Studio sulla collaborazione open source: opinioni sulla sicurezza e la privacy negli Stati Uniti e nell'area EMEA

Sponsorizzato da Zimbra

Condotto indipendentemente da Ponemon Institute LLC

Data di pubblicazione: Novembre 2014

Studio sulla collaborazione open source: opinioni sulla sicurezza e la privacy negli Stati Uniti e nell'area EMEA

Ponemon Institute, novembre 2014

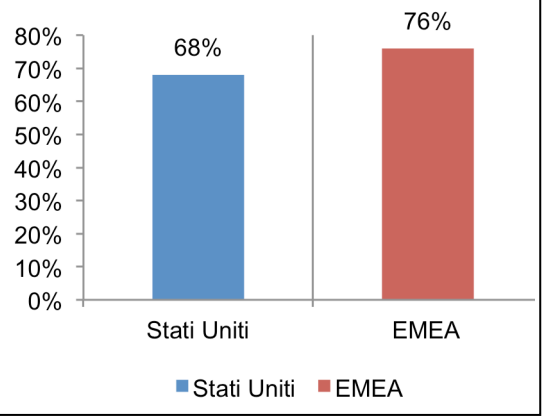
Parte 1. Introduzione

Ponemon Institute è lieto di presentare le conclusioni del rapporto *The Open Source Collaboration Study: Viewpoints on Security and Privacy in the US and EMEA, (Studio sulla collaborazione open source: opinioni sulla sicurezza e la privacy negli Stati Uniti e nell'area EMEA),* sponsorizzato da Zimbra. La ricerca si propone di conoscere dai professionisti IT e addetti alla sicurezza informatica il livello di coinvolgimento delle rispettive società nell'utilizzo di soluzioni di messaggistica e collaborazione open source e di capire il livello di percezione dei vantaggi relativi.

Sono stati intervistati 723 professionisti IT e addetti alla sicurezza IT negli Stati Uniti e 675 professionisti IT e addetti alla sicurezza IT nei seguenti 18 paesi dell'area EMEA: Regno Unito, Germania, Francia, Federazione Russa, Spagna, Arabia Saudita, Italia, Olanda, Turchia, Polonia, Emirati Arabi Uniti, Sudafrica, Irlanda, Svizzera, Danimarca, Svezia, Israele e Grecia.

La maggior parte degli intervistati (57%) negli Stati Uniti e nell'area EMEA conosce o conosce molto bene le politiche o i requisiti sulla sicurezza e la privacy delle organizzazioni in cui lavorano. Il 55% degli intervistati negli Stati Uniti e il 48% di quelli dell'area EMEA copre il ruolo di manager o un ruolo manageriale.

Figura 1. Il supporto commerciale e la trasparenza del codice consentono di aumentare l'affidabilità dell'applicazione?
(Risposte Sì)



Come mostrato nella Figura 1, gli intervistati negli Stati Uniti e nell'area EMEA ritengono che il supporto commerciale e la trasparenza del codice sorgente consentano di aumentare l'affidabilità della soluzione. Quando è stato chiesto il livello di responsabilità del reparto IT nella valutazione e/o nella selezione della soluzione di messaggistica e di collaborazione, il 39% degli intervistati degli Stati Uniti e il 30% di quelli dell'area EMEA ha confermato un coinvolgimento significativo. Secondo l'84% di intervistati degli Stati Uniti e l'82% di quelli dell'area EMEA, le loro organizzazioni cercano di controllare la proporzione tra software open source e software proprietario. La percentuale media di soluzioni aziendali a carattere commerciale open source è pari al 30% negli Stati Uniti e al 25% nell'area EMEA.

Nella presente indagine, il software open source (open source software, OSS) è definito come software per computer, dove il relativo codice sorgente è reso disponibile con una licenza in cui il detentore del copyright fornisce i diritti per studiare, modificare e distribuire il software a chiunque e per qualsiasi scopo. Il software open source viene spesso sviluppato in modo pubblico e collaborativo.

Di seguito sono elencate le principali conclusioni dello studio:

Si ritiene che il vantaggio principale del supporto commerciale di una soluzione open source sia la sicurezza di continuità con il supporto di un partner. Gli intervistati hanno un'opinione generalmente molto positiva sulle soluzioni commerciali open source.

Nonostante i vantaggi, le società introducono lentamente queste soluzioni. La percentuale media di soluzioni aziendali a carattere commerciale open source utilizzate nelle organizzazioni è pari al 30% negli Stati Uniti e al 25% nell'area EMEA.

Le organizzazioni nell'area EMEA sono più inclini all'implementazione di politiche sulla sicurezza e la privacy dei dati. Dallo studio emerge che le aziende dell'area EMEA fanno più attenzione alla privacy nella messaggistica e nella collaborazione. D'altra parte le organizzazioni statunitensi si focalizzano maggiormente sulla sicurezza.

Il supporto commerciale e la trasparenza del codice migliorano la sicurezza, la privacy e l'affidabilità delle soluzioni. Gli intervistati concordano sui vantaggi offerti dal supporto commerciale e dalla trasparenza del codice nelle soluzioni commerciali open source di messaggistica e collaborazione. La risposta degli intervistati dell'area EMEA è principalmente positiva, specialmente in merito alla riduzione dei rischi sulla privacy (il 66% degli intervistati dell'area EMEA rispetto al 52% degli Stati Uniti).

Quali sono i fattori importanti in una soluzione di messaggistica e collaborazione? Gli intervistati negli Stati Uniti sostengono la facilità di utilizzo, mentre nell'area EMEA è più importante il supporto del fornitore**.**

Parte 2. Principali conclusioni

Nella presente sezione sono analizzate le conclusioni della ricerca. I risultati completi sono presentati nell'appendice del presente rapporto. Il rapporto è organizzato in base ai seguenti temi:

- Percezione positiva delle soluzioni commerciali open source
- Rischi sulla privacy e sulla sicurezza di messaggistica e collaborazione
- Importanza delle funzionalità delle soluzioni di messaggistica e collaborazione
- Prospettiva futura di adozione

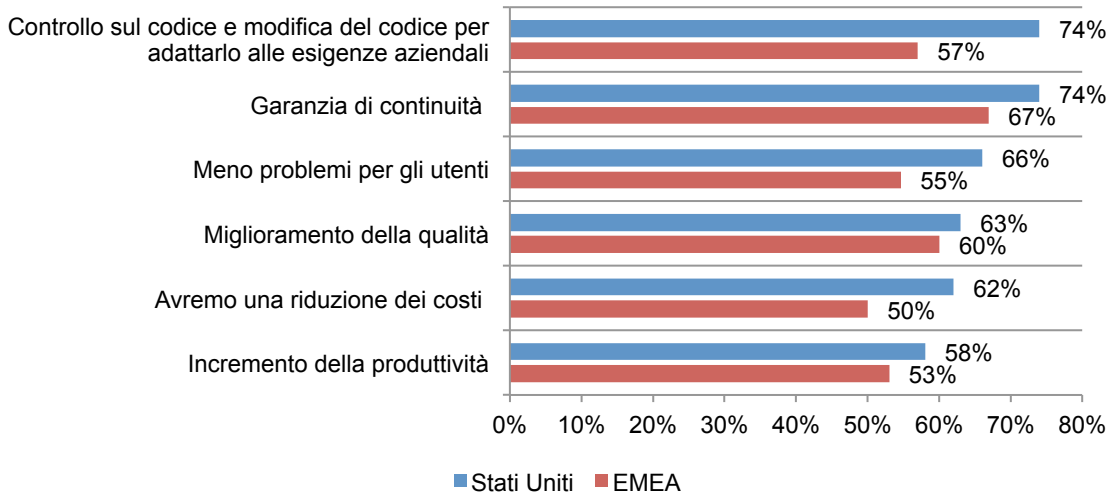
Percezione positiva delle soluzioni commerciali open source

Nella presente indagine, la definizione di open source commerciale riguarda un progetto open source supportato da un'entità commerciale. Non è stato preso in considerazione un progetto open source senza supporto commerciale. Le soluzioni commerciali open source sono diverse da quelle commerciali proprietarie, caratterizzate da un sistema chiuso supportato da un'entità commerciale.

Con le soluzioni commerciali open source si ritiene che il vantaggio principale sia la sicurezza di continuità offerta dal fornitore. Gli intervistati hanno un'opinione generalmente molto positiva sulle soluzioni commerciali open source, specialmente sulla sicurezza di continuità**.** Tuttavia, come mostrato nella Figura 2, gli intervistati degli Stati Uniti sono ancora più entusiasti. Nello specifico, gli intervistati americani concordano maggiormente sul fatto che i loro reparti saranno più produttivi: grazie alle comunità open source e alla collaborazione interna, il team tecnico comprenderà meglio le pratiche IT generali, le risorse e gli strumenti che consentono di servire al meglio l'organizzazione (il 74% degli intervistati degli Stati Uniti e il 57% dell'area EMEA).

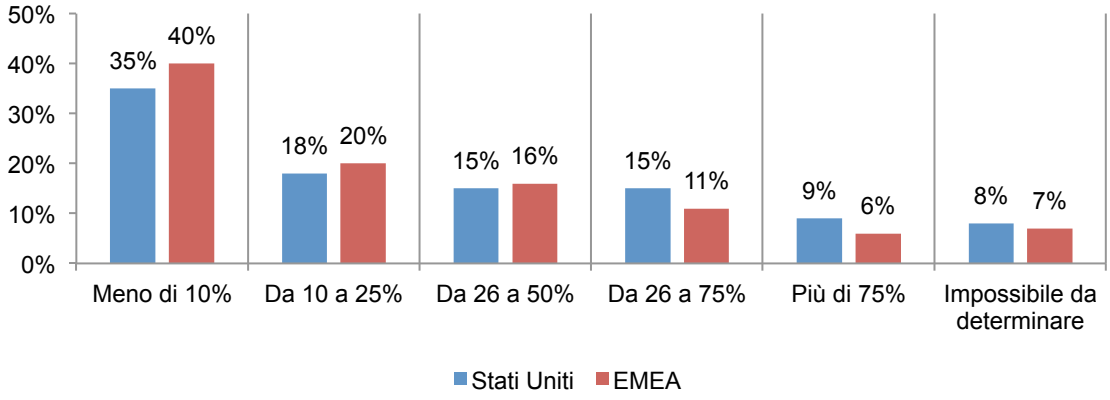
Altre differenze notevoli tra gli Stati Uniti e l'area EMEA sono riscontrabili nella possibilità di ridurre i costi grazie alla flessibilità offerta dal software open source, un vantaggio non offerto dal software proprietario (il 62% degli intervistati degli Stati Uniti contro il 50% dell'area EMEA) e nei problemi inferiori grazie alle continue verifiche del codice di base a cura dei molti membri della comunità che si impegnano a identificare i problemi e a risolverli velocemente ed efficacemente (il 66% degli intervistati degli Stati Uniti e il 55% dell'area EMEA).

Figura 2. Perché le soluzioni commerciali open source sono migliori del software proprietario commerciale?
Risposte combinate Sono pienamente d'accordo e Sono d'accordo



Nonostante i vantaggi, le imprese non introducono queste soluzioni velocemente. Come mostrato nella Figura 3, la percentuale media di soluzioni aziendali a carattere commerciale open source utilizzate nelle organizzazioni è pari al 30% negli Stati Uniti e al 25% nell'area EMEA. Il 39% degli intervistati degli Stati Uniti e il 30% dell'area EMEA afferma che il reparto IT delle loro organizzazioni è coinvolto nella valutazione e/o selezione delle soluzioni di messaggistica e collaborative.

Figura 3. Percentuale di soluzioni aziendali commerciali open source
Valore estrapolato: Stati Uniti = 30%, EMEA = 25%

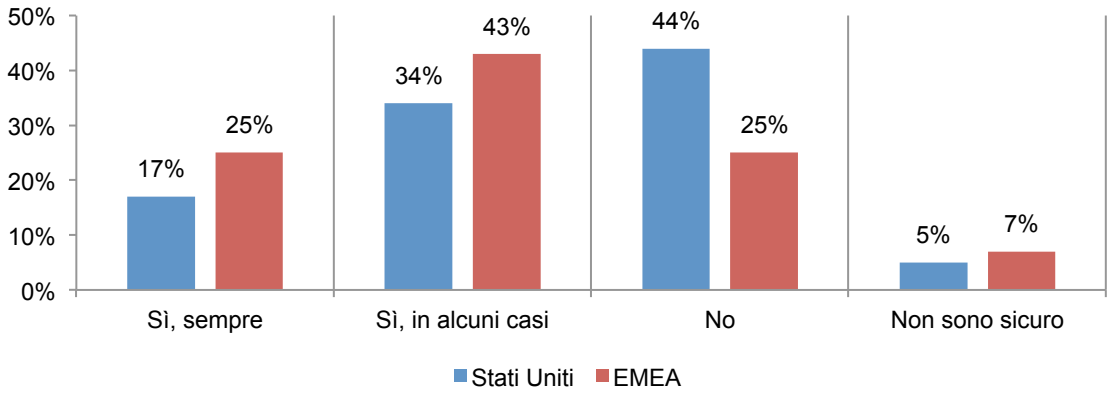


Rischi sulla privacy e sulla sicurezza di messaggistica e collaborazione

Le organizzazioni nell'area EMEA sono più inclini ad applicare politiche interne di sicurezza e la privacy. Dallo studio emerge che le organizzazioni EMEA pongono più attenzione alle possibili conseguenze sulla privacy della messaggistica e della collaborazione. D'altra parte le organizzazioni statunitensi si focalizzano maggiormente sulla sicurezza.

Dalle conclusioni è emerso che la maggior parte degli intervistati (57%) negli Stati Uniti e nell'area EMEA conosce o conosce molto bene le politiche o i requisiti globali sulla sicurezza e la privacy delle imprese in cui lavorano. Come appare nella Figura 4, una percentuale maggiore tra gli intervistati degli Stati Uniti afferma che l'organizzazione non applica politiche interne si sicurezza e la privacy rispetto alle controparti dell'area EMEA (il 44% rispetto al 25%).

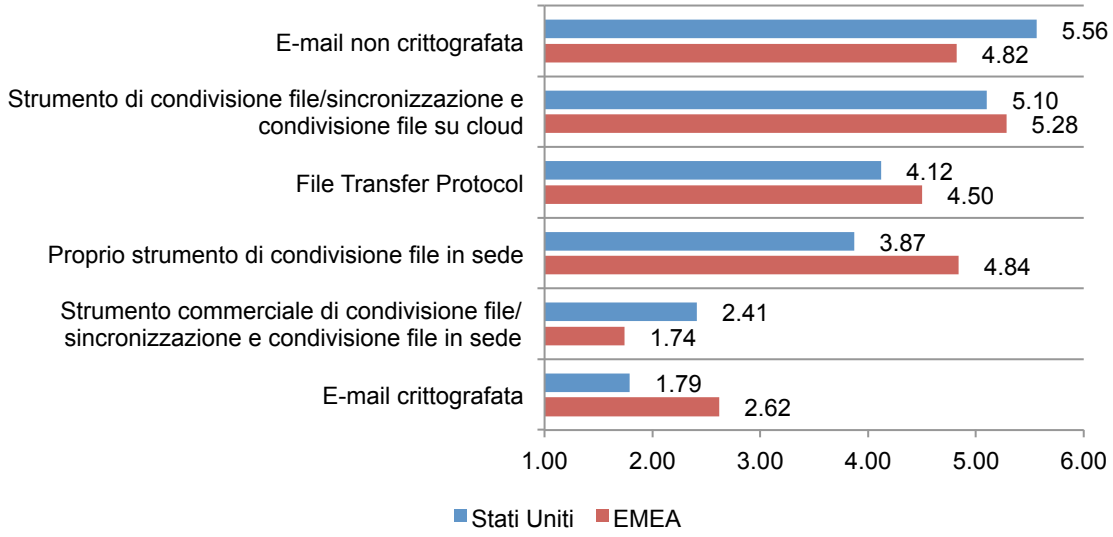
Figura 4. La sua organizzazione implementa politiche aziendali sulla sicurezza e la privacy dei dati?



Si ritiene che l'e-mail non crittografata sia la tecnologia di condivisione file più rischiosa. Entrambi gli intervistati degli Stati Uniti e dell'area EMEA ritengono che l'e-mail non crittografata, seguita dagli strumenti di condivisione file/sincronizzazione e condivisione file su cloud, siano i modi più rischiosi per condividere documenti (Figura 5).

Meno rischiosa è l'e-mail crittografata. Tra le differenze interessanti si può notare la percezione degli intervistati degli Stati Uniti in merito al maggiore rischio dell'utilizzo dell'e-mail non crittografata. Invece, gli intervistati dell'area EMEA sono più preoccupati degli strumenti di condivisione file/sincronizzazione e condivisione file su cloud.

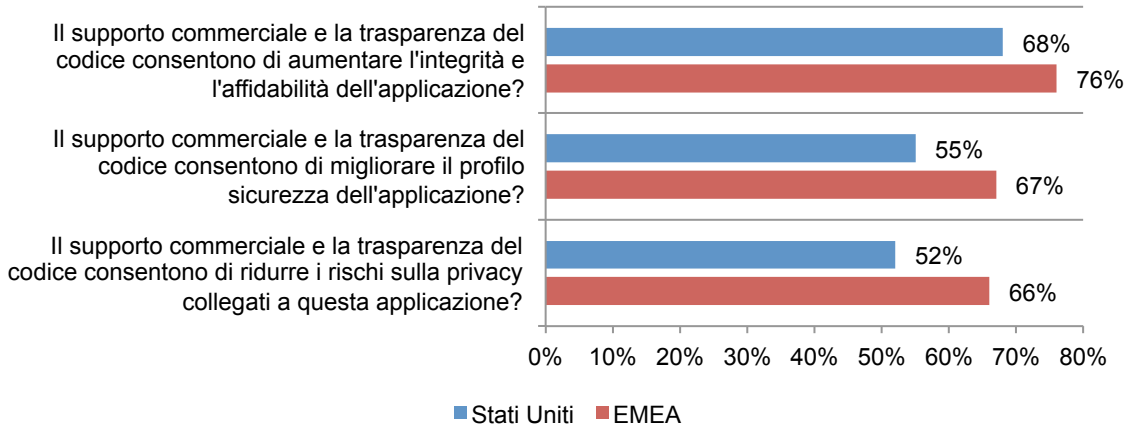
Figura 5. Tecnologie di condivisione file che presentano il rischio maggiore
Da 6 = rischio maggiore a 1 = rischio minore



Il supporto commerciale e la trasparenza del codice migliorano la sicurezza, la privacy e l'affidabilità delle soluzioni. Da quanto si può notare nella Figura 6, gli intervistati concordano sui vantaggi offerti dal supporto commerciale e dalla trasparenza del codice nelle soluzioni commerciali open source di messaggistica e collaborazione. La risposta degli intervistati dell'area EMEA è principalmente positiva, specialmente in merito alla riduzione dei rischi sulla privacy (il 66% degli intervistati dell'area EMEA rispetto al 52% degli Stati Uniti).

Inoltre, il 67% degli intervistati dell'area EMEA e il 55% degli Stati Uniti sostiene che migliori il profilo di sicurezza e la riduzione dei rischi aziendali. Il 76% degli intervistati dell'area EMEA e il 68% degli Stati Uniti afferma che aumenti l'integrità e l'affidabilità dell'soluzione.

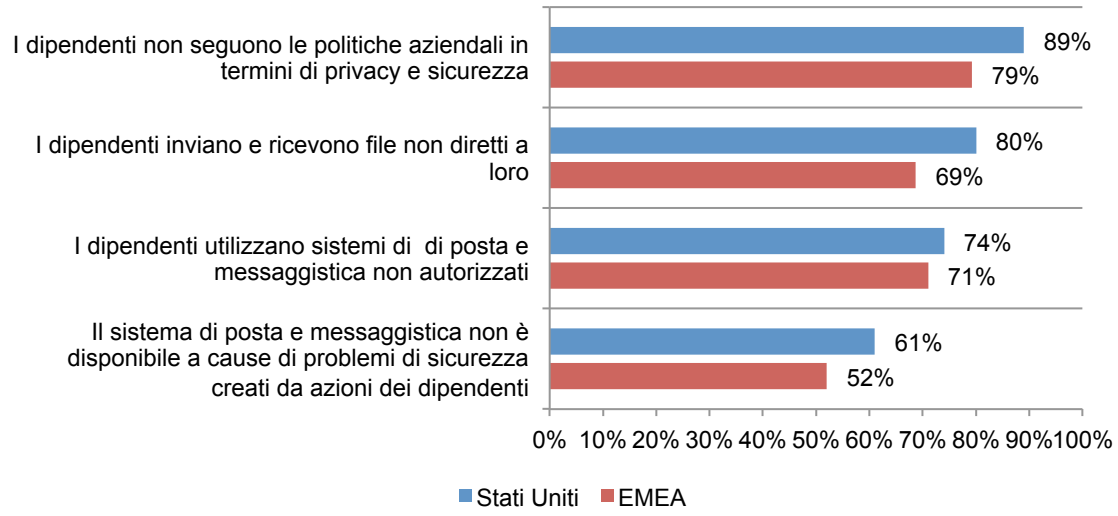
Figura 6. Il supporto commerciale e la trasparenza del codice consentono di migliorare la sicurezza, ridurre i rischi sulla privacy e aumentare l'affidabilità?
Risposte Sì



I dipendenti aumentano i rischi sulla privacy e sulla sicurezza. Secondo la ricerca i dipendenti statunitensi, più di quelli dell'area EMEA, possono mettere a rischio le soluzioni di messaggistica e di collaborazione delle organizzazioni. La Figura 7 mostra quattro pratiche che costituiscono delle minacce ai documenti riservati delle organizzazioni. Gli intervistati degli Stati Uniti credono sia più probabile che il problema risieda nei dipendenti.

Tuttavia, secondo gli intervistati di entrambe le aree, il rischio è alto se gli impiegati non si attengono alle politiche aziendali per quanto riguarda la condivisione di documenti riservati, l'invio e la ricezione di file non indirizzati a loro e l'utilizzo di soluzioni di messaggistica e collaborative non autorizzate dalla società. Il 61% degli intervistati degli Stati Uniti e il 52% dell'area EMEA riferisce che le soluzioni di messaggistica e collaborative delle loro società non sono state disponibili a causa di problemi di sicurezza.

Figura 7. I dipendenti aumentano i rischi sulla privacy e sulla sicurezza
Risposte combinate Spesso e Di frequente



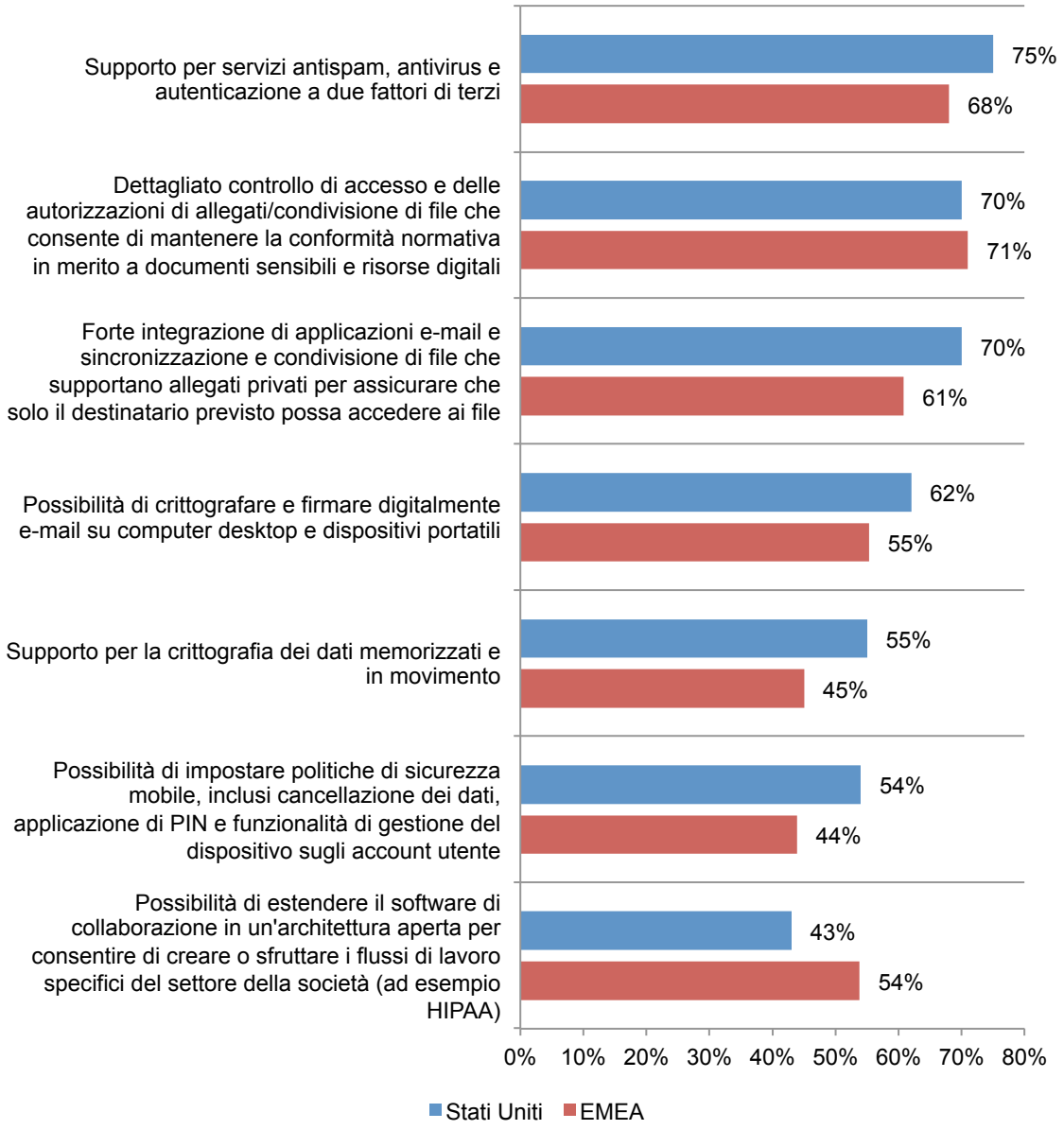
Importanza delle funzionalità delle soluzioni di messaggistica e collaborative

Più di 200.000 società si avvalgono di Zimbra, con più di 100 milioni di utenti commerciali e 500 milioni di utenti gratuiti globalmente. Agli intervistati è stato chiesto di valutare le funzionalità più importanti per le loro organizzazioni.

Gli intervistati degli Stati Uniti e dell'area EMEA indicano la sicurezza e la privacy tra le priorità. Come mostrato nella Figura 8, gli intervistati di entrambe le aree concordano sull'importanza del supporto per servizi antispam, antivirus e autenticazione a due fattori a opera di terzi e sull'importanza della possibilità di mantenere il controllo sulla residenza dei dati per consentire ai dati delle organizzazioni di rimanere in giurisdizioni definite e assicurare la conformità alle leggi sulla privacy dei dati.

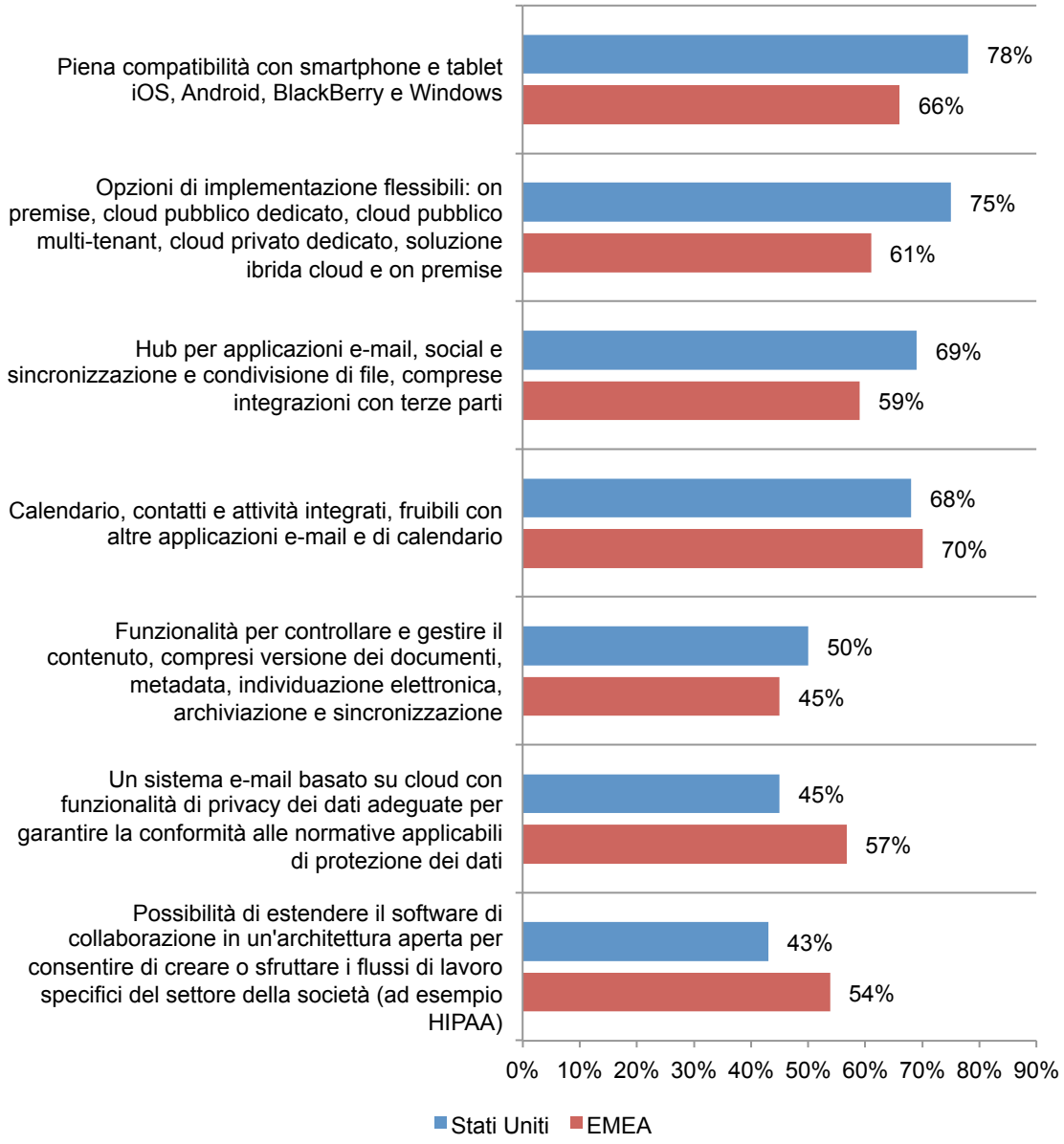
Tra le differenze maggiori tra gli intervistati delle due aree c'è la possibilità di estendere il software di collaborazione in un'architettura aperta per consentire di creare o sfruttare i flussi di lavoro specifici del settore della società (ad esempio HIPAA). Gli intervistati degli Stati Uniti credono che il supporto per la crittografia dei dati memorizzati e in movimento e la possibilità di impostare politiche di sicurezza mobile siano fattori più critici.

Figura 8. Le funzionalità più importanti in termine di privacy e sicurezza in una soluzione di messaggistica e collaborativa
Risposte combinate Molto importante e Importante



Gli intervistati dell'area EMEA e degli Stati Uniti hanno dimostrato diverse priorità in merito alle soluzioni di messaggistica e collaborativa. Le funzionalità principali per gli Stati Uniti sono: piena compatibilità con smartphone e tablet iOS, Android, BlackBerry e Windows, supporto per servizi antispam, antivirus e autenticazione a due fattori di terzi e opzioni di distribuzione flessibili per il cloud. Gli intervistati dell'area EMEA ritengono importante disporre di calendario, contatti e attività integrati, fruibili con altre soluzioni e-mail e di calendario. La Figura 9 mostra le maggiori differenze tra gli intervistati degli Stati Uniti e dell'area EMEA.

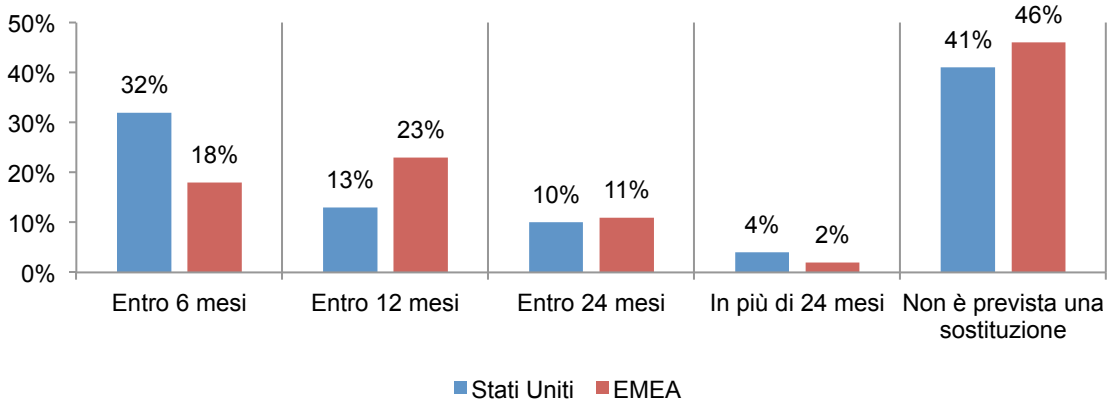
Figura 9. Funzionalità più rilevanti per una soluzione di messaggistica e collaborativa
Risposte combinate Molto importante e Importante



Prospettiva futura di adozione

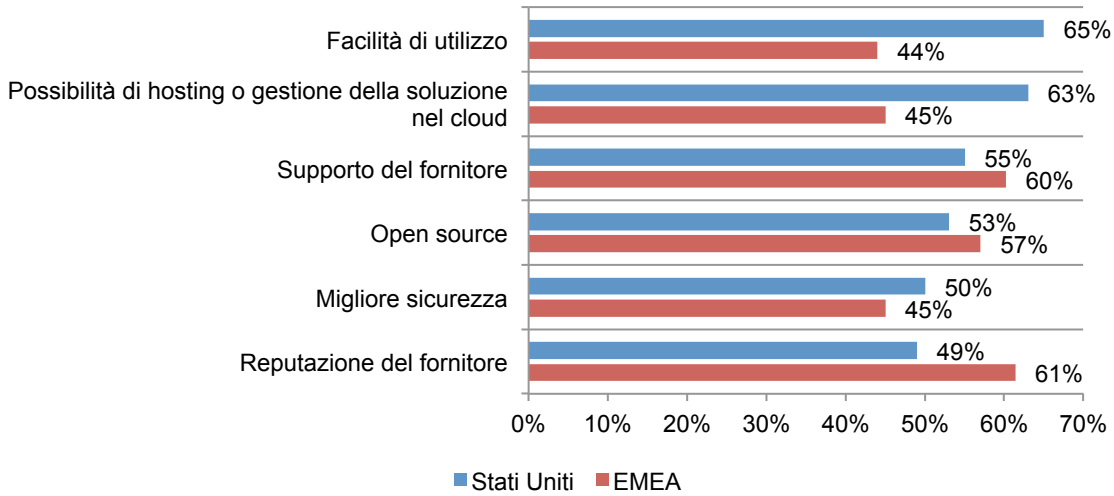
La maggior parte degli intervistati si divide tra "l'abbastanza soddisfatto" o "non soddisfatto" delle attuali soluzioni di messaggistica e collaborazione. Di conseguenza, come mostrato nella Figura 10, il 52% degli intervistati dell'area EMEA e il 55% degli Stati Uniti afferma che le loro organizzazioni sostituiranno le soluzioni di messaggistica e collaborative entro due anni. Una percentuale leggermente maggiore degli intervistati dell'area EMEA (46%) rispetto a quelli degli Stati Uniti (41%) non prevede di sostituire l'attuale soluzione di messaggistica e collaborazione.

Figura 10. Quando intendete sostituire l'attuale soluzione di messaggistica e collaborative?



Quali sono i fattori importanti in una soluzione di messaggistica e collaborazione? Gli intervistati negli Stati Uniti sostengono la facilità di utilizzo, mentre nell'area EMEA è più importante la reputazione del fornitore. Maggiore difformità tra gli intervistati delle due aree è la facilità di utilizzo, seguita dalla possibilità di hosting o gestione della soluzione nel cloud.

Figura 11. Fattori più importanti per la scelta di una soluzione di messaggistica e collaborativa
Sono consentite cinque risposte



Parte 3. Conclusioni

Globalmente, la soddisfazione dei professionisti IT che utilizzano software commerciale open source per la messaggistica e la collaborazione è più positiva rispetto alla soddisfazione di quelli che utilizzano il software proprietario. I professionisti IT statunitensi e dell'area EMEA condividono comunque l'insoddisfazione in merito alle attuali piattaforme di collaborazione e messaggistica, la cui maggioranza è costituita da soluzioni proprietarie. Inoltre, nonostante i professionisti IT americani e dell'area EMEA non concordano sull'importanza relativa della sicurezza rispetto alla privacy, concordano sul fatto che il software commerciale open source offra una maggiore riduzione dei costi, controllo qualità e continuità operativa rispetto al software proprietario.

Parte 4. Metodologia

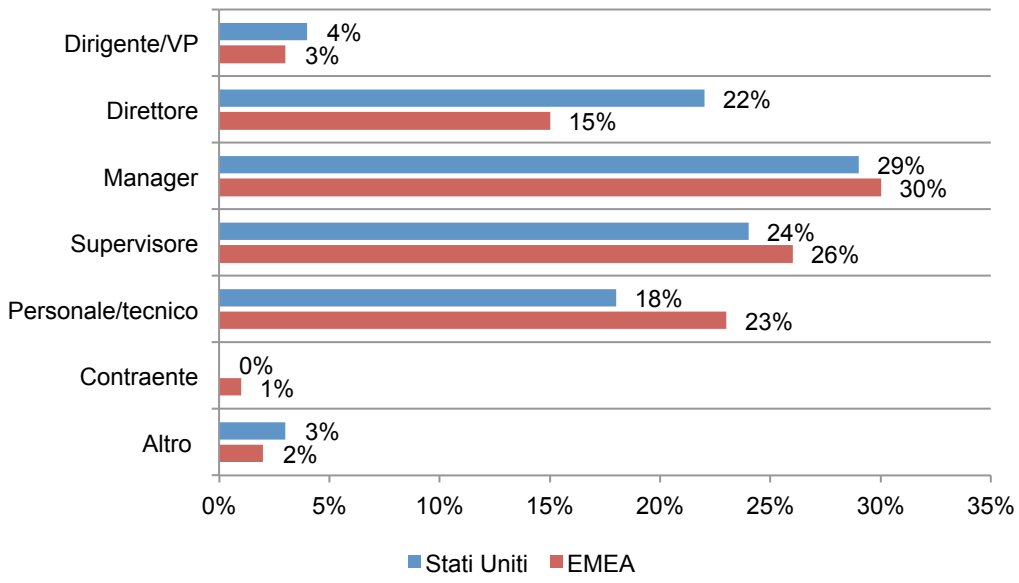
Per l'indagine è stato selezionato un campione di professionisti esperti IT e di sicurezza, intervistando 17.680 persone negli Stati Uniti e 16.700 nell'area EMEA. La Tabella 1 mostra un totale di 1.584 risposte. La selezione e i controlli di attendibilità hanno richiesto la rimozione di 186 sondaggi. Il campione finale è composto da 1.398 interviste ovvero un tasso di risposta del 4,1% per gli Stati Uniti e del 4% per l'area EMEA.

Tabella 1. Risposta all'indagine

Aree di riferimento	Base campione	Risposte totali	Interviste rigettate o selezionate	Campione finale	Tasso di risposta
Stati Uniti	17.680	821	98	723	4,1%
EMEA	16.700	763	88	675	4,0%

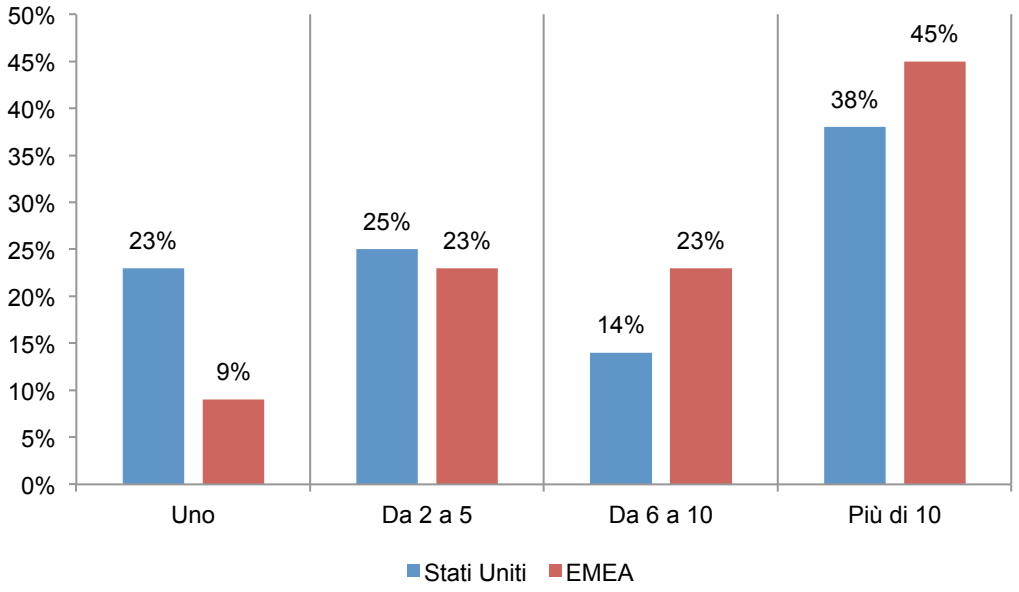
La Figura 12 mostra la posizione lavorativa degli intervistati all'interno delle organizzazioni partecipanti. Intenzionalmente, il 79% degli intervistati negli Stati Uniti e il 74% degli intervistati nell'area EMEA sono dei supervisori o coprono ruoli manageriali.

Figura 12. Posizione lavorativa corrente nell'organizzazione



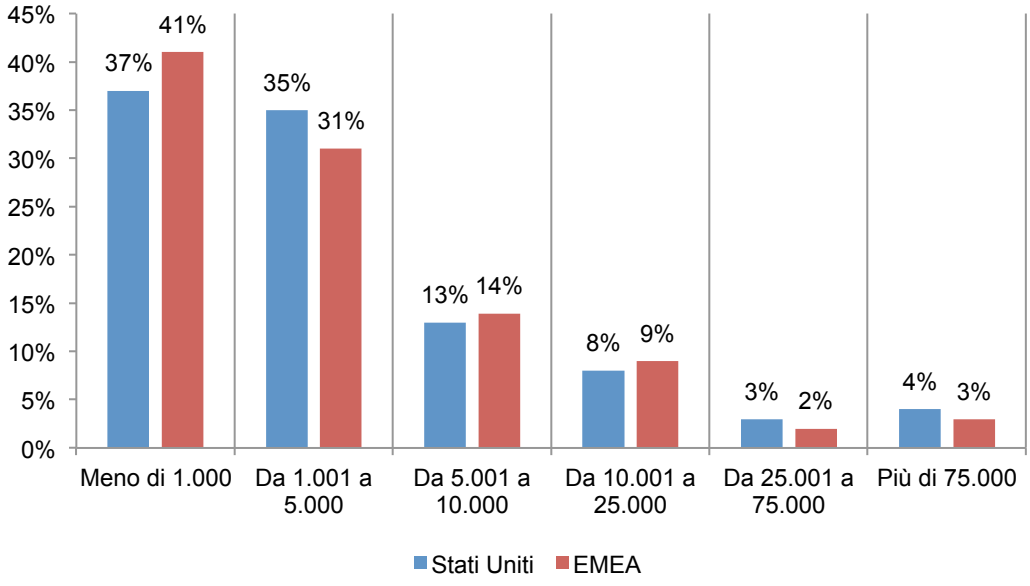
La Figura 13 mostra il numero di paesi in cui le organizzazioni degli intervistati hanno delle sedi aziendali. Il valore estrapolato per gli Stati Uniti è di 7,93 nazioni rispetto ai 9,49 dell'area EMEA.

Figura 13. In quante nazioni la vostra organizzazione ha delle sedi aziendali?



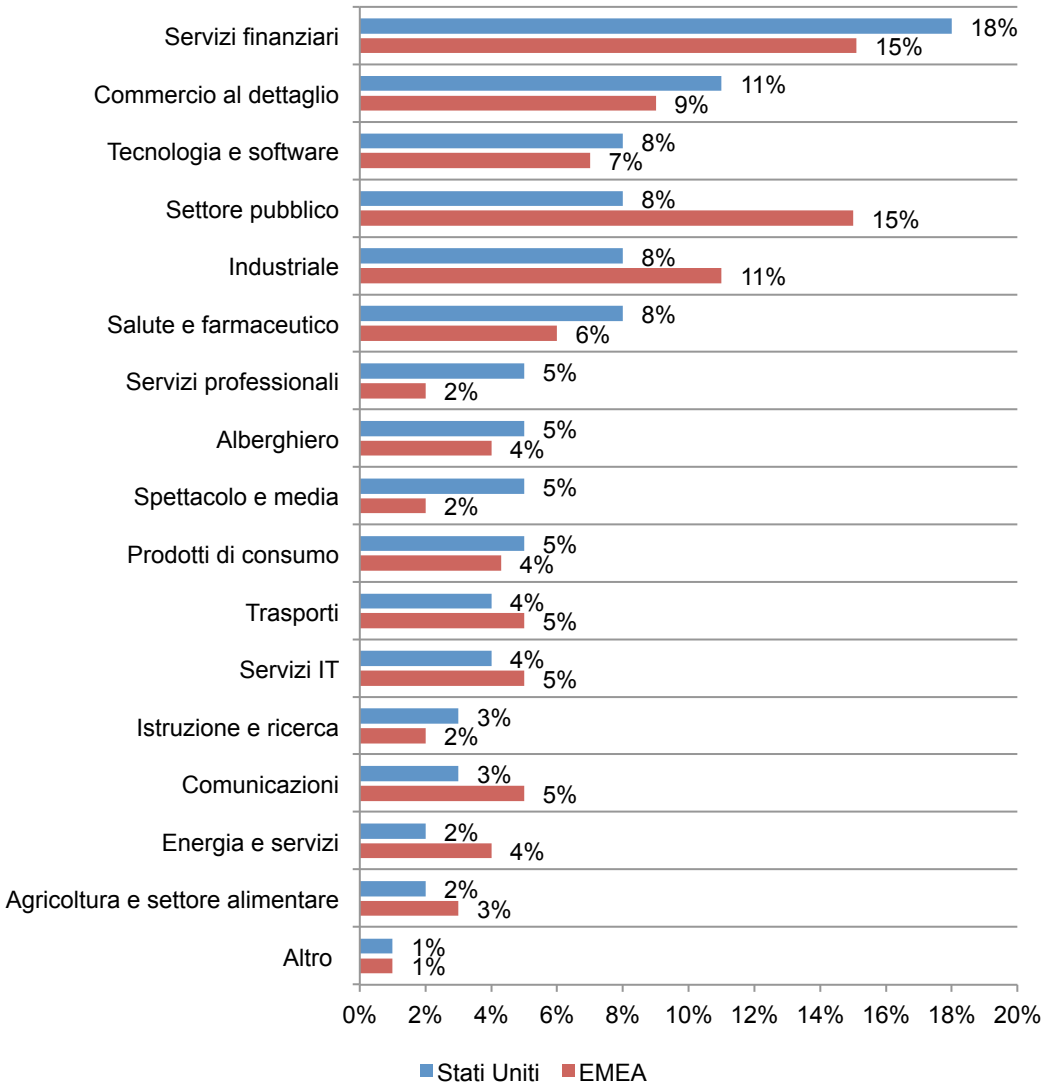
La Figura 14 mostra i dipendenti a tempo pieno dell'organizzazione globale degli intervistati. Il valore estrapolato per gli Stati Uniti è di 8,458 dipendenti rispetto ai 7,317 dell'area EMEA.

Figura 14. Dipendenti a tempo pieno della vostra organizzazione globale



La Figura 15 mostra la classificazione del settore principale delle organizzazioni degli intervistati. Il grafico mostra come i Servizi finanziari costituiscano il segmento più grande per gli Stati Uniti (18%) e per l'area EMEA (15%).

Figura 15. Classificazione del settore principale dell'organizzazione



Parte 4. Riserve

Esistono limiti alla ricerca che devono essere attentamente considerati prima di trarre delle implicazioni dalle conclusioni. Seguono delle limitazioni specifiche attinenti alla maggior parte delle indagini basate su Web.

Errori sulle mancate risposte: le attuali conclusioni si basano su un campione di risposte all'indagine. Per l'indagine è stato coinvolto un campione rappresentativo di persone appartenenti a due regioni globali, producendo una grande quantità di risposte restituite utilizzabili. Nonostante i test di non risposta, è da ritenersi sempre possibile che le persone che non hanno partecipato all'indagine abbiano delle credenze sostanzialmente diverse da coloro che hanno completato lo strumento.

Errori sulla base di campionamento: la precisione si basa sulle informazioni di contatto e sul livello di attinenza dell'elenco a professionisti IT e addetti alla sicurezza IT. Riconosciamo che i risultati possono essere pregiudicati da eventi esterni come coperture mediatiche. Riconosciamo inoltre l'inaccuratezza dei dati a causa della compensazione dei soggetti per completare la ricerca in un periodo di resistenza.

Risultati auto dichiarati: la qualità della ricerca di indagine si basa sull'integrità delle risposte riservate ricevute dai soggetti. Sebbene sia possibile integrare al processo di indagine alcuni controlli e fattori di equilibrio, è sempre possibile che un soggetto non abbia fornito una risposta precisa.

Appendice: risultati dettagliati dell'indagine

Le tabelle di seguito forniscono la frequenza percentuale delle risposte a tutte le domande dell'indagine su base consolidata (globale) in quattro gruppi regionali. Tutte le risposte della ricerca sono state raccolte nel mese di ottobre 2014.

Risposta all'indagine	Freq	Stati Uniti	Freq	EMEA
Base di campionamento totale	17.680	100,0%	16.700	100,0%
Risposte totali	821	4,6%	763	4,6%
Interviste rigettate o selezionate	98	0,6%	88	0,5%
Campione finale	723	4,1%	675	4,0%

I1. La sua organizzazione cerca di controllare la proporzione tra software open source e soluzioni aziendali proprietarie?	Freq	Stati Uniti	Freq	EMEA
Sì	609	84%	556	82%
No	114	16%	119	18%
Totale	723	100%	675	100%

I2. Come definirebbe la sua familiarità delle politiche o i requisiti globali sulla sicurezza e la privacy dei dati della sua organizzazione?	Freq	Stati Uniti	Freq	EMEA
Grande familiarità	175	29%	156	28%
Familiarità normale	168	28%	159	29%
Familiarità sufficiente	156	26%	160	29%
Scarsa familiarità	78	13%	57	10%
Non familiare	32	5%	24	4%
Totale	609	100%	556	100%

Campione utilizzato nella seguente analisi	577		532

Parte 2. Ruolo e caratteristiche organizzative

D1. Quale tra queste cariche descrive meglio la sua posizione all'interno dell'organizzazione?	Stati Uniti		EMEA
Dirigente/VP	4%		3%
Direttore	22%		15%
Manager	29%		30%
Supervisore	24%		26%
Personale/tecnico	18%		23%
Contraente	0%		1%
Altro (specificare)	3%		2%
Totale	100%		100%

D2. In quanti paesi all'incirca la sua organizzazione ha delle attività aziendali?	Stati Uniti		EMEA
Uno	23%		9%
Da 2 a 5	25%		23%
Da 6 a 10	14%		23%
Più di 10	38%		45%
Totale	100%		100%
Valore estrapolato	7,93		9,49

D3. Quanti dipendenti a tempo pieno sono presenti nella sua organizzazione globale?	Stati Uniti	EMEA
Meno di 1.000	37%	41%
Da 1.001 a 5.000	35%	31%
Da 5.001 a 10.000	13%	14%
Da 10.001 a 25.000	8%	9%
Da 25.001 a 75.000	3%	2%
Più di 75.000	4%	3%
Totale	100%	100%
Valore estrapolato	8.458	7.317

D4. A quanto potrebbe ammontare la percentuale media di soluzioni aziendali a carattere commerciale open source utilizzate nella sua organizzazione?	Stati Uniti	EMEA
Meno di 10%	35%	40%
Da 10 a 25%	18%	20%
Da 26 a 50%	15%	16%
Da 26 a 75%	15%	11%
Più di 75%	9%	6%
Impossibile da determinare	8%	7%
Totale	100%	100%
Valore estrapolato	30%	25%

D5. Qual è il sistema operativo principalmente utilizzato nella sua organizzazione? Selezionarne solo uno.	Stati Uniti	EMEA
Linux	36%	39%
Windows	43%	41%
Mac	16%	14%
Altro (specificare)	5%	6%
Totale	100%	100%

D6. La sua organizzazione applica politiche sulla sicurezza e la privacy dei dati?	Stati Uniti	EMEA
Sì, sempre	17%	25%
Sì, in alcuni casi	34%	43%
No	44%	25%
Non sono sicuro	5%	7%
Totale	100%	100%

D7. Quale tra questi settori descrive meglio il settore principale della sua organizzazione?	Stati Uniti	EMEA
Agricoltura e settore alimentare	2%	3%
Comunicazioni	3%	5%
Prodotti di consumo	5%	4%
Difesa e aerospaziale	0%	1%
Istruzione e ricerca	3%	2%
Energia e servizi	2%	4%
Spettacolo e media	5%	2%
Servizi finanziari	18%	15%
Salute e farmaceutico	8%	6%
Alberghiero	5%	4%
Industriale	8%	11%
Servizi IT	4%	5%
Servizi professionali	5%	2%
Settore pubblico	8%	15%
Commercio al dettaglio	11%	9%
Tecnologia e software	8%	7%
Trasporti	4%	5%
Altro (specificare)	1%	0%
Totale	100%	100%

Parte 3. Attribuzioni su soluzioni commerciali open source: di seguito sono elencati sei vantaggi del software commerciale open source secondo un articolo pubblicato di recente (fonte CIO Insight). Valutare ciascuna affermazione in base alla scala fornita di seguito.		
D1a. I costi saranno ridotti grazie alla flessibilità offerta dal software open source, un vantaggio non offerto dal software proprietario.	Stati Uniti	EMEA
Sono pienamente d'accordo	26%	20%
Sono d'accordo	36%	30%
Non sono sicuro	28%	30%
Non sono d'accordo	8%	15%
Non sono per niente d'accordo	2%	5%
Totale	100%	100%

D1b. Sarà possibile aumentare la qualità perché le soluzioni commerciali open source sono collaborative e sono in continuo miglioramento.	Stati Uniti	EMEA
Sono pienamente d'accordo	31%	30%
Sono d'accordo	32%	30%
Non sono sicuro	24%	24%
Non sono d'accordo	10%	14%
Non sono per niente d'accordo	3%	2%
Totale	100%	100%

D1c. Sarà possibile aver maggior controllo, a differenza del mondo delle soluzioni proprietarie dove i fornitori definiscono il codice e i budget. In una soluzione commerciale open source, è possibile modificare il codice per adattarlo alle proprie esigenze rispettando il budget.	Stati Uniti	EMEA
Sono pienamente d'accordo	26%	23%
Sono d'accordo	32%	30%
Non sono sicuro	30%	28%
Non sono d'accordo	9%	16%
Non sono per niente d'accordo	3%	3%
Totale	100%	100%

D1d. Sarà possibile garantire la continuità, a differenza di quando una società di software proprietario fallisce o sospende l'assistenza a un prodotto software. Quando un leader di soluzioni commerciali open source abbandona un progetto o una comunità, altri ne prendono il posto.	Stati Uniti	EMEA
Sono pienamente d'accordo	33%	29%
Sono d'accordo	41%	38%
Non sono sicuro	18%	20%
Non sono d'accordo	6%	11%
Non sono per niente d'accordo	2%	2%
Totale	100%	100%

D1e. Il suo reparto sarà migliore: grazie alle comunità open source e alla collaborazione interna, il team tecnico comprenderà meglio le pratiche IT generali, le risorse e gli strumenti che consentono di servire al meglio l'organizzazione.	Stati Uniti	EMEA
Sono pienamente d'accordo	39%	30%
Sono d'accordo	35%	27%
Non sono sicuro	19%	23%
Non sono d'accordo	5%	16%
Non sono per niente d'accordo	2%	4%
Totale	100%	100%

D1f. Gli utenti riscontreranno meno problemi. Si può contare sulle continue verifiche del codice di base a cura dei molti membri della comunità che si impegnano a identificare i problemi e a risolverli velocemente ed efficacemente.	Stati Uniti	EMEA
Sono pienamente d'accordo	33%	28%
Sono d'accordo	33%	27%
Non sono sicuro	21%	25%
Non sono d'accordo	9%	18%
Non sono per niente d'accordo	4%	3%
Totale	100%	100%

Parte 4. Domande generiche

Q2. Classificare il seguente elenco di tecnologie di condivisione file sulla base del livello di rischio di sicurezza delle informazioni che ciascuna tecnologia rappresenta per la sua organizzazione. Da 1 = rischio maggiore a 6 = rischio minore.	Stati Uniti	EMEA
E-mail non crittografata	1,44	2,18
E-mail crittografata	5,21	4,38
File Transfer Protocol (FTP)	2,88	2,50
Strumento di condivisione file/sincronizzazione e condivisione file su cloud	1,90	1,72
Strumento commerciale di condivisione file/sincronizzazione e condivisione file in sede	4,59	5,26
Proprio strumento di condivisione file in sede	3,13	2,16
Media	3,19	3,37

Q3. Come può essere definito il livello di coinvolgimento del reparto IT della sua organizzazione nella valutazione e/o selezione delle soluzioni di messaggistica e collaborazione?	Stati Uniti	EMEA
Coinvolgimento significativo	39%	30%
Piuttosto coinvolto	43%	53%
Nessun coinvolgimento	18%	17%
Totale	100%	100%

Q4. Qual è il livello di soddisfazione della sua organizzazione rispetto alle soluzioni attuali di messaggistica collaborativa?	Stati Uniti	EMEA
Molto soddisfatta	16%	11%
Soddisfatta	28%	24%
Piuttosto soddisfatta	20%	21%
Non soddisfatta	36%	44%
Totale	100%	100%

D5a. Quali sono gli attuali modelli di distribuzione?	Stati Uniti	EMEA
In sede	56%	69%
Cloud pubblico con host a singolo tenant	27%	22%
Cloud pubblico con host a più tenant	45%	40%
Cloud privato con host a singolo tenant	17%	24%
Soluzione ibrida cloud e in sede	45%	31%
Totale	190%	186%

D5b. Qual è il livello di soddisfazione della sua organizzazione con l'attuale modello di distribuzione?	Stati Uniti	EMEA
Molto soddisfatta	15%	12%
Soddisfatta	24%	19%
Piuttosto soddisfatta	24%	26%
Non soddisfatta	37%	43%
Totale	100%	100%

Q6. Scegliere dal seguente elenco i cinque (5) fattori più importanti per la selezione di una soluzione di messaggistica e collaborazione.	Stati Uniti	EMEA
Possibilità di hosting o gestione della soluzione nel cloud	63%	45%
Facilità di installazione	28%	26%
Facilità di gestione	37%	42%
Facilità di utilizzo	65%	44%
Migliore privacy	9%	38%
Migliore sicurezza	50%	45%
Open source	53%	57%
Supporto per l'accesso all'e-mail crittografata da dispositivi portatili	21%	17%
Certificazioni tecniche	15%	12%
Costo totale di proprietà	39%	37%
Programmi di formazione o materiali per la preparazione dell'utente	16%	15%
Reputazione del fornitore	49%	61%
Supporto del fornitore	55%	60%
Totale	500%	500%

Q7. La sua organizzazione prevede di sostituire le soluzioni di messaggistica e collaborazione?	Stati Uniti	EMEA
Entro 6 mesi	32%	18%
Entro 12 mesi	13%	23%
Entro 24 mesi	10%	11%
In più di 24 mesi	4%	2%
Non è prevista una sostituzione	41%	46%
Totale	100%	100%

Q8. In merito alle soluzioni commerciali open source di messaggistica e collaborativa, il supporto commerciale e la trasparenza del codice consentono di aumentare il profilo di sicurezza dell'soluzione?	Stati Uniti	EMEA
Sì	55%	67%
No	34%	24%
Non sono sicuro	11%	9%
Totale	100%	100%

Q9. In merito alle soluzioni commerciali open source di messaggistica e collaborazione, il supporto commerciale e la trasparenza del codice consentono di ridurre i rischi sulla privacy associati all'soluzione?	Stati Uniti	EMEA
Sì	52%	66%
No	37%	26%
Non sono sicuro	11%	8%
Totale	100%	100%

Q10. In merito alle soluzioni commerciali open source di messaggistica e collaborazione, il supporto commerciale e la trasparenza del codice consentono di aumentare l'integrità e l'affidabilità della soluzione?	Stati Uniti	EMEA
Sì	68%	76%
No	23%	16%
Non sono sicuro	9%	8%
Totale	100%	100%

Con quale frequenza i seguenti scenari si verificano in merito alla privacy e alla sicurezza del software di messaggistica di collaborazione della sua organizzazione?		
D11a. I dipendenti inviano e ricevono file non indirizzati a loro.	Stati Uniti	EMEA
Mai	8%	18%
Raramente	12%	13%
Spesso	56%	50%
Di frequente	24%	19%
Totale	100%	100%

D11b. I dipendenti non si attengono alle politiche aziendali in merito alla condivisione di documenti riservati.	Stati Uniti	EMEA
Mai	5%	16%
Raramente	6%	5%
Spesso	34%	33%
Di frequente	55%	46%
Totale	100%	100%

D11c. I dipendenti utilizzano soluzioni di messaggistica e collaborazione non autorizzate dalla società.	Stati Uniti	EMEA
Mai	11%	16%
Raramente	15%	13%
Spesso	38%	31%
Di frequente	36%	40%
Totale	100%	100%

D11d. La soluzione di messaggistica e collaborazione della società non è disponibile a causa di problemi di sicurezza.	Stati Uniti	EMEA
Mai	13%	23%
Raramente	26%	25%
Spesso	35%	24%
Di frequente	26%	28%
Totale	100%	100%

Q12. State utilizzando uno dei seguenti software di messaggistica collaborativa? Selezionare tutte le risposte applicabili.	Stati Uniti	EMEA
Zimbra	41%	30%
Microsoft Exchange	71%	61%
Microsoft Office 365	53%	44%
Google Apps/Gmail	56%	44%
IBM Domino	27%	29%
Novell GroupWise	35%	23%
Altro (specificare)	9%	9%
Nessuno dei precedenti	5%	17%
Totale	297%	257%

Q13. Quali dei seguenti tipi di soluzioni software di messaggistica e collaborativa sono utilizzati nella sua organizzazione? Selezionare tutte le risposte applicabili.	Stati Uniti	EMEA
Versioni gratuite di soluzioni di sincronizzazione e condivisione di file per utenti consumer (ad esempio Dropbox, Google)	66%	37%
Soluzioni di memorizzazione file su cloud pubblico per utenti consumer (ad esempio Box, Microsoft)	72%	57%
Condivisione di file su cloud privato classe Enterprise (ad esempio Syncplicity by EMC, Egnyte)	34%	41%
Soluzioni di condivisione file in azienda (ad esempio Accellion, IBM)	49%	65%
Nessuno dei precedenti	5%	7%
Totale	226%	207%

Parte 5. Funzionalità del prodotto: Più di 200.000 società si avvalgono di Zimbra, con più di 100 milioni di utenti commerciali e 500 milioni di utenti gratuiti globalmente. Valutare ciascuna funzionalità in base all'importanza nella scelta della soluzione di messaggistica di collaborazione per la sua organizzazione.

D14a. Hub per soluzioni e-mail, social e sincronizzazione e condivisione di file, comprese integrazioni con terze parti	Stati Uniti	EMEA
Molto importante	36%	28%
Importante	33%	31%
Importante a volte	16%	25%
Non importante	8%	11%
Irrilevante	7%	5%
Totale	100%	100%

D14b. Calendario, contatti e attività integrati, fruibili con altre soluzioni e-mail e di calendario	Stati Uniti	EMEA
Molto importante	36%	37%
Importante	32%	33%
Importante a volte	19%	22%
Non importante	8%	6%
Irrilevante	5%	2%
Totale	100%	100%

D14c. Possibilità di crittografare e firmare digitalmente e-mail su computer desktop e dispositivi portatili	Stati Uniti	EMEA
Molto importante	29%	26%
Importante	33%	29%
Importante a volte	23%	26%
Non importante	8%	13%
Irrilevante	7%	5%
Totale	100%	100%

D14d. Supporto per servizi antispam, antivirus e autenticazione a due fattori di terzi	Stati Uniti	EMEA
Molto importante	41%	32%
Importante	34%	36%
Importante a volte	16%	21%
Non importante	8%	6%
Irrilevante	1%	5%
Totale	100%	100%

Q14e Come valuta la possibilità di impostare politiche di sicurezza mobile, inclusi cancellazione dei dati, soluzione di PIN e funzionalità di gestione del dispositivo sugli account utente?	Stati Uniti	EMEA
Molto importante	25%	19%
Importante	29%	25%
Importante a volte	23%	29%
Non importante	15%	19%
Irrilevante	8%	9%
Totale	100%	100%

D14f. Supporto per la crittografia dei dati memorizzati e in movimento	Stati Uniti	EMEA
Molto importante	26%	20%
Importante	29%	25%
Importante a volte	22%	32%
Non importante	16%	15%
Irrilevante	7%	8%
Totale	100%	100%

D14g. Piena compatibilità con smartphone e tablet iOS, Android, BlackBerry e Windows	Stati Uniti	EMEA
Molto importante	48%	36%
Importante	30%	30%
Importante a volte	13%	22%
Non importante	8%	12%
Irrilevante	1%	0%
Totale	100%	100%

D14h. Opzioni di implementazione flessibili: in sede, cloud pubblico con host a singolo tenant, cloud pubblico con host a più tenant, cloud privato con host a singolo tenant, soluzione ibrida cloud e in sede	Stati Uniti	EMEA
Molto importante	46%	31%
Importante	29%	30%
Importante a volte	15%	24%
Non importante	8%	12%
Irrilevante	2%	3%
Totale	100%	100%

D14i. Come valuta la possibilità di mantenere il controllo sulla residenza dei dati per consentire ai dati delle organizzazioni di rimanere in giurisdizioni definite e assicurare la conformità alle leggi sulla privacy dei dati?	Stati Uniti	EMEA
Molto importante	23%	23%
Importante	29%	27%
Importante a volte	26%	28%
Non importante	18%	20%
Irrilevante	4%	2%
Totale	100%	100%

D14j. Forte integrazione di soluzioni e-mail e sincronizzazione e condivisione di file che supportano allegati privati per assicurare che solo il destinatario previsto possa accedere ai file (in base all'indirizzo e-mail)	Stati Uniti	EMEA
Molto importante	39%	36%
Importante	31%	25%
Importante a volte	19%	19%
Non importante	10%	15%
Irrilevante	1%	5%
Totale	100%	100%

D14l. Dettagliato controllo di accesso e delle autorizzazioni di allegati/condivisione di file che consente di mantenere la conformità normativa in merito a documenti sensibili e risorse digitali	Stati Uniti	EMEA
Molto importante	35%	34%
Importante	35%	37%
Importante a volte	15%	13%
Non importante	9%	13%
Irrilevante	6%	3%
Totale	100%	100%

D14m. Possibilità di estendere il software di collaborazione in un'architettura aperta per consentire di creare o sfruttare i flussi di lavoro specifici del settore della società (ad esempio HIPAA)	Stati Uniti	EMEA
Molto importante	23%	25%
Importante	20%	29%
Importante a volte	29%	18%

Non importante	21%	22%
Irrilevante	7%	6%
Totale	100%	100%

D14n. Un sistema e-mail basato su cloud con funzionalità di privacy dei dati adeguate per garantire la conformità alle normative applicabili di protezione dei dati	Stati Uniti	EMEA
Molto importante	24%	28%
Importante	21%	29%
Importante a volte	30%	20%
Non importante	20%	21%
Irrilevante	5%	2%
Totale	100%	100%

D14o. Funzionalità per controllare e gestire il contenuto, compresi versione dei documenti, metadati, individuazione elettronica, archiviazione e sincronizzazione	Stati Uniti	EMEA
Molto importante	21%	20%
Importante	29%	25%
Importante a volte	32%	26%
Non importante	15%	23%
Irrilevante	3%	6%
Totale	100%	100%

D14p. Come valuta la funzionalità di gestione, accesso o integrazione con servizi posteriori come file system di rete, directory, sistemi di gestione, archivi e soluzioni aziendali?	Stati Uniti	EMEA
Molto importante	23%	19%
Importante	23%	25%
Importante a volte	31%	29%
Non importante	17%	20%
Irrilevante	6%	7%
Totale	100%	100%

Composizione dei paesi del gruppo EMEA	Freq.	Perc%
Danimarca	12	2%
Francia	69	10%
Germania	98	15%
Grecia	7	1%
Irlanda	22	3%
Israele	10	1%
Italia	41	6%
Olanda	35	5%
Polonia	29	4%
Federazione Russa	48	7%
Arabia Saudita	43	6%
Sudafrica	23	3%
Spagna	48	7%
Svezia	12	2%
Svizzera	13	2%
Turchia	30	4%

Emirati Arabi Uniti	27	4%
Regno Unito	108	16%
Totale	675	100%

Per ulteriori informazioni sulla presente indagine, contattare il Ponemon Institute inviando una e-mail all'indirizzo research@ponemon.org o chiamando il numero verde 1.800.887.3118.

Ponemon Institute

Miglioramento della gestione dell'informazione responsabile

Il Ponemon Institute si dedica alla ricerca indipendente e alla formazione che consentono il miglioramento delle pratiche di gestione dell'informazione responsabile e della privacy nel settore aziendale e governativo. L'Istituto ha la missione di condurre studi empirici di alta qualità su problematiche critiche con impatto sulla gestione e la sicurezza di informazioni sensibili su persone e organizzazioni.

In quanto membro del **Council of American Survey Research Organizations (CASRO)**, l'istituto garantisce i massimi standard sulla riservatezza dei dati, della privacy e della ricerca etica. Non vengono raccolte informazioni che consentono l'identificazione personale degli individui (o informazioni che consentono l'identificazione societaria nelle ricerche aziendali). Inoltre, si applicano standard elevati di qualità per assicurare che ai soggetti non vengano poste domande non pertinenti, irrilevanti o inappropriate.