Secure Enterprise Messaging in the Age of the Chat App
Summary

In brief

Ovum’s Secure Enterprise Messaging Survey 2017, conducted in partnership with messaging and mobility platform provider Infinite Convergence Solutions, canvassed 300 companies in four countries: Germany, Singapore, the UK, and the US. The survey was conducted in September 2017, across multiple industry verticals, with most respondents operating in the manufacturing, healthcare, retail/wholesale, professional services, education, and financial services sectors. Company size ranged from 101 employees to more than 10,000 employees, although most respondents were in the 2,500–10,000-employee range. Respondents were surveyed on their use of and attitudes toward consumer mobile messaging applications and secure enterprise messaging applications within their organizations.

Ovum view

Consumer use of chat apps such as WhatsApp, Facebook Messenger, and WeChat has grown. Both WhatsApp and Facebook Messenger now have 1.3 billion monthly active users (MAUs). The use of these apps in the workplace has also grown, causing major concern for enterprises, since employees are using them without the knowledge or approval of IT departments. Moreover, chat apps have deployed increasing levels of security, including end-to-end encryption, making it near impossible for organizations to monitor their employees’ communications via these apps.

Consequently, enterprises risk not complying with regulations governing communications services, since being able to audit and store communications is a key legal or customer service requirement for organizations in many industry verticals. Some companies – particularly those in the banking and finance sector – have banned the use of chat apps, but they have not offered their employees an alternative secure mobile messaging platform, citing a lack of financial or technical resources.

Companies offering their employees an authorized secure mobile messaging app mostly offer purpose-built apps, often alongside other communications apps and services such as SMS, email, collaboration tools, and chat apps. Company-authorized secure mobile messaging apps include similar capabilities to chat apps – such as messaging, voice and video calling, group communications, and encryption – but add capabilities focused on business needs, such as guest access, remote wipe, archiving, collaboration, and centralized administration.

In this paper, we analyze the results of Ovum’s Secure Enterprise Messaging Survey 2017, assessing use of consumer messaging apps and secure mobile messaging apps in common types of organization.

Key messages

- Enterprises have significant concerns about employees using consumer messaging apps at work. The survey found that 65% of respondents were concerned that chat apps represented a security loophole and that half were troubled by their inability to monitor their employees’ chat app communications. Alarmingly, 41% of respondents did not know which of their employees were using chat apps.

- Among those organizations whose employees were using consumer messaging apps (authorized or not), 70% had put in place controls, including circulating policies governing the
use of chat apps, restricting chat app usage to company-provided devices or phone numbers, and requiring that employees disclose their log-in details.

- Almost two-fifths of respondents (38%) that provided a company-authorized mobile messaging application also allowed the use of a consumer messaging application such as WhatsApp or Facebook.
- Many enterprises appeared to dislike their employees’ use of consumer messaging apps: 67% of those that authorized chat apps said they only did so because it was impossible for them to block them.
- Of the half of survey respondents that offered a company-authorized mobile messaging app, a significant proportion provided more than one app, including channels for SMS and email. This suggests that enterprises believe their employees need different methods of communication depending on use case.
- The overwhelming majority of respondents (76%) provided an internal secure mobile messaging app such as Microsoft's Skype for Business. Skype for Business was the most widely deployed secure messaging app (74%), followed by Cisco's Spark (9%) and then NetSfere (5%).
- Of those enterprises that provided their employees with a secure mobile messaging app, 65% did so because the app included features more relevant for business use compared with the features typically found in a consumer messaging app.
- Respondents rated communications services such as voice calls, video calls, and security in the form of end-to-end encryption (E2EE) as the most desirable features that a secure mobile messaging app could include. These capabilities are in line with what consumer messaging apps already offer. However, collaboration options and cloud storage were also rated as important for enterprise apps, as well as compliance with relevant regulations governing electronic communications.

Employee use of consumer messaging apps troubles enterprises

The three largest consumer messaging apps in the world today are WhatsApp, Facebook Messenger, and WeChat. WhatsApp and Facebook Messenger each have 1.3 billion MAUs, while WeChat is close to breaking the 1 billion barrier with 938 million MAUs as of July 2017. Ovum expects that all three of these players will experience strong growth in 2018 and that WhatsApp and Facebook Messenger will reach 1.5 billion MAUs by the middle of the year.

The pervasive nature of consumer messaging apps is undoubttable, and users are no longer restricting themselves to chat on them; video and voice calling are proving popular chat app activities as well. Facebook Messenger and WeChat both offer channels to engage with brands, purchase services and products, and even consume media such as videos and games. The scope of messaging apps is therefore extending well beyond messaging and even communications.

As more and more time is spent on these apps, they will increasingly be used for both social and business purposes. Use of chat apps for business communications is not surprising given their widespread reach and the deep level of engagement they attract. In China, the popularity of WeChat for business use has been so high that its parent company, Tencent, has launched Enterprise


WeChat. Enterprise WeChat includes all the communication features of WeChat, but adds services that enable users to track annual leave and expenses. There is a clear demand to use consumer messaging apps for business, especially for chat, voice, and video calls. However, employee use of consumer messaging apps presents several challenges for companies, mostly because the inability to monitor these apps poses a security risk.

Most companies have regulations and policies in place for employee communications either internally or externally with customers and suppliers. Enterprises in multiple industry verticals are required to store their employees' communications records for auditing purposes; they need to monitor conversations while ensuring that these communications are secure and confidential. Consumer messaging apps do not necessarily provide these vital features, and therefore enterprises are taking steps to block the use of consumer messaging apps or are seeking ways to regulate or control them.

**Popularity of chat apps forces enterprises' hand**

As mentioned, chat apps have seen impressive growth over the past few years, achieving global penetration among consumers, which has led to their unofficial use within enterprises. Despite worries that consumer messaging apps create security risks and make it difficult to audit employee communications, organizations have still allowed their employees to use them. For instance, 67% of respondents in Ovum's Secure Enterprise Messaging Survey 2017 stated that they allowed employees to use consumer mobile messaging apps because the apps were widely used and it was impossible to effectively block their usage (see Figure 1). Meanwhile, 14% of respondents said that their organization did not have adequate technical or financial resources to deploy a secure enterprise messaging app of its own.

Although a large proportion of respondents stated they were forced to allow these apps to be used due to their widespread popularity, 47% felt that chat apps were a secure and effective mode of communication. This demonstrates demand for a chat app specifically for the enterprise space. Such an app would be most effective if it facilitated compliance with company policies and industry regulation.

From a country perspective, 79% of Singaporean respondents indicated that they allowed employee use of messaging apps due to their widespread use, compared to 50% of US respondents.
Figure 1: Organizations’ reasons for enabling employees to use consumer messaging apps

<table>
<thead>
<tr>
<th>Reason</th>
<th>Proportion of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer mobile messaging applications are so widely used it would be impossible for my organization to effectively block employees’ use of them</td>
<td>60%</td>
</tr>
<tr>
<td>My organization believes that consumer messaging apps are more effective communications tools than alternatives such as email</td>
<td>50%</td>
</tr>
<tr>
<td>My organization believes that consumer messaging apps enable secure communications</td>
<td>40%</td>
</tr>
<tr>
<td>My organization does not require communications to be tracked or monitored</td>
<td>30%</td>
</tr>
<tr>
<td>My organization does not have the technical or financial resources to deploy a secure enterprise mobile messaging application</td>
<td>20%</td>
</tr>
</tbody>
</table>

Source: Ovum's Secure Enterprise Messaging Survey 2017 (n=57)

Messaging, voice, and video calling lead use cases

Chat apps are no longer limited to messaging alone, and most now offer a portfolio of communications services including video calling; VoIP; media, file, and location sharing; and, of course, group voice and video calling. In the consumer domain, messaging, video calling, and voice calling are all growing in popularity, and this seems to be mirrored in the business domain. Ovum’s Secure Enterprise Messaging Survey looked at how organizations’ employees used consumer messaging apps. Unsurprisingly, most respondents (70%) stated that they used chat apps for messaging on a one-to-one basis for daily work tasks; 61% used them for group messaging; and 60% used them for one-to-one voice or video communications. Interestingly, 49% used consumer messaging apps to share non-confidential documents, while 28% used them to share confidential documents.

Taking a deeper look at country-level data, an overwhelming 86% of German respondents used chat apps for video and voice communications, while only 43% used them for messaging. US respondents went in the opposite direction, with 78% using chat apps for messaging and only 33% (the lowest across all four markets surveyed) using them for one-to-one voice or video communications.

Security is important, but chat apps represent a loophole

Due to the widespread popularity of chat apps, there is now a fair bit of concern from companies about their use for business purposes. The survey found that 65% of respondents were concerned about chat apps creating security loopholes, while 50% were concerned about their inability to monitor communications via chat apps (see Figure 2). Lack of visibility of which employees were using consumer messaging apps (41%) and the inability to archive or store communications in case of an audit (45%) were also key concerns. In fact, 30% of respondents stated that the use of chat apps meant that their organization was not compliant with industry regulations.
Singapore stood out as the market where respondents were most concerned about the use of messaging apps: 73% of Singaporean respondents felt that these apps represented a security loophole and 56% expressed their concern that employee communications could not be monitored.

The fact that organizations are concerned about using messaging apps is evident from the survey. A resounding 50% of respondents said their companies were taking steps to identify and control the use of messaging apps, while 17% had even banned messaging apps. German respondents stood out once again, with 22% stating that they had banned the use of messaging apps.

**Figure 2: Organizations’ key concerns about employee use of consumer messaging apps**

<table>
<thead>
<tr>
<th>Concern</th>
<th>Proportion of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer messaging apps may represent a security loophole</td>
<td>73%</td>
</tr>
<tr>
<td>Inability to monitor internal or external communications</td>
<td>56%</td>
</tr>
<tr>
<td>Communications cannot be stored/archived for the purposes of auditing</td>
<td>48%</td>
</tr>
<tr>
<td>My organization has no visibility of which employees are using consumer messaging apps</td>
<td>43%</td>
</tr>
<tr>
<td>Employee use of consumer messaging apps means my organization is not compliant with relevant industry regulations</td>
<td>42%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
</tr>
</tbody>
</table>

Source: Ovum's Secure Enterprise Messaging Survey 2017 (n=300)

**Companies strive to block or control use of chat apps**

With their numerous security risks and lack of monitoring opportunities, chat apps clearly present a challenge for enterprises that need to take steps to ensure accountability and compliance. Ovum’s survey revealed that 43% of organizations had developed and circulated a policy detailing appropriate use of consumer mobile messaging apps for internal and external communications (e.g. barring employees from exchanging or sharing confidential company information). Meanwhile, 36% only allowed consumer chat apps to be used on company-provided devices or phone numbers. Surprisingly, 34% of companies required employees to provide their log-in details for the messaging app.

Although most respondents seemed to have actionable plans and policies in place for the use of chat apps, 30% stated that they did not have any controls to monitor and manage their employees’ use of consumer messaging apps.

At a country level, Singaporean respondents seemed to be taking the most actionable steps toward controlling the use of chat apps, with 48% of respondents stating that they required employees to submit log-in details for their messaging app, and 59% having developed and circulated a policy detailing appropriate use of consumer mobile messaging apps for internal and external communications.
Secure enterprise messaging apps: A viable alternative to chat apps

As outlined above, a substantial proportion of organizations' employees are already using consumer messaging apps for internal or external communications. Although enterprises had significant concerns about their employees' use of consumer messaging apps, a worryingly high number of respondents indicated that they did not know which of their employees were using these apps or said they did not have any controls in place to manage the use of chat apps.

Yet, 96% of respondents across the four countries felt that secure, auditable communications were either extremely important or important to their company, as their organization’s communications records were closely monitored and audited because compliance with relevant industry regulation was strictly enforced and non-compliance would cause at least some loss of reputation.

Such findings highlight a market need for a secure enterprise messaging app that would provide similar functionality to that of a consumer messaging app, but with additional features to enable secure and auditable communications for employees. When respondents were asked if their organizations would like to offer employees a secure enterprise messaging application, almost half (46%) said yes, with another 41% indicating that it was something their company had yet to determine. German respondents were most reluctant to do this, with just 24% saying yes, and the overwhelming majority, 62%, saying they had yet to decide. By contrast, more than half of respondents in the UK and the US said that they would like to offer such an app to their workforce.
Email and SMS still rank as important "official" messaging apps

Exactly half of enterprises surveyed said they already offered their employees a company-authorized mobile messaging application. But when respondents were asked what type of company-authorized mobile messaging app they allowed their employees to use, 76% stated that their company offered an internal secure messaging app such as Microsoft's Skype for Business, Slack, or Symphony (see Figure 4).

Although it is encouraging that such a high proportion of respondents used an internal secure messaging app, much of this penetration was likely due to the tight integration of Skype for Business into Microsoft's office productivity tools suite. The issue here, of course, is that an organization may enable Skype for Business (which can be accessed via mobile devices), but it does not mean that its employees are necessarily using it, or that they are using it to the exclusion of other types of mobile messaging app.

The survey results also make it clear that companies enable multiple secure mobile messaging capabilities for their employees and that they still view email and SMS as important communications tools for their employees. For instance, 71% of respondents stated that their companies enabled email as a secure messaging application and 43% indicated that their organizations allowed SMS. Email and SMS continue to rank ahead of collaboration tools and consumer messaging apps as organizations' preferred channels for secure messaging.

The survey indicated that collaboration tools and consumer messaging apps were increasing in importance and were not far off the penetration level of SMS. Given that collaboration tools and consumer messaging apps are on a growth trajectory and offer employees richer communication capabilities than SMS, these channels might soon overtake SMS as complementary internal and external messaging channels – or even start to supplant SMS in some organizations.

**Figure 4: Types of company-authorized mobile messaging apps**

<table>
<thead>
<tr>
<th>What type of company-authorized mobile messaging application does your company enable its employees to use?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal, company-authorized secure messaging app (e.g. Skype for Business, Slack, Symphony, Net2Fone)</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td>SMS</td>
</tr>
<tr>
<td>Collaboration tool (e.g. Salesforce Chatter, Workplace by Facebook)</td>
</tr>
<tr>
<td>Consumer messaging application (e.g. WhatsApp, Facebook Messenger)</td>
</tr>
<tr>
<td>Other (please specify)</td>
</tr>
</tbody>
</table>

Source: Ovum's Secure Enterprise Messaging Survey 2017 (n=150)
Business benefits of secure messaging apps include reduced risk of non-compliance

Of the organizations that had already enabled a secure enterprise messaging app, 65% said that they had done so because the app included features that were more relevant for business use than those provided in a consumer messaging app (see Figure 5). This finding emphasizes that enterprises prefer to deploy messaging apps that allow employees to interact effectively with colleagues and customers, but within the requirements of the enterprise (i.e. the provision of secured communications that can be monitored and stored to maintain accountability).

It is also telling that 47% of respondents indicated that they would like to enable their employees to use a messaging app, but that they did not believe that the use of consumer messaging apps would allow them to comply with relevant industry regulation. Again, this is in line with the earlier finding that almost all respondents view secure and auditable communications as extremely important or important, and are particularly concerned about regulatory compliance.

In Germany, the highest proportion of respondents (60%) said that they offered a secure enterprise messaging application because its built-in tools or integrated third-party software helped employees collaborate or better manage their workflow. This finding suggests that enterprises in Germany have taken a more pragmatic approach toward secure enterprise messaging applications, and are more likely than enterprises in the other three markets surveyed to have deployed an app that is already a business tool or that integrates into the organization’s existing business tools. Meanwhile, in the UK, the second-highest proportion of respondents indicated that they offered their employees a secure enterprise messaging app because having banned consumer messaging apps, they recognized the usefulness of such apps as a tool for internal and external communications.

---

**Figure 5: Organizations’ reasons for offering a secure enterprise messaging application**

<table>
<thead>
<tr>
<th>Reason</th>
<th>Proportion of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>My organization’s secure messaging app includes features that are more relevant for business use than those provided in consumer messaging apps</td>
<td>65%</td>
</tr>
<tr>
<td>My organization wants to provide its employees with a messaging app, but does not believe that consumer messaging apps allow it to comply with relevant industry regulation</td>
<td>47%</td>
</tr>
<tr>
<td>My organization’s secure messaging app enables other types of business tool (e.g. for collaboration, workflow management) either within the app itself or via third-party software</td>
<td>30%</td>
</tr>
<tr>
<td>My organization has banned consumer messaging apps, but recognizes the usefulness of messaging applications as an internal/external communications tool</td>
<td>20%</td>
</tr>
</tbody>
</table>

Source: Ovum’s Secure Enterprise Messaging Survey 2017 (n=114)
Skype for Business dominates; use cases replicate chat apps

Microsoft’s Skype for Business ranked highest in popularity of the seven secure mobile messaging apps listed in the survey: Skype for Business, Spark (Cisco), NetSfere, Slack, Symphony, Team-One (BroadSoft), and HipChat (Atlassian). Some 74% of respondents indicated that their company offered Skype for Business to employees. This was consistent across Germany, Singapore, the UK, and the US, although in Singapore the penetration of Skype for Business was lower, at 44%, with Spark and Slack both at 15% and NetSfere and Symphony at 7% each. NetSfere was the second-most-popular app among respondents in Germany, at 13% penetration, followed by Symphony (7%). Meanwhile, BroadSoft’s Team-One app ranked second in the UK, at 10%, followed by Spark (5%). Spark was the second-most-popular app in the US, at 10%, followed by NetSfere (4%).

The high penetration of Skype for Business reflects the dominance of Microsoft’s suite of office productivity tools, which Skype for Business is tightly integrated into. As mentioned, even though a high proportion of respondents enabled Skype for Business, employees do not necessarily use the app or use it in isolation. The survey results indicate that a high proportion of enterprises have deployed secure enterprise mobile messaging software as part of an integrated communications platform from vendors such as Microsoft, Cisco, and BroadSoft. The fact that Slack, Symphony, and NetSfere have gained market share indicates that enterprises are open to using apps that stand alone – particularly larger enterprises (i.e. those employing more than 500 people) in the manufacturing, retail, telecommunications, finance, and utility industries.

Not surprisingly, enabling one-to-one messaging about daily work tasks ranked as the most popular use case for secure enterprise messaging applications (at 86%). Voice or video calls for both one-to-one communications or for conference calls ranked equal second (76%). These findings suggest that, in line with consumer messaging apps, enterprise messaging apps are increasingly providing a bundle of communications services – not just messaging. The findings also suggest that enabling collaboration is an important use case for secure enterprise messaging apps, with 71% of respondents across the four countries indicating that they enabled their employees to use such apps to create groups for sharing information about projects or clients.

How important different use cases were varied across the four countries, with almost all of the respondents in Singapore (93%) indicating that group communications was the key use case, followed by one-to-one messaging (85%). Meanwhile, in Germany, one-to-one voice or video calling was important to 80% of respondents, while group communications was important to 73%. In the UK, 100% of respondents stated that their organization primarily enabled employees to use secure messaging apps for one-to-one messaging about daily work tasks.

Again, perhaps not surprisingly, fewer respondents said that their organization enabled employees to use secure messaging apps to send non-confidential documents or files (51%), and respondents were understandably reluctant to let employees use secure messaging apps to send confidential information. Enterprises in Germany were far less likely to enable employees to use secure messaging apps to send documents or files containing confidential information, with just 20% of respondents saying that their organization would allow this. However, enterprises in Singapore were more trusting, with 56% of respondents saying that their organization would allow employees to send confidential information via secure messaging apps. Clearly, there is work still to be done, either to ensure that the secure messaging apps available to enterprises meet or exceed their expectations for the transmission of confidential information or – if the suppliers believe that they have already met
stringent security requirements – to convince enterprises that they can confidently use such apps to send sensitive data.

**Enterprises want voice and video calling – and encryption**

Consumer messaging apps have evolved beyond messaging into fully fledged communications platforms that enable voice and video calling, access to content (including personalization), and the sharing of content (such as images and videos), as well as payments and commerce. The same will be expected of secure enterprise mobile messaging apps that have styled themselves on consumer mobile messaging apps. However, enterprise mobile messaging apps will need to offer capabilities that consumer chat apps do not support and omit irrelevant features. As well as complying with relevant regulation, enterprise mobile messaging apps will need to offer features that allow cloud storage, centralized administration and policy control, customization, and remote wipe. They will also need to support communications services other than messaging. Remote wipe especially is regarded as a desirable feature, since it gives the organization control over potentially sensitive communications data held on an employee’s mobile devices when that employee leaves the company.

Ovum asked survey respondents to rank their top three most desirable features on a secure enterprise mobile messaging application, aside from messaging. Voice calls led as the most desirable feature (21% of respondents), followed by E2EE (see Figure 6). E2EE was rated the second-most-desirable feature by 12% of respondents, followed by the option to collaborate and support for video calls, which were given second place by 10% of respondents each. A standard security feature on consumer messaging apps, E2EE was also ranked the third-most-desirable feature on a secure enterprise mobile messaging application by 11% of respondents, followed by cloud storage and compliance with relevant regulation, which were given third place by 10% of respondents each.
Addressing the challenges of cost and complexity

Of the organizations that did not offer their employees a secure enterprise messaging app, 47% stated that it was because they allowed the use of consumer messaging applications, which they believed offered adequate levels of security. However, for 33% of respondents, the lack of financial or technical resources was a key factor in not offering employees a secure enterprise messaging app. This finding suggests that enterprises may be more open to deploying a secure enterprise messaging app if they could do so cost-effectively, using technologies such as cloud-based communications.

Rolling out a cloud-based secure enterprise messaging platform developed and managed by a third party could help an organization cost-effectively deploy a secure enterprise messaging app across multiple platforms and scale it as business grows. It would remove the onus on the organization to manage and operate an off-the-shelf platform which may be expensive, difficult to customize, time-consuming, and potentially disruptive to upgrade. Responsibility for adding features to the app would lie with the service provider, which would likely work closely with its enterprise clients to ensure that relevant features are added and that under-used features are dropped.

Enterprises also need to keep in mind that even though overall they might see cost reductions, there will still be costs associated with moving to a cloud-based secure enterprise messaging platform, such as service rental, upgrades, data storage, and maintenance. Some level of cloud knowledge within the organization’s IT department will also be necessary, so that enterprises are aware of how they can most effectively use cloud to help solve business problems, including employees’ unauthorized use of consumer messaging apps.
Conclusions

Mobile messaging apps are an increasingly pervasive feature in consumers’ daily lives, so much so that they are encroaching on the workplace. Employees should have access to technologies that enable them to be more productive, provide better customer service, and help improve their company’s financial performance or meet other business objectives. However, Ovum’s Secure Enterprise Messaging Survey clearly indicates that while enterprises believe that messaging apps have significant business benefits, the fact that employees’ use of consumer messaging apps cannot be monitored or controlled is a major cause for concern.

For the large majority of enterprises in all industry verticals, securing the communications channel is paramount to ensure confidentiality, data security, and compliance. Within vertical markets such as healthcare and finance, monitoring and auditing employee communications is a legal requirement. But it is difficult, if not impossible, for organizations to monitor conversations and interactions via consumer messaging apps, since one of the key features of these apps is the encryption of messaging and voice calls. As Ovum’s survey reveals, some enterprises have attempted to control their employees’ use of consumer messaging apps, by banning them or by creating policies around their use. Others are offering their employees a range of company-authorized mobile messaging apps – including traditional channels such as email and SMS alongside internal secure mobile messaging apps and collaboration tools – without necessarily banning consumer messaging apps.

Internal, company-authorized secure mobile messaging apps appear to have the highest penetration among enterprises that provide their employees with a company-authorized mobile messaging app – higher even than email and SMS. Microsoft’s Skype for Business leads this market, but the survey suggests some degree of diversity, with standalone apps such as Slack, Symphony, and NetSfere also among the rankings.

Not surprisingly, the key drivers for enterprises to provide employees with a company-authorized secure messaging app center on the inclusion of features that are more business-relevant than those in consumer messaging apps, and the fact that such apps allow them to comply with industry regulation. Other than messaging, voice and video calling, and compliance, security in the form of E2EE (albeit likely with some mechanism that still allows organizations to monitor communications) was highly rated as one of the top three features that enterprises would like to see in a company-authorized secure enterprise messaging application. Other highly ranked features were cloud storage, collaboration, and guest access.

For organizations that did not offer their employees a secure mobile messaging app, the key pain point was a lack of financial or technical resources, suggesting that there is still a growth opportunity for third-party providers of secure mobile messaging apps, which can enable these apps as a cloud-based service. Finally, the survey confirms that organizations trust a secure mobile messaging app more than a consumer messaging app for all the main use cases: messaging, voice and video calling (one-to-one and conferencing), group communications, and the sharing of both confidential and non-confidential files.
Appendix

Authors
Pamela Clark-Dickson, Practice Leader, Digital Communications and Social Networking, Consumer and Entertainment Services
pamela.clark-dickson@ovum.com
Neha Dharia, Senior Analyst, Digital Communications and Social Networking, Consumer and Entertainment Services
neha.dharia@ovum.com

Ovum Consulting
We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer
The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.
CONTACT US
www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES
Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo