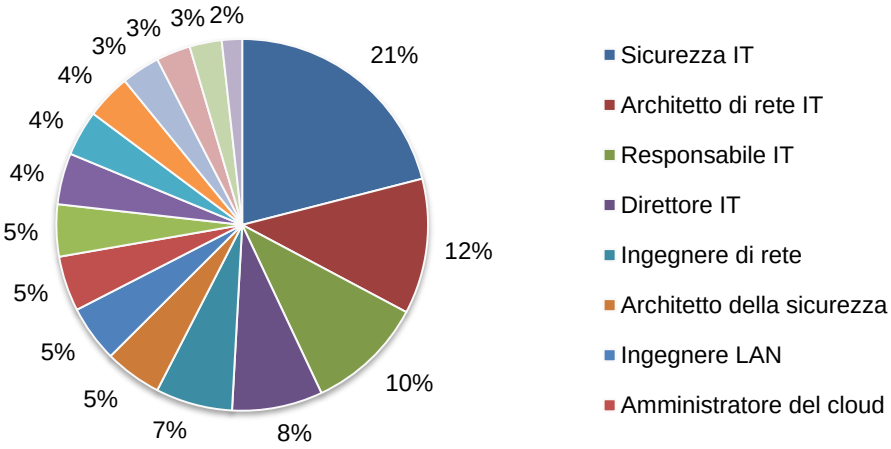
Il grafico a torta 1 mostra la qualifica o la posizione ricoperta degli intervistati al momento della risposta. Il 58% degli intervistati dichiara di ricoprire un ruolo di responsabilità o supervisione, mentre il 32% dichiara di ricoprire un ruolo tecnico.

Grafico a torta 1. Distribuzione degli intervistati in base alla posizione ricoperta



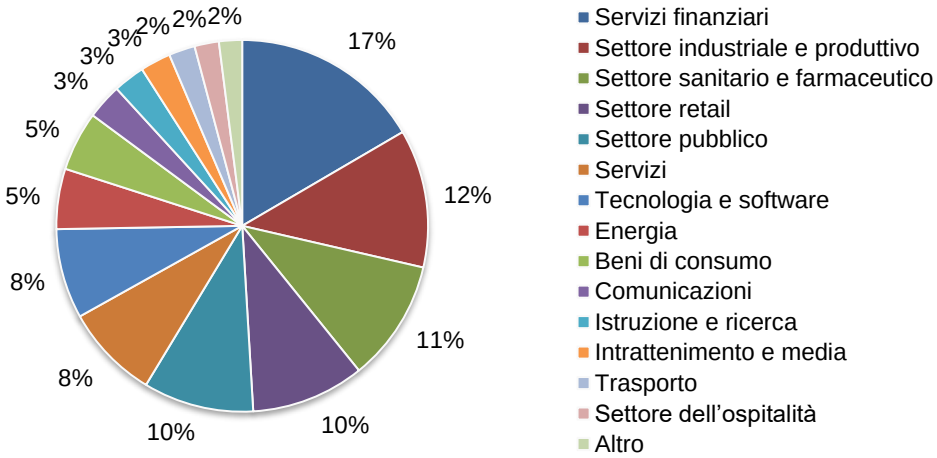
Il grafico a torta 2 mostra il ruolo primario dell'intervistato. Il 21% degli intervistati ha definito il proprio ruolo nell'ambito della sicurezza IT, il 12% si è identificato come architetto di rete IT, il 10% come responsabile IT e l'8% come direttore IT.

Grafico a torta 2. Distribuzione degli intervistati in base al ruolo primario svolto all'interno dell'organizzazione



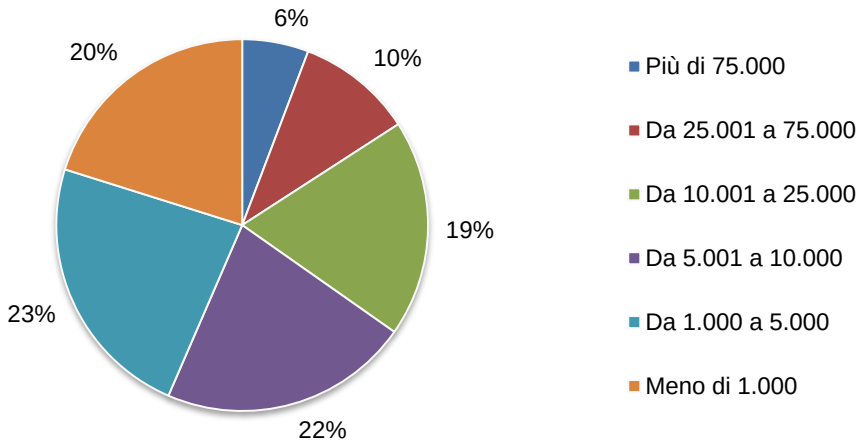
Il grafico a torta 3 mostra la categoria primaria di appartenenza delle organizzazioni degli intervistati. Dal grafico si evince che la fetta più ampia è rappresentata dalla categoria dei servizi finanziari (17%), che include le banche, le assicurazioni e le società d'intermediazione, di gestione degli investimenti e di elaborazione dei pagamenti. Gli altri macrosettori più rappresentati sono quello industriale/produttivo (12%), quello sanitario e farmaceutico (11%), quello retail (10%) e il settore pubblico (10%).

Grafico a torta 3. Distribuzione degli intervistati in base alla categoria primaria di appartenenza dell'organizzazione



Come si vede nel grafico a torta 4, più della metà degli intervistati (57%) lavora per un'organizzazione con almeno 5.000 dipendenti a livello globale.

Grafico a torta 4. Distribuzione degli intervistati in base al numero di dipendenti dell'organizzazione



Parte 4. Avvertenze

Le ricerche basate su sondaggi presentano alcuni limiti intrinseci che occorre considerare con molta attenzione prima di trarre conclusioni dai risultati ottenuti. Di seguito sono elencati alcuni limiti estremamente comuni alla maggior parte dei sondaggi condotti via web.

Bias di non risposta: I risultati presentati si basano su un campione di risposte al sondaggio. Abbiamo inviato il sondaggio a un campione rappresentativo di individui, ottenendo un elevato numero di risposte utilizzabili. Nonostante i test per la valutazione del bias di non risposta, è sempre possibile che gli individui che non hanno partecipato avessero opinioni significativamente differenti da quelle di coloro che hanno completato il sondaggio.

Bias del frame di campionamento: L'accuratezza dipende dalle informazioni di contatto e dal grado di rappresentatività della lista degli interpellati rispetto ai professionisti della sicurezza e del networking che lavorano in vari tipi di organizzazioni nelle regioni Asia-Pacifico, EMEA, Nord America e LATAM. Siamo inoltre consapevoli che i risultati potrebbero essere stati influenzati da eventi esterni, come per esempio la copertura mediatica, e dal fatto di aver promesso un compenso a chi avesse completato il sondaggio entro un determinato periodo di tempo.

Dichiarazioni autovalutative: La qualità di una ricerca basata su un sondaggio dipende dall'integrità delle risposte confidenziali ricevute dagli intervistati. Sebbene sia possibile incorporare nel sondaggio alcuni meccanismi di controllo e contrappeso, esiste sempre la possibilità che l'intervistato non fornisca risposte accurate.

Appendice: Risultati dettagliati del sondaggio

Le seguenti tabelle contengono la frequenza o la frequenza percentuale delle risposte a tutti i quesiti del sondaggio su cui si basa la presente ricerca. Tutte le risposte sono state acquisite nel febbraio 2021.

Risposte al sondaggio	NA	EMEA	APAC	LATAM	Totale
Frame di campionamento complessivo	16.248	12.445	11.891	10.664	51.248
Sondaggi completati	663	501	456	420	2.040
Sondaggi esclusi	65	47	54	48	214
Campione finale	598	454	402	372	1.826
Tasso di risposta	3.7%	3.6%	3.4%	3.5%	3.6%
Peso dei campioni	32.7%	24.9%	22.0%	20.4%	100.0%

Parte 1. Screening

S1. Quale delle seguenti affermazioni descrive meglio il tuo ruolo all'interno dell'organizzazione?	NA	EMEA	APAC	LATAM	Totale
Sono principalmente un professionista della sicurezza	41%	35%	36%	30%	36%
Sono principalmente un professionista del networking	27%	37%	39%	42%	35%
Sono un professionista della sicurezza e del networking	32%	28%	25%	28%	29%
Nessuna delle precedenti (interruzione del sondaggio)	0%	0%	0%	0%	0%
Totale	100%	100%	100%	100%	100%

Parte 2. Utilizzo di SD-WAN, sicurezza basata sul cloud, architettura SASE e architettura di sicurezza Zero Trust

D1. Quanto conosci l'architettura di sicurezza Zero Trust?	NA	EMEA	APAC	LATAM	Totale
Grande familiarità	34%	30%	28%	27%	30%
Familiarità	30%	29%	34%	35%	32%
Una qualche familiarità	27%	30%	28%	17%	26%
Nessuna familiarità	9%	11%	10%	21%	12%
Totale	100%	100%	100%	100%	100%

D2. La tua organizzazione ha implementato o intende implementare un'architettura di sicurezza Zero Trust?	NA	EMEA	APAC	LATAM	Totale
Sì, l'ha già implementata	24%	19%	18%	15%	20%
Sì, la implementerà nel giro di 12 mesi	19%	14%	13%	11%	15%
Sì, ma l'implementazione non è stata ancora programmata	23%	19%	20%	24%	22%
Non so se esistono piani al riguardo	16%	25%	27%	15%	20%
Non c'è nessun piano al riguardo	18%	23%	22%	35%	24%
Totale	100%	100%	100%	100%	100%

D3. Che grado di familiarità hai con le soluzioni SD-WAN?	NA	EMEA	APAC	LATAM	Totale
Grande familiarità	21%	16%	13%	17%	17%
Familiarità	23%	19%	22%	20%	21%
Una qualche familiarità	32%	23%	30%	33%	30%
Nessuna familiarità	24%	42%	35%	30%	32%
Totale	100%	100%	100%	100%	100%

D4. La tua organizzazione ha implementato o intende implementare soluzioni SD-WAN?	NA	EMEA	APAC	LATAM	Totale
Sì, l'ha già implementata	15%	9%	11%	8%	11%
Sì, la implementerà nel giro di 12 mesi	20%	19%	14%	17%	18%
Sì, ma l'implementazione non è stata ancora programmata	11%	20%	23%	14%	16%
Non so se esistono piani al riguardo	18%	12%	19%	16%	16%
Non c'è nessun piano al riguardo	36%	40%	33%	45%	38%
Totale	100%	100%	100%	100%	100%

D5. Chi ha o avrà la maggior influenza sull'implementazione di soluzioni SD-WAN?	NA	EMEA	APAC	LATAM	Totale
È il team della sicurezza a guidare l'implementazione, con la consulenza del team di rete.	40%	34%	38%	36%	37%
È il team di rete a guidare l'implementazione, con la consulenza del team della sicurezza.	45%	47%	50%	42%	46%
Il team di rete prende le decisioni relative alla rete e quello della sicurezza le decisioni relative alla sicurezza.	15%	19%	12%	22%	17%
Totale	100%	100%	100%	100%	100%

D6. Che grado di familiarità hai con l'architettura di sicurezza SASE?	NA	EMEA	APAC	LATAM	Totale
Grande familiarità	24%	18%	17%	19%	20%
Familiarità	23%	29%	27%	23%	25%
Una qualche familiarità	30%	28%	25%	28%	28%
Nessuna familiarità	23%	25%	31%	30%	27%
Totale	100%	100%	100%	100%	100%

D7. La tua organizzazione ha implementato o intende implementare un'architettura di sicurezza SASE?	NA	EMEA	APAC	LATAM	Totale
Sì, l'ha già implementata	12%	8%	9%	10%	10%
Sì, la implementerà nel giro di 12 mesi	18%	12%	9%	13%	14%
Sì, ma l'implementazione non è stata ancora programmata	23%	28%	27%	24%	25%
Non so se esistono piani al riguardo	15%	21%	18%	15%	17%
Non c'è nessun piano al riguardo	32%	31%	37%	38%	34%
Totale	100%	100%	100%	100%	100%

D8. Se la tua organizzazione dovesse implementare una SD-WAN e una soluzione di sicurezza basata sul cloud per un'architettura SASE, come verrebbero scelti i fornitori? (Una sola risposta ammessa)	NA	EMEA	APAC	LATAM	Totale
Ci rivolgeremmo allo stesso fornitore per le soluzioni SD-WAN e di sicurezza basate sul cloud	29%	28%	31%	30%	29%
Ci rivolgeremmo a fornitori leader di soluzioni di rete in grado di offrire un'integrazione con fornitori leader di soluzioni di sicurezza basate sul cloud	23%	27%	25%	19%	24%
Ci rivolgeremmo a fornitori leader di soluzioni SD-WAN in grado di offrire un'integrazione con fornitori leader di soluzioni di sicurezza basate sul cloud	25%	24%	18%	17%	22%
Ci rivolgeremmo a fornitori leader di soluzioni di sicurezza basate sul cloud in grado di offrire un'integrazione con fornitori leader di soluzioni SD-WAN	23%	21%	26%	34%	25%
Totale	100%	100%	100%	100%	100%

D9. Chi prende le decisioni su prodotti/architetture di soluzioni di sicurezza?	NA	EMEA	APAC	LATAM	Totale
Il team di rete	40%	48%	38%	42%	42%
Il team della sicurezza	33%	29%	33%	27%	31%
Il team di rete e quello della sicurezza insieme	27%	23%	29%	31%	27%
Totale	100%	100%	100%	100%	100%

D10. Come verrebbe scelto il fornitore con riguardo all'implementazione di servizi di sicurezza basati sul cloud (per es. Firewall-as-a-Service basato sul cloud, Cloud Access Security Broker, ecc.)? (**Una sola** risposta ammessa)	NA	EMEA	APAC	LATAM	Totale
La nostra organizzazione si rivolgerebbe a fornitori leader indipendenti specializzati in soluzioni di questo tipo	47%	41%	43%	45%	44%
La nostra organizzazione si rivolgerebbe al nostro fornitore di soluzioni di rete	23%	26%	28%	22%	25%
La nostra organizzazione si rivolgerebbe a fornitori di soluzioni di sicurezza che offrano questi servizi nell'ambito di un portfolio di soluzioni di sicurezza più ampio	30%	33%	29%	33%	31%
Totale	100%	100%	100%	100%	100%

D11. Quanta fiducia ripone la tua organizzazione nell'efficacia della sua architettura di sicurezza e della sua implementazione? (1 = scarsa fiducia, 10 = fiducia massima)	NA	EMEA	APAC	LATAM	Totale
1 o 2	5%	8%	11%	9%	8%
3 o 4	15%	6%	8%	13%	11%
5 o 6	25%	15%	8%	25%	19%
7 o 8	33%	36%	35%	34%	34%
9 o 10	22%	35%	38%	19%	28%
Totale	100%	100%	100%	100%	100%
Valore estrapolato	6.54	7.18	7.12	6.32	6.78

D12. Ritieni possibile che un unico fornitore possa soddisfare tutte le vostre **esigenze di sicurezza**?	NA	EMEA	APAC	LATAM	Totale
Sì	68%	64%	59%	57%	63%
No	27%	30%	37%	36%	32%
Non saprei	5%	6%	4%	7%	5%
Totale	100%	100%	100%	100%	100%

D13. Ritieni possibile che un unico fornitore possa soddisfare tutte le vostre **esigenze di rete**?	NA	EMEA	APAC	LATAM	Totale
Sì	48%	45%	41%	39%	44%
No	45%	47%	53%	55%	49%
Non saprei	7%	8%	6%	6%	7%
Totale	100%	100%	100%	100%	100%

D14. Ritieni possibile che un unico fornitore possa soddisfare tutte le vostre **esigenze di rete e di sicurezza**?	NA	EMEA	APAC	LATAM	Totale
Sì	57%	52%	50%	47%	52%
No	35%	42%	43%	45%	41%
Non saprei	8%	6%	7%	8%	7%
Totale	100%	100%	100%	100%	100%

Parte 3. Il tuo ruolo e le tue caratteristiche organizzative

D1. Quale livello organizzativo descrive meglio la posizione che ricopri attualmente?	NA	EMEA	APAC	LATAM	Totale
Dirigente senior/Vice presidente	8%	6%	7%	8%	7%
Direttore	16%	14%	13%	15%	15%
Responsabile	21%	23%	19%	22%	21%
Supervisore	15%	17%	15%	14%	15%
Tecnico	30%	31%	35%	33%	32%
Personale	7%	8%	8%	5%	7%
Appaltatore	2%	1%	3%	2%	2%
Altro	1%	0%	0%	1%	1%
Totale	100%	100%	100%	100%	100%

D2. Quale tra queste definizioni descrive meglio il tuo ruolo primario all'interno dell'organizzazione?	NA	EMEA	APAC	LATAM	Totale
Amministratore del cloud	5%	6%	3%	5%	5%
Responsabile della protezione dei dati	0%	0%	0%	0%	0%
Direttore IT	7%	8%	9%	8%	8%
Responsabile IT	11%	8%	9%	13%	10%
Architetto di rete IT	12%	10%	13%	12%	12%
Sicurezza IT	20%	19%	23%	23%	21%
Ingegnere LAN	5%	3%	6%	6%	5%
Amministratore di rete	3%	3%	2%	4%	3%
Ingegnere di rete	6%	7%	8%	6%	7%
Responsabile operazioni di rete	4%	3%	4%	2%	3%
Specialista di rete	3%	6%	4%	3%	4%
Amministratore della sicurezza	5%	3%	5%	2%	4%
Analista della sicurezza	6%	5%	2%	4%	4%
Architetto della sicurezza	4%	8%	3%	5%	5%
Specialista della sicurezza	3%	3%	3%	2%	3%
Ingegnere WAN	4%	7%	3%	4%	5%
Altro (specificare)	2%	1%	3%	1%	2%
Totale	100%	100%	100%	100%	100%

D3. Quale tra questi settori individua meglio il focus della tua organizzazione?	NA	EMEA	APAC	LATAM	Totale
Agricoltura e ristorazione	1%	1%	1%	1%	1%
Comunicazioni	3%	2%	4%	3%	3%
Beni di consumo	5%	5%	5%	6%	5%
Difesa, industria aerospaziale	1%	1%	2%	1%	1%
Istruzione e ricerca	2%	2%	4%	3%	3%
Energia	5%	5%	6%	5%	5%
Intrattenimento e media	2%	2%	3%	4%	3%
Servizi finanziari	18%	15%	17%	15%	17%
Settore sanitario e farmaceutico	11%	12%	9%	10%	11%
Settore dell'ospitalità	2%	2%	2%	3%	2%
Settore industriale e produttivo	12%	15%	11%	10%	12%
Settore pubblico	9%	10%	9%	11%	10%
Settore retail	10%	10%	9%	10%	10%
Servizi	9%	9%	8%	7%	8%
Tecnologia e software	8%	8%	8%	7%	8%
Trasporto	2%	2%	2%	3%	2%
Altro	0%	0%	0%	0%	0%
Totale	100%	100%	100%	100%	100%

D4. In quale tra questi intervalli rientra la tua organizzazione in termini di lavoratori impiegati a tempo pieno?	NA	EMEA	APAC	LATAM	Totale
Meno di 1.000	18%	24%	21%	18%	20%
Da 1.000 a 5.000	20%	25%	24%	26%	23%
Da 5.001 a 10.000	19%	20%	23%	27%	22%
Da 10.001 a 25.000	22%	17%	19%	16%	19%
Da 25.001 a 75.000	13%	9%	8%	9%	10%
Più di 75.000	8%	5%	5%	4%	6%
Totale	100%	100%	100%	100%	100%

In caso di domande, scrivi a research@ponemon.org o chiama il numero 800.887.3118.

Ponemon Institute

Promuoviamo la gestione responsabile delle informazioni

Il Ponemon Institute si dedica ad attività di istruzione e ricerca indipendenti che promuovano nelle aziende e nel settore pubblico pratiche di gestione responsabile della privacy e delle informazioni. La nostra mission è condurre studi empirici di elevata qualità su questioni chiave in merito alla gestione e alla sicurezza di informazioni sensibili relative a individui e organizzazioni.

In qualità di membro della **Insights Association**, il Ponemon Institute rispetta elevati standard di confidenzialità dei dati, riservatezza ed etica della ricerca. Nelle nostre ricerche aziendali non raccogliamo dati che consentano l'identificazione di individui od organizzazioni. Inoltre, rispettiamo elevati standard qualitativi per essere sicuri di non porre agli interpellati domande non pertinenti, irrilevanti o improprie.