The Open Source Collaboration Study: Viewpoints on Security & Privacy in the US & EMEA

Sponsored by Zimbra

Independently conducted by Ponemon Institute LLC

Publication Date: November 2014

The Open Source Collaboration Study: Viewpoints on Security & Privacy in the US & EMEA

Ponemon Institute, November 2014

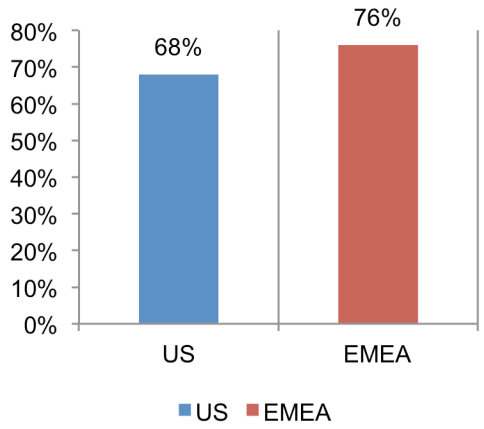
Part 1. Introduction

Ponemon Institute is pleased to present the findings of *The Open Source Collaboration Study: Viewpoints on Security & Privacy in the US & EMEA* sponsored by Zimbra. The purpose of this research is to learn from IT and IT security practitioners about their companies' involvement in the use of open source messaging and collaboration solutions and their perceptions about the benefits.

We surveyed 723 IT and IT security practitioners in the United States and 675 IT and IT security practitioners in the following 18 EMEA countries: United Kingdom, Germany, France, Russian Federation, Spain, Saudi Arabia, Italy, Netherlands, Turkey, Poland, United Arab Emirates, South Africa, Ireland, Switzerland, Denmark, Sweden, Israel and Greece.

The majority of respondents (57 percent) in the US and EMEA are either very familiar or familiar about their organizations' security and data privacy policies or requirements. Fifty-five percent of US respondents and 48 percent of EMEA respondents are at the manager level or above.

Figure 1. Does commercial backing & code transparency increase the trustworthiness of the application? (Yes responses)



As shown in Figure 1, respondents in the US and EMEA believe commercial backing and code transparency increases the trustworthiness of the application. When asked how involved their IT department is in the evaluation and/or selection of messaging and collaboration, 39 percent of US respondents and 30 percent of EMEA respondents say it has significant involvement. According to 84 percent of US and 82 percent of EMEA respondents, their organization attempts to control the ratio of open source software to proprietary business applications. The average percentage of business applications that is commercial open source is 30 percent in the US and 25 percent in EMEA.

In this study, we define open source software (OSS) as computer software with its source code made available with a license in which the copyright holder provides the rights to study, change and distribute the software to anyone and for any purpose. Open source software is very often developed in a public, collaborative manner.

Following are the key findings from this study:

An assurance of continuity with commercial open source applications is believed to be the most important benefit. Respondents in general are very positive about commercial open source applications, especially about the assurance of continuity**.**

Despite benefits, companies are slow to adopt. The average percentage of business applications used by their organization that is commercial open source is 30 percent in the US and 25 percent in EMEA.

EMEA organizations are more likely to enforce security and data privacy policies. Throughout this study, there is evidence that EMEA organizations are more concerned with the privacy consequences of messaging and collaboration. US organizations focus more on security.

Security, privacy and trustworthiness of applications are all improved with commercial backing and code transparency. Respondents agree with the improvements created by commercial backing and code transparency for commercial open source messaging and collaboration solutions. EMEA respondents are most positive, especially about the reduction of privacy risks (66 percent of EMEA respondents and 52 percent of US respondents).

What factors in messaging and collaboration solutions are important? US respondents say it is ease of use and EMEA respondents say vendor support is most important when selecting a messaging and collaboration solution.

Part 2. Key findings

In this section, we analyze the findings of this research. The complete audited findings are presented in the appendix of this report. The report is organized according to the following themes:

- Positive perceptions about commercial open source applications
- Security and privacy risks in messaging and collaboration
- Importance of messaging and collaboration solution features
- Future outlook for adoption

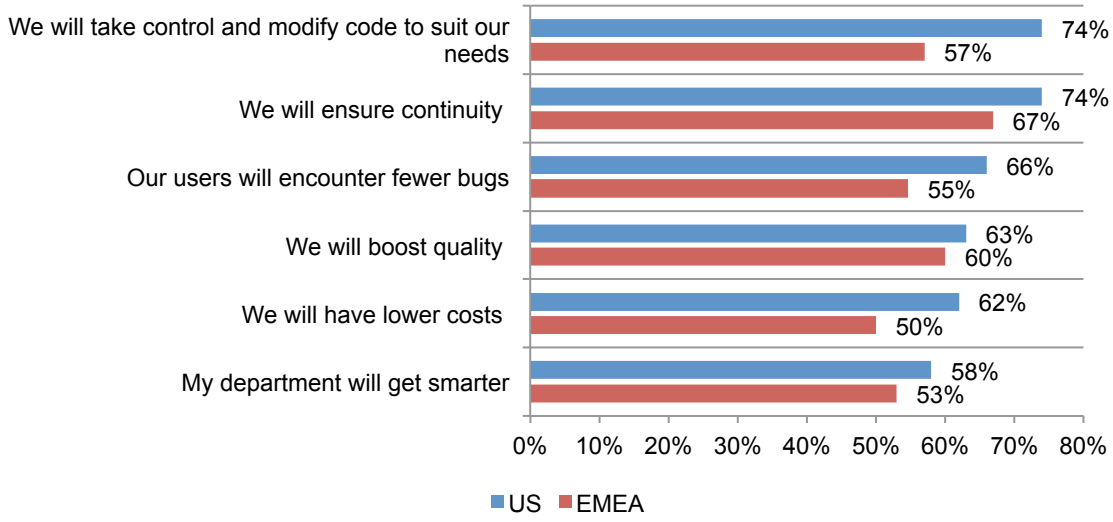
Positive perceptions about commercial open source applications

In this study, commercial open source is defined as an open source project that is backed by a commercial entity. In contrast, a community open source project does not have commercial backing. Commercial open source also differs from a commercial proprietary program, which is the standard closed system proprietary methodology backed by a commercial entity.

An assurance of continuity with commercial open source applications is believed to be the most important benefit. Respondents in general are very positive about commercial open source applications, especially about the assurance of continuity**.** However, as shown in Figure 2, US respondents are even more so. Specifically, US respondents have a higher level of agreement that their departments will get smarter—through both open source communities and internal collaboration and the tech team will get a better sense of the overall IT practices, resources and tools out there to best serve your organization (74 percent of US respondents and 57 percent of EMEA respondents).

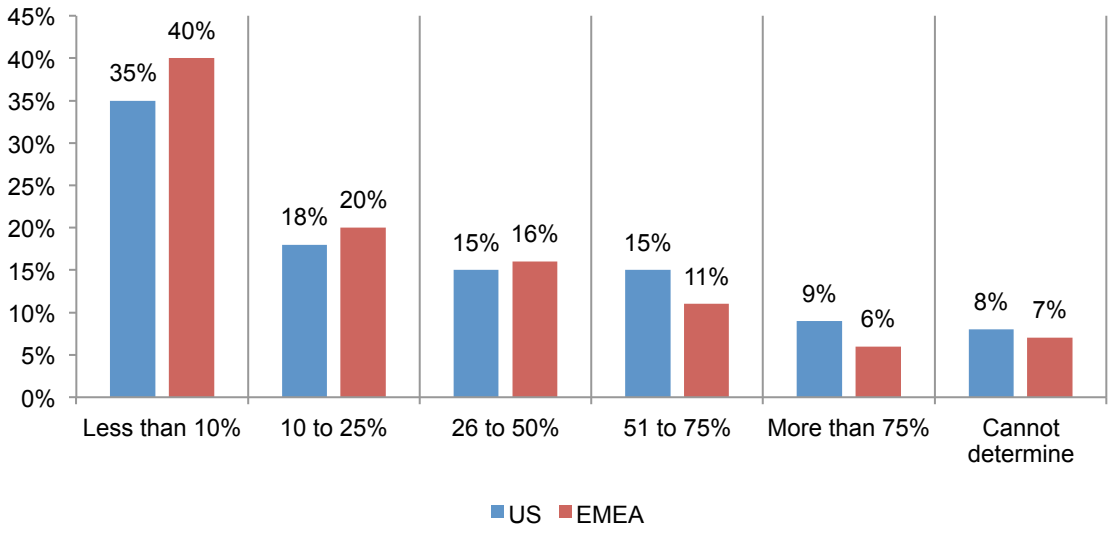
Other big differences between the US and EMEA are the ability to lower costs because open source software provides flexibility not offered by proprietary software (62 percent of US respondents vs. 50 percent of EMEA respondents) and fewer bugs because the many community members are constantly scrutinizing the codebase to ensure bugs are found and fixed quickly and effectively (66 percent of US respondents and 55 percent of EMEA respondents).

Figure 2. Why is commercial open source better than commercial proprietary software?
Strongly agree and agree response combined



Despite benefits, companies are slow to adopt. According to Figure 3, the average percentage of business applications used by their organization that is commercial open source is 30 percent in the US and 25 percent in EMEA. Thirty-nine percent of US respondents and 30 percent of EMEA respondents say their organizations' IT department is involved in the evaluation and/or selection of messaging and collaboration solutions.

Figure 3. Percentage of business applications that are commercial open source
Extrapolated value: US = 30 percent, EMEA = 25 percent

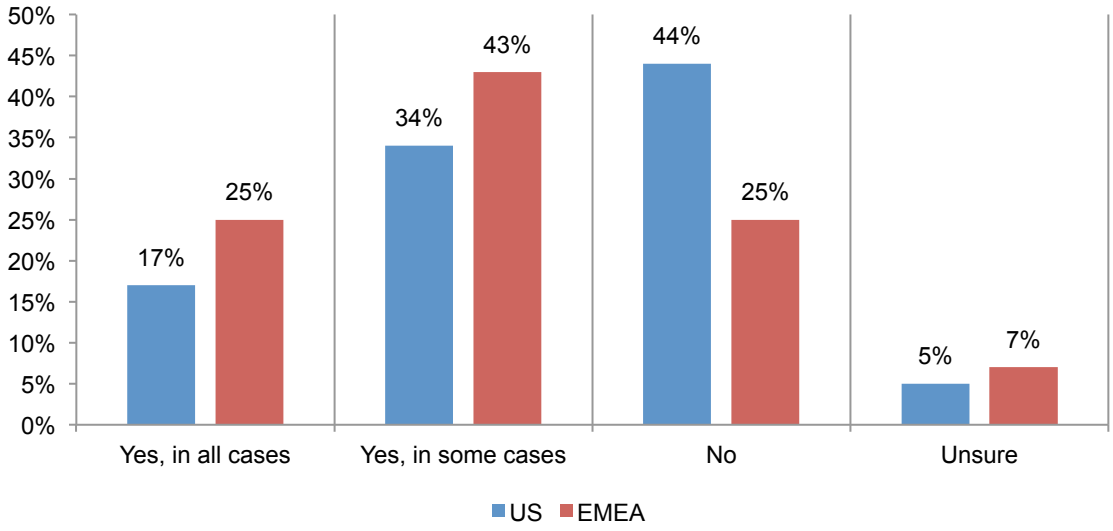


Security and privacy risks in messaging and collaboration

EMEA organizations are more likely to enforce security and data privacy policies. Throughout this study, there is evidence that EMEA organizations are more concerned with the privacy consequences of messaging and collaboration. US organizations focus more on security.

According to the findings, 57 percent of respondents in the US and EMEA are very familiar or familiar with their organizations' overall information security and data privacy policies or requirements. As shown in Figure 4, a higher percentage of US respondents say the organization does not enforce its security and data privacy policies than their EMEA counterparts (44 percent vs. 25 percent).

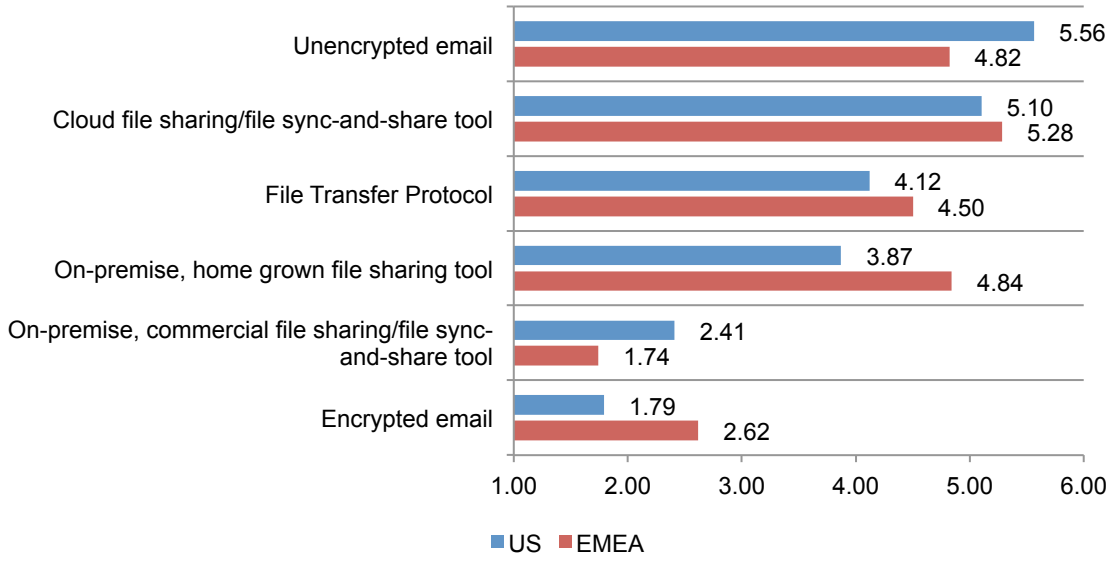
Figure 4. Does your organization enforce its security and data privacy policies?



Unencrypted email is considered the most risky file sharing technology. Respondents in both the US and EMEA believe unencrypted email followed by cloud file sharing/file sync-and-share tool are the most risky ways to share documents (Figure 5).

Least risky is encrypted email. Some interesting differences include the perception by US respondents that the use of unencrypted email is more risky. Whereas, EMEA respondents are more concerned about cloud file sharing/file sync-and-share tools.

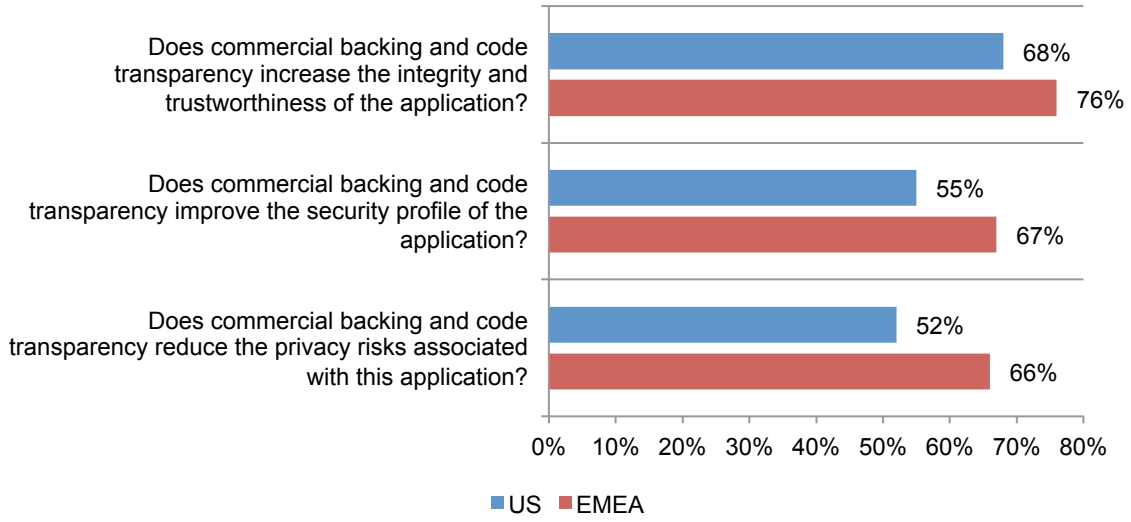
Figure 5. File sharing technologies that pose the greatest risk
6 = highest risk to 1 = lowest risk



Security, privacy and trustworthiness of applications are all improved with commercial backing and code transparency. According to Figure 6, respondents agree with the improvements created by commercial backing and code transparency for commercial open source messaging and collaboration solutions. EMEA respondents are most positive, especially about the reduction of privacy risks (66 percent of EMEA respondents and 52 percent of US respondents).

In addition, 67 percent of EMEA and 55 percent of US respondents say it improves the security profile of the application and risks. Seventy-six percent of EMEA and 68 percent of US respondents say it increases the integrity and trustworthiness of the application.

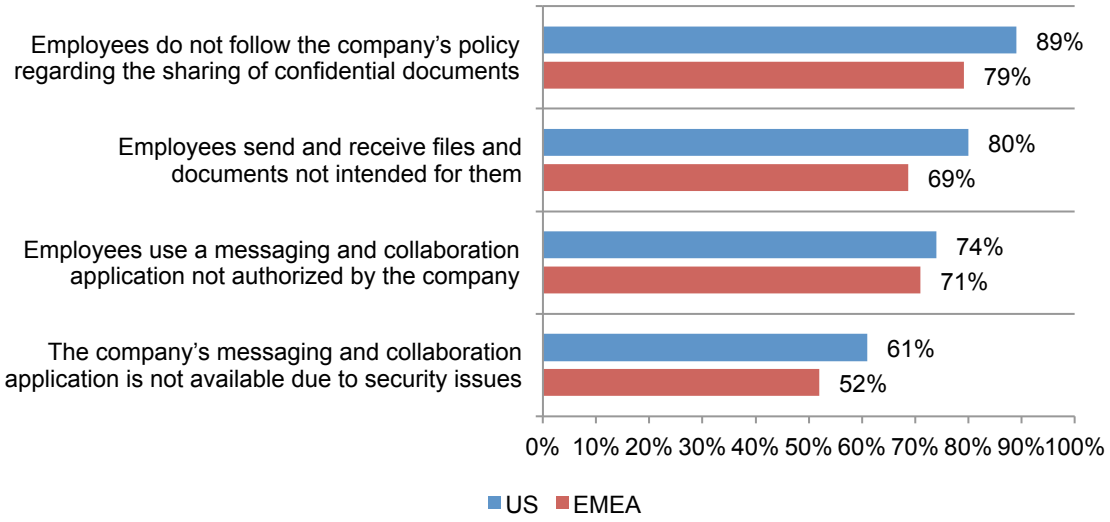
Figure 6. Does commercial backing and code transparency improve security, reduce privacy risks and increase trustworthiness?
Yes responses



Employees increase privacy and security risks. US employees are more likely than EMEA employees to put their organizations' messaging and collaboration solutions at risk. Figure 7 shows four practices that are threats to an organization's confidential documents. US respondents are more likely to believe their organizations have a problem with employees.

However, according to respondents in both regions, the risk is high when employees are not following the company's policy regarding the sharing of confidential documents, sending and receiving files not intended for them and using a messaging and collaboration application not authorized by the company. Sixty-one percent of respondents in the US and 52 percent in EMEA report that their companies' messaging and collaboration applications have been unavailable due to security issues.

Figure 7. Employees increase privacy and security risks
Often and frequently response combined



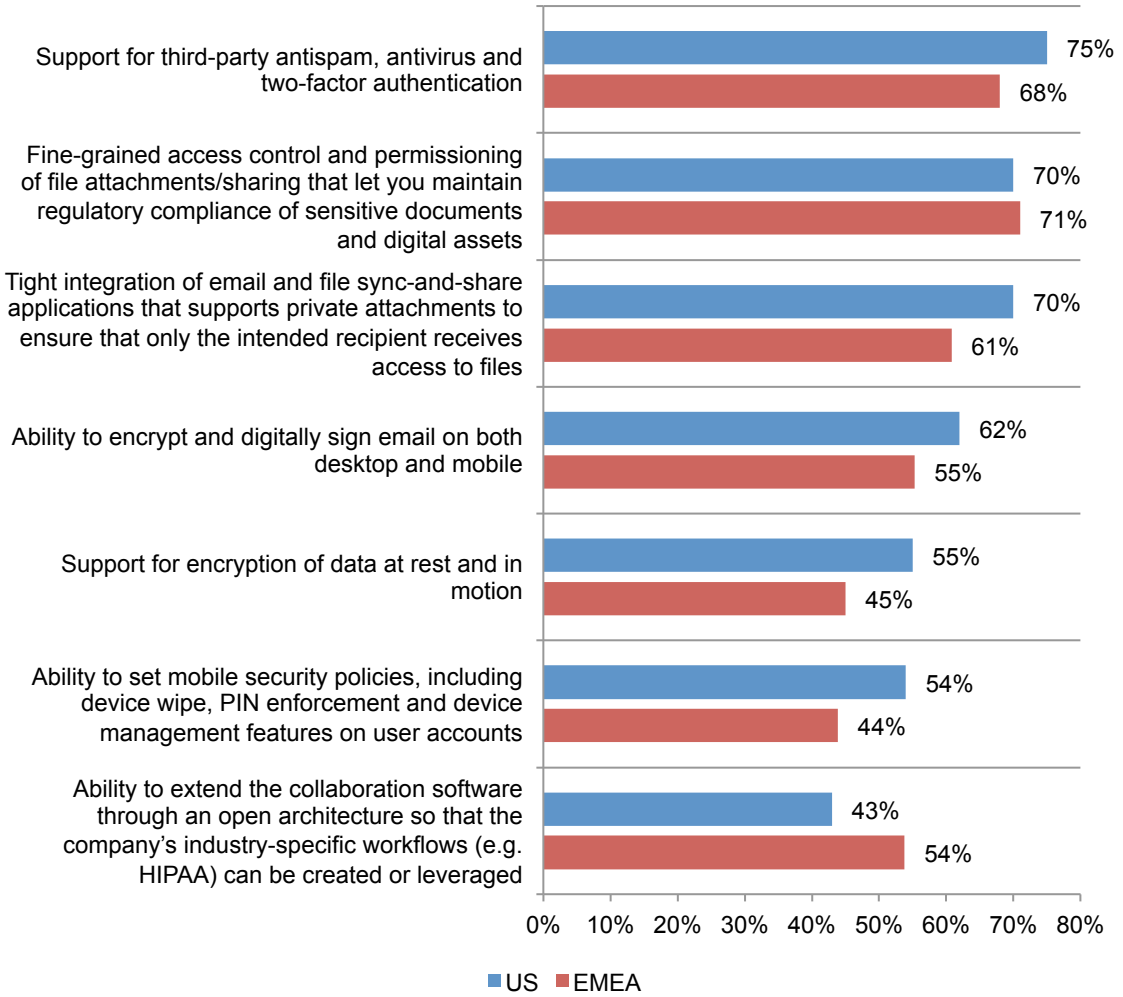
Importance of messaging and collaboration solution features

More than 200,000 companies use Zimbra, with more than 100 million commercial users and 500 million free users globally. Respondents were asked to rate the features most important to their organization.

EMEA and US respondents have security and privacy priorities. As shown in Figure 8, both the US and EMEA agree that support for third-party antispam, antivirus and two-factor authentication is important as well as the ability to maintain control over data residency so that the organization's data stays within defined jurisdictions and ensures compliance with data privacy laws.

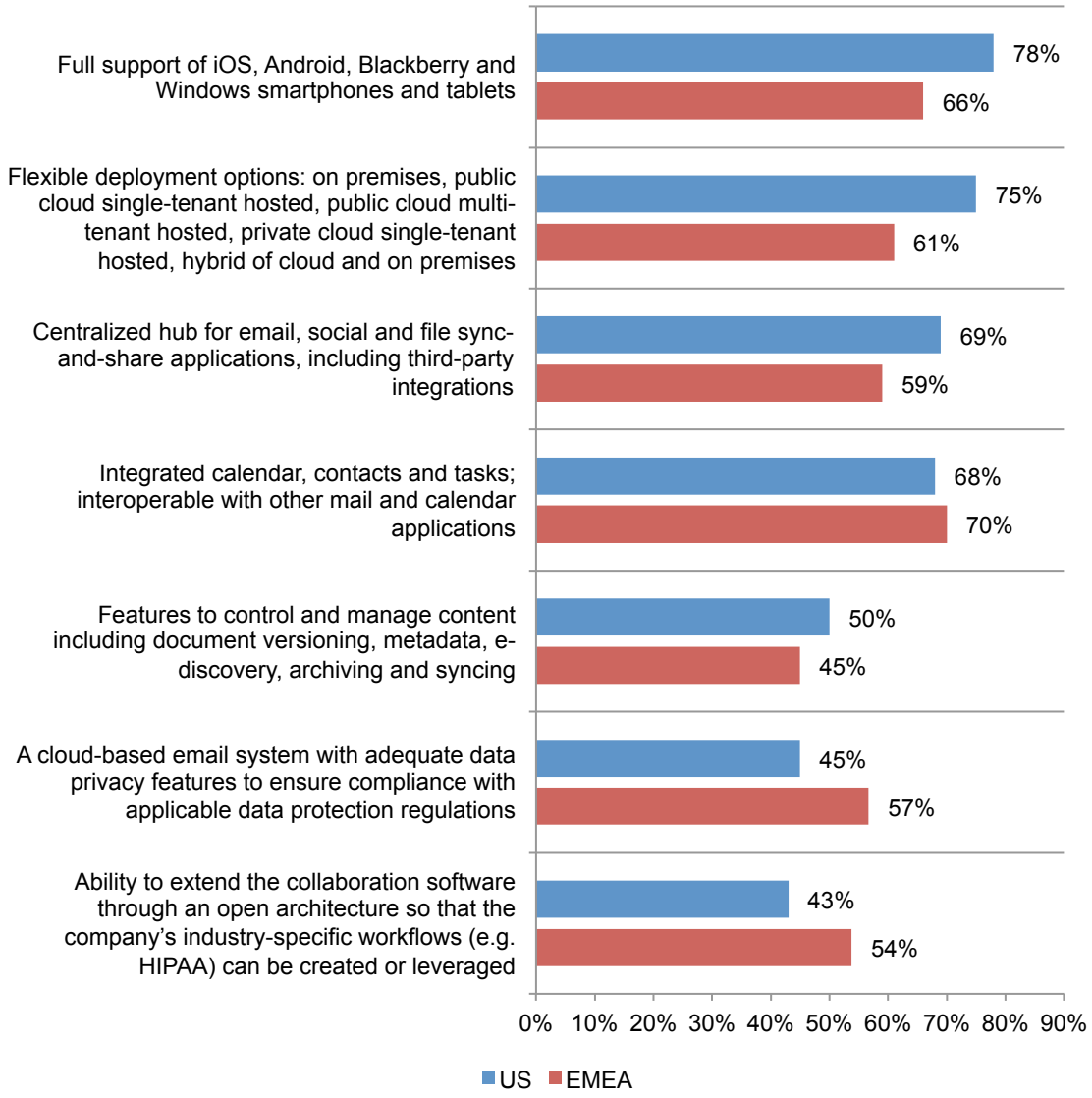
Major differences between respondents in the US and EMEA include the ability to extend the collaboration software through an open architecture so that the company's industry-specific workflows (e.g. HIPAA) can be created or leveraged. US respondents are more likely to believe that support for encryption of data at rest and in motion and the ability to set mobile security policies are critical.

Figure 8. Most messaging and collaboration privacy and security features
Very important and important response combined



Respondents in the US and EMEA have different priorities for messaging and collaboration solutions. The top features for US are full support of iOS, Android, Blackberry and Windows smartphones and tablets, support for third-party antispam, antivirus and two-factor authentication and flexible deployment options for the cloud. EMEA respondents believe it is important to have integrated calendar, contacts and tasks and interoperability with other mail and calendar applications. Figure 9 reveals the biggest differences between US and EMEA respondents.

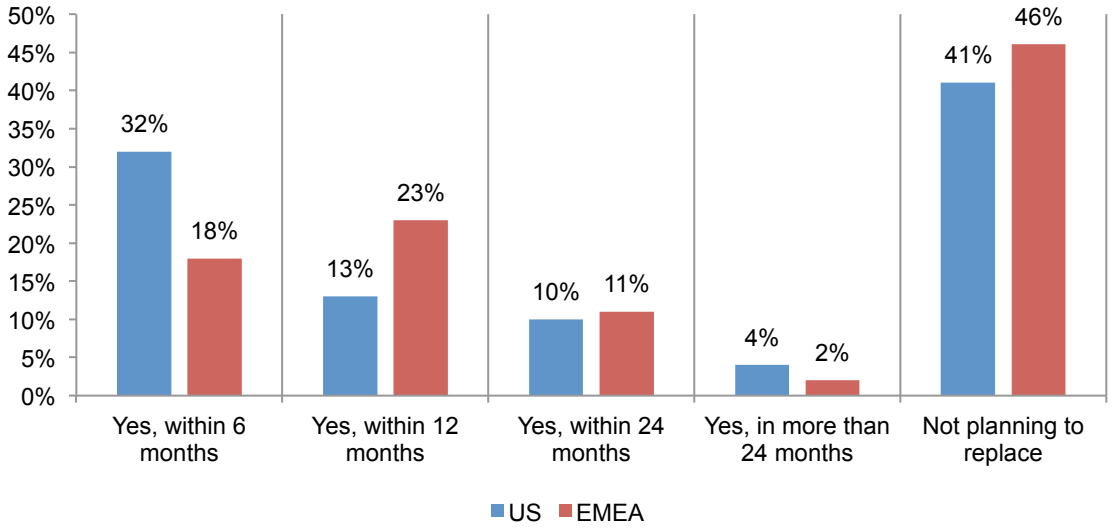
Figure 9. More important features for messaging and collaboration
Very important and important response combined



Future outlook for adoption

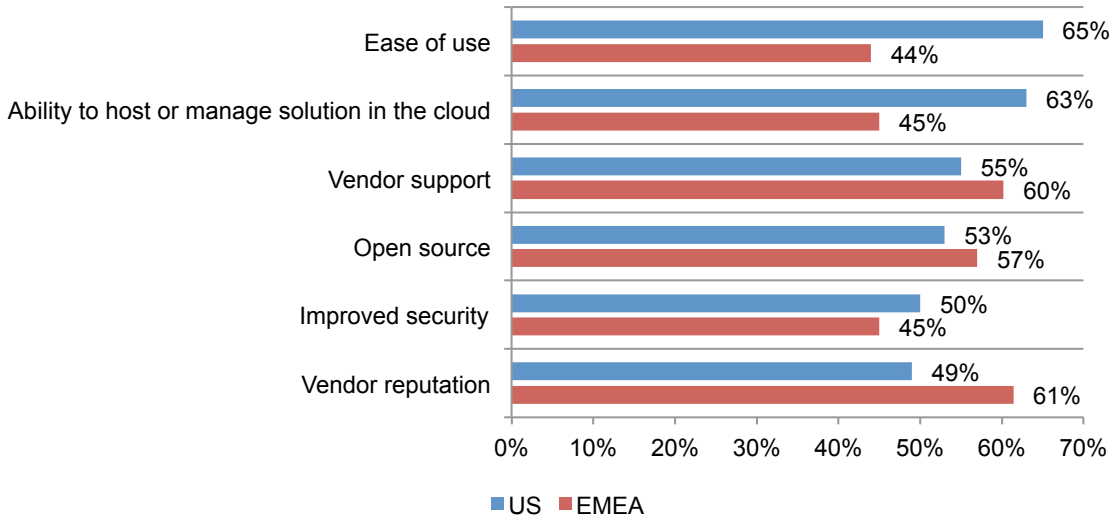
Most respondents are only somewhat or not satisfied with their current messaging and collaboration solutions. Consequently, as shown in Figure 10, 55 percent of US respondents and 52 percent of EMEA respondents say their organizations will be replacing their messaging and collaboration solutions within two years. A slightly higher percentage of EMEA respondents (46 percent) than US respondents (41 percent) do not plan to replace their current messaging and collaboration solution.

Figure 10. When do you plan to replace your current messaging and collaboration solution?



What factors in a messaging and collaboration solutions are important? US respondents say it is ease of use and EMEA respondents say vendor reputation is most important when selecting a messaging and collaboration solution. The biggest difference between respondents in the US and EMEA is ease of use followed by ability to host or manage solutions in the cloud.

Figure 11. Most important factors for selecting a messaging and collaboration solution
Five responses permitted



Part 3. Conclusion

Overall, IT professionals' perceptions of commercial open source software for messaging and collaboration are more positive than their perceptions of proprietary software. Common to both the US and EMEA, is IT professionals' dissatisfaction with their current messaging and collaboration platforms, the majority of which are proprietary solutions. And, while IT professionals in the US and EMEA disagree on the relative importance of security versus privacy, there is agreement among IT professionals that commercial open source software offers better cost, control, quality and business continuity than proprietary software.

Part 4. Methods

A sampling frame of 17,680 US and 16,700 EMEA experienced IT and IT security practitioners were selected as participants to this survey. Table 1 shows 1,584 total returns. Screening and reliability checks required the removal of 186 surveys. Our final sample consisted of 1,398 surveys or a 4.1% percent response rate for the US and 4.0 percent response rate for the EMEA.

Table 1. Survey response

Regional clusters	Sampling frames	Total returns	Rejected or screened surveys	Final sample	Response rate
US	17,680	821	98	723	4.1%
EMEA	16,700	763	88	675	4.0%

Figure 12 reports the respondent's organizational level within participating organizations. By design, 79 percent of US respondents and 74 percent of EMEA respondents are at or above the supervisory levels.

Figure 12. Current position within the organization

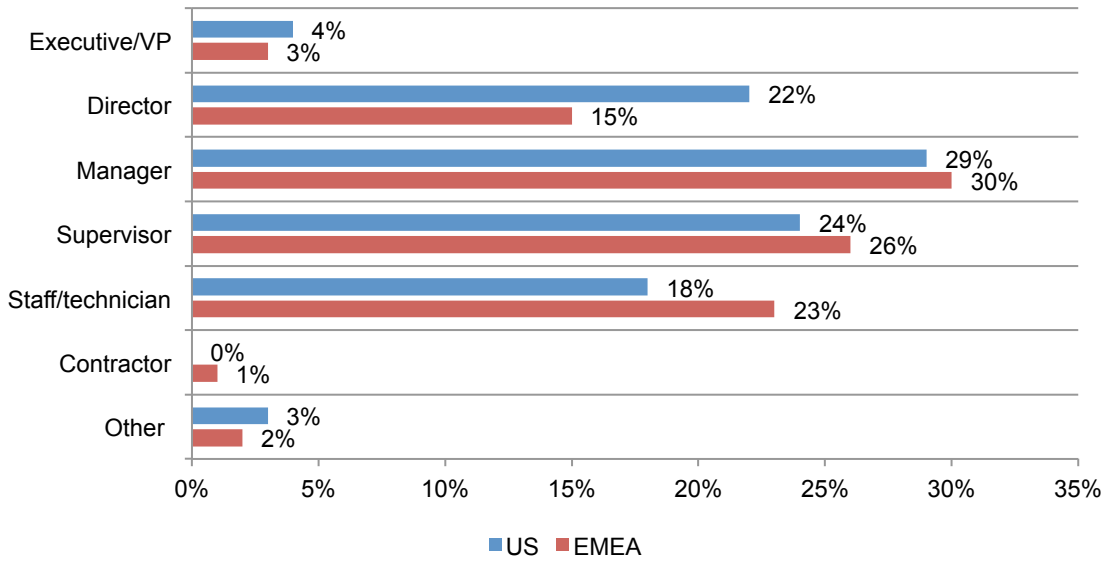


Figure 13 reports the number of countries the respondent's organizations have business operations in. The extrapolated value for the US is 7.93 countries and for the EMEA is 9.49 countries.

Figure 13. How many countries does your organization have business operations?

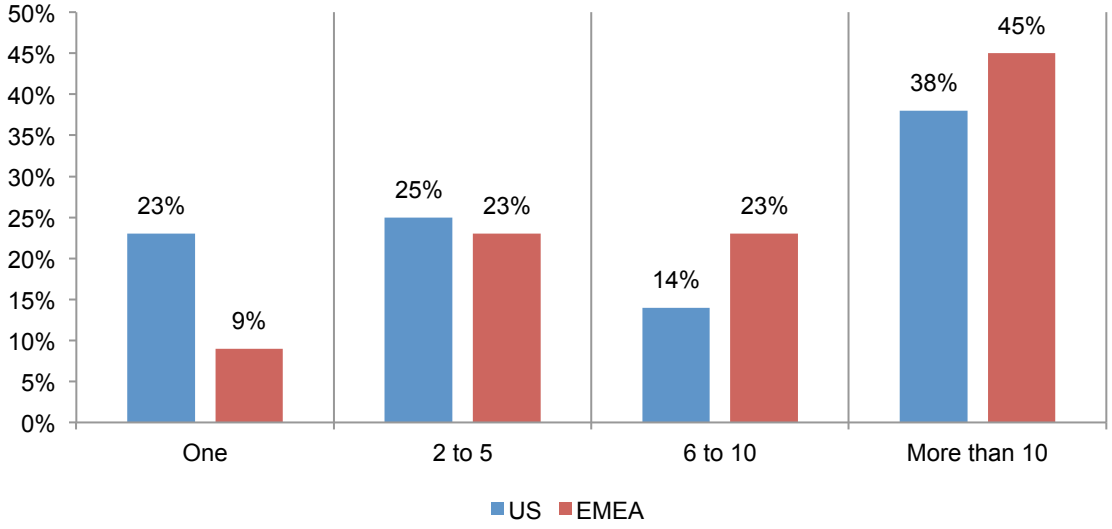


Figure 14 reports the full-time headcount of the respondent's global organization. The extrapolated value for the US is 8,458 employees and 7,317 employees for the EMEA.

Figure 14. The full-time headcount of your global organization

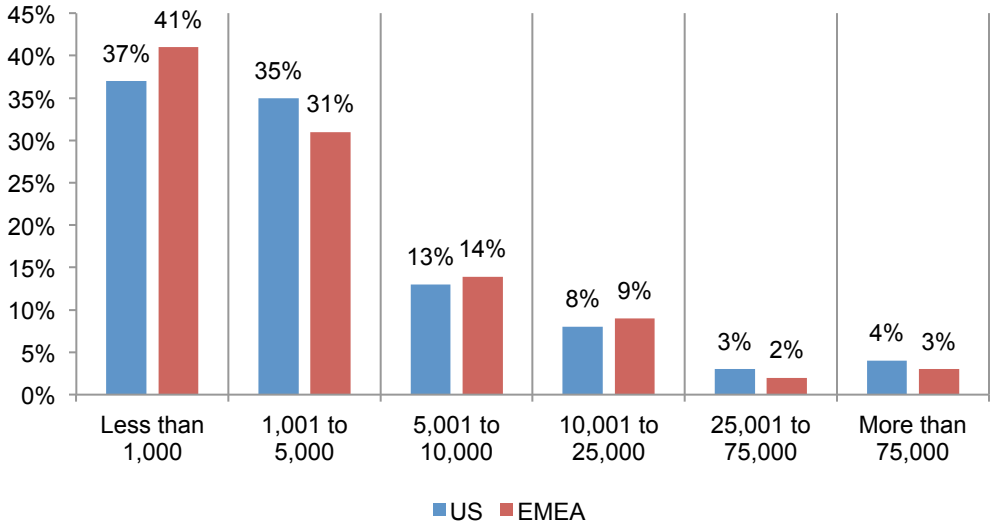
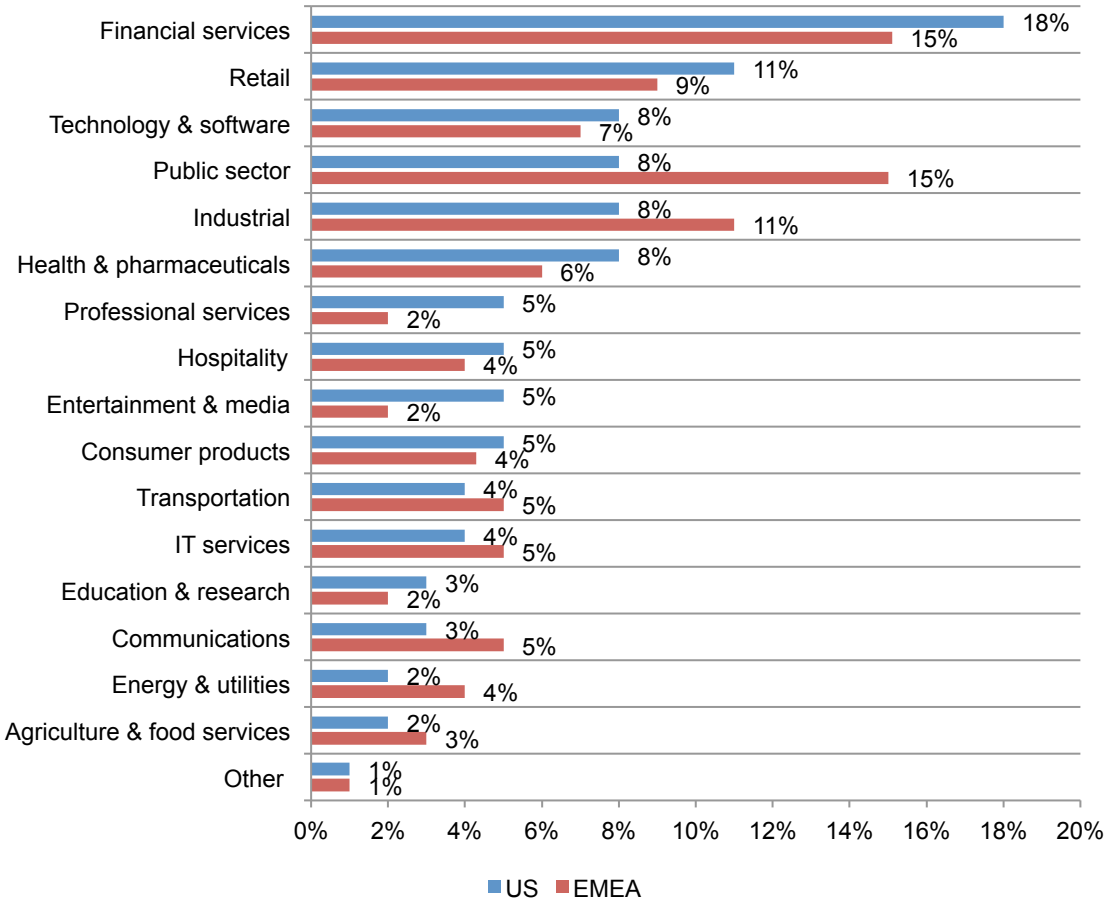


Figure 15 reports the primary industry classification of respondents' organizations. This chart identifies financial services as the largest segment for both the US (18 percent) and EMEA (15 percent).

Figure 15. The organization's primary industry classification



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals located in two global regions, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate response.

Appendix: Detailed Survey Results

The following tables provide the percentage frequency of responses to all survey questions on a consolidated (global) basis across four regional clusters. All survey responses were captured in October 2014.

Survey response	Freq	US	Freq	EMEA
Total sampling frame	17,680	100.0%	16,700	100.0%
Total returns	821	4.6%	763	4.6%
Rejected or screened surveys	98	0.6%	88	0.5%
Final sample	723	4.1%	675	4.0%

S1. Does your organization attempt to control the ratio of open source software to proprietary business applications?	Freq	US	Freq	EMEA
Yes	609	84%	556	82%
No	114	16%	119	18%
Total	723	100%	675	100%

S2. What best describes your familiarity with your organization's overall information security and data privacy policies or requirements?	Freq	US	Freq	EMEA
Very familiar	175	29%	156	28%
Familiar	168	28%	159	29%
Somewhat familiar	156	26%	160	29%
Not familiar	78	13%	57	10%
No knowledge	32	5%	24	4%
Total	609	100%	556	100%

Sample used in the following analysis	577		532

Part 2. Role & organizational characteristics

D1. What best describes your position within your organization?	US		EMEA
Executive/VP	4%		3%
Director	22%		15%
Manager	29%		30%
Supervisor	24%		26%
Staff/technician	18%		23%
Contractor	0%		1%
Other (please specify)	3%		2%
Total	100%		100%

D2. In approximately how many countries does your organization have business operations?	US		EMEA
One	23%		9%
2 to 5	25%		23%
6 to 10	14%		23%
More than 10	38%		45%
Total	100%		100%
Extrapolated value	7.93		9.49

D3. What range best describes the full-time headcount of your global organization?	US	EMEA
Less than 1,000	37%	41%
1,001 to 5,000	35%	31%
5,001 to 10,000	13%	14%
10,001 to 25,000	8%	9%
25,001 to 75,000	3%	2%
More than 75,000	4%	3%
Total	100%	100%
Extrapolated value	8,458	7,317

D4. Please estimate the percentage of business applications used by your organization that is commercial open source.	US	EMEA
Less than 10%	35%	40%
10 to 25%	18%	20%
26 to 50%	15%	16%
51 to 75%	15%	11%
More than 75%	9%	6%
Cannot determine	8%	7%
Total	100%	100%
Extrapolated value	30%	25%

D5. What best defines your organization's primary operating system? Please select only one.	US	EMEA
Linux	36%	39%
Windows	43%	41%
Mac	16%	14%
Other (please specify)	5%	6%
Total	100%	100%

D6. Does your organization enforce its security and data privacy policies?	US	EMEA
Yes, in all cases	17%	25%
Yes, in some cases	34%	43%
No	44%	25%
Unsure	5%	7%
Total	100%	100%

D7. What best describes your organization's primary industry classification?	US	EMEA
Agriculture & food services	2%	3%
Communications	3%	5%
Consumer products	5%	4%
Defense & aerospace	0%	1%
Education & research	3%	2%
Energy & utilities	2%	4%
Entertainment & media	5%	2%
Financial services	18%	15%
Health & pharmaceuticals	8%	6%
Hospitality	5%	4%
Industrial	8%	11%
IT services	4%	5%
Professional services	5%	2%
Public sector	8%	15%
Retail	11%	9%
Technology & software	8%	7%
Transportation	4%	5%
Other (please specify)	1%	0%
Total	100%	100%

Part 3. Attributions about commercial open source applications: Following are six advantages of commercial open source software according to a recently published article (source CIO Insight). Please rate each statement using the scale provided below.		
Q1a. You will lower costs because open source provides flexibility not offered by proprietary software.	US	EMEA
Strongly agree	26%	20%
Agree	36%	30%
Unsure	28%	30%
Disagree	8%	15%
Strongly disagree	2%	5%
Total	100%	100%

Q1b. You will boost quality because commercial open source is collaborative and constantly being improved upon.	US	EMEA
Strongly agree	31%	30%
Agree	32%	30%
Unsure	24%	24%
Disagree	10%	14%
Strongly disagree	3%	2%
Total	100%	100%

Q1c. You will take control – in the proprietary world, vendors dictate code and budgets. In commercial open source, you modify code to suit your needs within budget.	US	EMEA
Strongly agree	26%	23%
Agree	32%	30%
Unsure	30%	28%
Disagree	9%	16%
Strongly disagree	3%	3%
Total	100%	100%

Q1d. You will ensure continuity – when a proprietary software company goes out of business or stops servicing a software product, you are out of luck. If any commercial open source leader leaves a project or community, others take over.	US	EMEA
Strongly agree	33%	29%
Agree	41%	38%
Unsure	18%	20%
Disagree	6%	11%
Strongly disagree	2%	2%
Total	100%	100%

Q1e. Your department will get smarter – through both open source communities and internal collaboration, your tech team will get a better sense of the overall IT practices, resources and tools out there to best serve your organization.	US	EMEA
Strongly agree	39%	30%
Agree	35%	27%
Unsure	19%	23%
Disagree	5%	16%
Strongly disagree	2%	4%
Total	100%	100%

Q1f. Your users will encounter fewer bugs. There is an abundance of community members constantly scrutinizing the codebase, ensuring bugs are found and fixed quickly and effectively.	US	EMEA
Strongly agree	33%	28%
Agree	33%	27%
Unsure	21%	25%
Disagree	9%	18%
Strongly disagree	4%	3%
Total	100%	100%

Part 4. General questions

Q2. Please rank the following list of file sharing technologies based on the level of information security risk each presents to your organization. Let 1 = highest risk to 6 = lowest risk.	US	EMEA
Unencrypted email	1.44	2.18
Encrypted email	5.21	4.38
File Transfer Protocol (FTP)	2.88	2.50
Cloud file sharing/file sync-and-share tool	1.90	1.72
On-premise, commercial file sharing/file sync-and-share tool	4.59	5.26
On-premise, home grown file sharing tool	3.13	2.16
Average	3.19	3.37

Q3. What best describes the level of involvement of your organization's IT department in the evaluation and/or selection of messaging and collaboration solutions?	US	EMEA
Significantly involved	39%	30%
Somewhat involved	43%	53%
Not involved	18%	17%
Total	100%	100%

Q4. How satisfied is your organization with its current messaging and collaboration solution(s)?	US	EMEA
Very satisfied	16%	11%
Satisfied	28%	24%
Somewhat satisfied	20%	21%
Not satisfied	36%	44%
Total	100%	100%

Q5a. What are your current deployment models?	US	EMEA
On premises	56%	69%
Public cloud, single tenant hosted	27%	22%
Public cloud, multi tenant hosted	45%	40%
Private cloud, single tenant hosted	17%	24%
Hybrid of cloud and on premises	45%	31%
Total	190%	186%

Q5b. How satisfied is your organization with your current deployment model?	US	EMEA
Very satisfied	15%	12%
Satisfied	24%	19%
Somewhat satisfied	24%	26%
Not satisfied	37%	43%
Total	100%	100%

Q6. From the list below, please choose the five (5) most important factors for selecting a messaging and collaboration solution.	US	EMEA
Ability to host or manage solution in the cloud	63%	45%
Ease of installation	28%	26%
Ease of management	37%	42%
Ease of use	65%	44%
Improved privacy	9%	38%
Improved security	50%	45%
Open source	53%	57%
Support for access to encrypted email from mobile devices	21%	17%
Technical certifications	15%	12%
Total cost of ownership	39%	37%
User training program or awareness materials	16%	15%
Vendor reputation	49%	61%
Vendor support	55%	60%
Total	500%	500%

Q7. Is your organization planning on replacing its messaging and collaboration solutions?	US	EMEA
Yes, within 6 months	32%	18%
Yes, within 12 months	13%	23%
Yes, within 24 months	10%	11%
Yes, in more than 24 months	4%	2%
Not planning to replace	41%	46%
Total	100%	100%

Q8. In your opinion, for commercial open source messaging and collaboration solutions, does commercial backing and code transparency improve the security profile of the application?	US	EMEA
Yes	55%	67%
No	34%	24%
Unsure	11%	9%
Total	100%	100%

Q9. In your opinion, for commercial open source messaging and collaboration solutions, does commercial backing and code transparency reduce the privacy risks associated with this application?	US	EMEA
Yes	52%	66%
No	37%	26%
Unsure	11%	8%
Total	100%	100%

Q10. In your opinion, for commercial open source messaging and collaboration solutions, does commercial backing and code transparency increase the integrity and trustworthiness of the application?	US	EMEA
Yes	68%	76%
No	23%	16%
Unsure	9%	8%
Total	100%	100%

How frequently do the following scenarios occur regarding the privacy and security of your organization's messaging and collaboration software?		
Q11a. Employees send and receive files and documents not intended for them.	US	EMEA
Never	8%	18%
Rarely	12%	13%
Often	56%	50%
Frequently	24%	19%
Total	100%	100%

Q11b. Employees do not follow the company's policy regarding the sharing of confidential documents.	US	EMEA
Never	5%	16%
Rarely	6%	5%
Often	34%	33%
Frequently	55%	46%
Total	100%	100%

Q11c. Employees use a messaging and collaboration application not authorized by the company.	US	EMEA
Never	11%	16%
Rarely	15%	13%
Often	38%	31%
Frequently	36%	40%
Total	100%	100%

Q11d. The company's messaging and collaboration application is not available due to security issues.	US	EMEA
Never	13%	23%
Rarely	26%	25%
Often	35%	24%
Frequently	26%	28%
Total	100%	100%

Q12. Are you using any of the following messaging and collaboration software? Please select all that apply.	US	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%
Other (please specify)	9%	9%
None of the above	5%	17%
Total	297%	257%

Q13. Which of the following types of messaging and collaboration software applications are used in your organization? Please select all that apply.	US	EMEA
Free versions of consumer file sync-and-share applications (i.e. Dropbox, Google)	66%	37%
Consumer-grade file storage applications on a public cloud (i.e. Box, Microsoft)	72%	57%
Enterprise-grade file sharing on a private cloud (i.e. Syncplicity by EMC, Egnyte)	34%	41%
In-house file sharing applications (i.e. Accellion, IBM)	49%	65%
None of the above	5%	7%
Total	226%	207%

Part 5. Product features: More than 200,000 companies use Zimbra, with more than 100 million commercial users and 500 million free users globally. Please rate each feature according to its importance in selecting this messaging and collaboration solution for your organization.		
Q14a. Centralized hub for email, social and file sync-and-share applications, including third-party integrations	US	EMEA
Very important	36%	28%
Important	33%	31%
Sometimes important	16%	25%
Not important	8%	11%
Irrelevant	7%	5%
Total	100%	100%

Q14b. Integrated calendar, contacts and tasks; interoperable with other mail and calendar applications	US	EMEA
Very important	36%	37%
Important	32%	33%
Sometimes important	19%	22%
Not important	8%	6%
Irrelevant	5%	2%
Total	100%	100%

Q14c. Ability to encrypt and digitally sign email on both desktop and mobile	US	EMEA
Very important	29%	26%
Important	33%	29%
Sometimes important	23%	26%
Not important	8%	13%
Irrelevant	7%	5%
Total	100%	100%

Q14d. Support for third-party antispam, antivirus and two-factor authentication	US	EMEA
Very important	41%	32%
Important	34%	36%
Sometimes important	16%	21%
Not important	8%	6%
Irrelevant	1%	5%
Total	100%	100%

Q14e Ability to set mobile security policies, including device wipe, PIN enforcement and device management features on user accounts	US	EMEA
Very important	25%	19%
Important	29%	25%
Sometimes important	23%	29%
Not important	15%	19%
Irrelevant	8%	9%
Total	100%	100%

Q14f. Support for encryption of data at rest and in motion	US	EMEA
Very important	26%	20%
Important	29%	25%
Sometimes important	22%	32%
Not important	16%	15%
Irrelevant	7%	8%
Total	100%	100%

Q14g. Full support of iOS, Android, Blackberry and Windows smartphones and tablets	US	EMEA
Very important	48%	36%
Important	30%	30%
Sometimes important	13%	22%
Not important	8%	12%
Irrelevant	1%	0%
Total	100%	100%

Q14h. Flexible deployment options: on premises, public cloud single-tenant hosted, public cloud multi-tenant hosted, private cloud single-tenant hosted, hybrid of cloud and on premises	US	EMEA
Very important	46%	31%
Important	29%	30%
Sometimes important	15%	24%
Not important	8%	12%
Irrelevant	2%	3%
Total	100%	100%

Q14i. The ability to maintain control over data residency so that the organization's data stays within defined jurisdictions and ensures compliance with data privacy laws	US	EMEA
Very important	23%	23%
Important	29%	27%
Sometimes important	26%	28%
Not important	18%	20%
Irrelevant	4%	2%
Total	100%	100%

Q14j. Tight integration of email and file sync-and-share applications that supports private attachments to ensure that only the intended recipient receives access to files (based on their email address)	US	EMEA
Very important	39%	36%
Important	31%	25%
Sometimes important	19%	19%
Not important	10%	15%
Irrelevant	1%	5%
Total	100%	100%

Q14l. Fine-grained access control and permissioning of file attachments/sharing that let you maintain regulatory compliance of sensitive documents and digital assets	US	EMEA
Very important	35%	34%
Important	35%	37%
Sometimes important	15%	13%
Not important	9%	13%
Irrelevant	6%	3%
Total	100%	100%

Q14m. Ability to extend the collaboration software through an open architecture so that the company's industry-specific workflows (e.g. HIPAA) can be created or leveraged	US	EMEA
Very important	23%	25%
Important	20%	29%
Sometimes important	29%	18%
Not important	21%	22%
Irrelevant	7%	6%
Total	100%	100%

Q14n. A cloud-based email system with adequate data privacy features to ensure compliance with applicable data protection regulations	US	EMEA
Very important	24%	28%
Important	21%	29%
Sometimes important	30%	20%
Not important	20%	21%
Irrelevant	5%	2%
Total	100%	100%

Q14o. Features to control and manage content including document versioning, metadata, e-discovery, archiving and syncing	US	EMEA
Very important	21%	20%
Important	29%	25%
Sometimes important	32%	26%
Not important	15%	23%
Irrelevant	3%	6%
Total	100%	100%

Q14p. Capabilities to manage, access or otherwise integrate with back-end services such as network file systems, directories, workflow systems, repositories and business applications	US	EMEA
Very important	23%	19%
Important	23%	25%
Sometimes important	31%	29%
Not important	17%	20%
Irrelevant	6%	7%
Total	100%	100%

EMEA cluster country composition	Freq.	Pct%
Denmark	12	2%
France	69	10%
Germany	98	15%
Greece	7	1%
Ireland	22	3%
Israel	10	1%
Italy	41	6%
Netherlands	35	5%
Poland	29	4%
Russian Federation	48	7%
Saudi Arabia	43	6%
South Africa	23	3%
Spain	48	7%
Sweden	12	2%
Switzerland	13	2%
Turkey	30	4%
United Arab Emirates	27	4%
United Kingdom	108	16%
Total	675	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.