Whitepaper

ADEYA

Secure Mobile Collaboration in the Financial Industry

Published: 2nd quarter 2018

www.adeya.ch

Download printable version here: https://adeya.ch/

over
$2.5bn
Mobile messaging value by 2021

over
$73bn
Estimated BYOD market value by 2021

98%
Estimated increase of mobile messaging by 2022.

Part One:

The Mobile Messaging Security Landscape

In 2016, smartphones made history - more people used a smartphone than a desktop to access the Internet[1].

This tipping point is reflected not only in the consumer space but also in business. The Bring Your Own Device (BYOD) movement has been building over several years now, with the market expected to be worth over $73 billion by 2021[2]. This push towards enterprise mobility is also due to an increasingly distributed and mobile workforce. There are now 7.8 billion smartphone subscriptions globally - a smartphone for almost every human on the planet[3]. As we move further into the 21st century, modes of working are becoming more fluid and mobile communications are essential to enabling this movement.

The freedom that they offer is one of the driving forces behind a more innovative way of working. This enables a business to reach outside of geographical boundaries to find the best person for the job. It gives the enterprise and its workforce the tools to communicate within teams and with external clients and partners in a seamless and engaging manner. The mobile enterprise is the enterprise that communicates.

This communication drive is evident in the rise of the mobile messaging app. With remote teams, having a messaging app can be crucial to improving productivity. Mobile messaging has seen a surge in use amongst consumers with an expected 2.48 billion messaging app users by 2021[4]. This is reflected in the business world as people use messaging apps outside of work, then bring them into the office for convenience. A study by Radicati [5] shows that mobile messaging is expected to steadily increase until 2022; with an open rate for a mobile message of 98% compared to 22% for an email a compelling use case.

However, less positive forces, a very compelling use case for messaging, are coming into play. As we change our business models and embrace new technologies, we also open up opportunities for malicious forces.

MOBILE MESSAGING MINDFULNESS

Benefits of Mobile Messaging

Mobile messaging within an enterprise has a number of positive forces that are too compelling to ignore.

This is in line with the modern workforce's expectations of a more open work-place, as well as businesses changing to accommodate new technologies. The benefits of mobile messaging include:

IMPROVED PRODUCTIVITY:
In a report by Aruba Networks[6] 60% of employees said a mobile-first business made them more productive.

EMPLOYEE SATISFACTION:
The digital workplace is seen as an attractive one.

ACCOMMODATING WORKERS IN THE FIELD:
Mobile messaging allows a business to look further afield in recruitment and build effective remote teams.

REDUCED RESPONSE TIME AND SEAMLESS WORKFLOW:
The instant nature of mobile messaging keeps work flowing.

THE MOBILE MESSAGING SECURITY LANDSCAPE

COMMUNICATION IS ABOUT SHARING INFORMATION, AND IN THE WORLD OF CYBERCRIME INFORMATION IS A VALUABLE COMMODITY.

As enterprises increasingly use a mobile-first business model. Exposure to malicious mobile attacks will increase exponentially.

The threats within the mobile landscape are compounded by the use of employees' own devices and apps. The entire threat matrix of mobile is one that is complex and overlapping, linking connections, apps, and the devices themselves.

In a survey of security professionals by CheckPoint [7] it was found that 64% of participants felt unable to prevent a mobile cyberattack.

More than half of the respondents said that loss of data via mobile device was serious an issue as that from desk-tops and laptops.

Mobile attack vectors include both internal (insider) as well as external threats. In this report, the type of security threats that affect mobile devices reflect the same threats that an enterprise sees across the board. Data exposure, ransomware that locks devices, and theft of intellectual property are as prevalent on mobile devices as they are on traditional computers.

Mobile security attacks equate to lost revenue: in the "Cisco 2017 Annual Security Report"[8] they found that 1 in 4 enterprises that had suffered a mobile-based security attack, lost business opportunities, with 30% losing revenue. The same report for 2018 found that mobile security threats were the number one most difficult risk for enterprises to defend against[8].

64% OF PARTICIPANTS FELT UNABLE TO PREVENT A MOBILE CYBERATTACK

Let's look at some of the specifics of mobile threats against business mobile users across three layers:

DEVICE LEVEL

Mobile devices are vulnerable to the same threats as the desktop or laptop. Mobile malware is proliferating as we move to a more mobile-first environment. Mobile trojans and ransomware are of particular concern for the mobile-led enterprise. In Q3 of 2017, Kaspersky Lab detected 1,598,196 instances of mobile malware - 1.2 times up from the previous quarter [9].

Pre-installed malware is also a concern for enterprises. The idea that malware is installed unwittingly by the user is no longer valid: this is evidenced by the recent case of a telecom company who inducted 36 Android devices that were pre-infected with malware - the infection propagated via someone with exposure administrator privileges [10].

MOBILE LEVEL

A Sting in the tail: International Mobile Subscriber Identity (ISMI) is being misused through the use of ISMI-catchers which are malicious (rogue) cellular transmitters that use device surveillance to eavesdrop and/or spam mobile devices.

An ISMI-catcher, also commonly referred to as a 'stingray' is commonly used by law enforcement to detect illegal activities, but the same tech is also being used by cybercriminals to perform mobile-based Man-in-the-Middle Attacks.

APP LEVEL

Mobile app security has long been known to be a general issue. In a report by WhiteHat Security [11] into mobile apps, they found that 90% of Android apps they tested had a vulnerability that allowed private data to be exposed. The same report found that 33% of business apps had security vulnerabilities. IOS has fared somewhat better with 30% of apps having a security vulnerability and around 18.8% using no encryption, thus allowing sensitive data to be communicated with no protection.

An interesting development in the use of encryption that should be on the radar is a recent move by Apple to allow the storage of iCloud encryption keys. The Chinese government has successfully enforced the requirement of storing the encryption keys of Chinese users in China, no longer needing to go through the U.S. courts to gain access to data in that jurisdiction [12]. This could set a precedent for other jurisdictions impacting he security and confidentiality of organizations.

KASPERSKY LAB DETECTED 1,598,196 INSTANCES OF MOBILE MALWARE

90% OF ANDROID APPS TESTED HAD ALLOWED PRIVATE DATA TO BE EXPOSED

Public vs. Private Messaging Apps

The security of mobile devices and mobile apps is often a case of deciding which type of app to choose. There are a number of messaging apps available, but some are more public than others. This design remit impacts the level of security offered by the app and needs to be factored in when making a choice about which to employ in your enterprise.

PUBLIC MESSAGING APPS:

Confidentiality is a key concern for enterprises. Proprietary information and even intellectual property is shared between employees as part of their day-to-day communication. One area that is causing concern for business is the use of consumer messaging apps for work communication. A survey of over 300 companies, carried out by Ovum[13] into the use of messaging apps, found that 65% of respondents were concerned about security issues when employees used 'chat apps' like WhatsApp for work. Worryingly, over 50% of respondents were unable to monitor this use. In a recent case, a former UK investment banker was fine £37,000 for sharing confidential company information using WhatsApp[14].

There have also been issues found with the implementation of encryption in apps like WhatsApp. A group of security researchers from Ruhr University Bochum in Germany [15] have described flaws in encrypted messaging apps such as WhatsApp, Signal, and Three-ma. These flaws allow external parties to insert new people into private messaging groups and compromise the integrity of these applications.

PRIVATE MESSAGING APPS

Private Messaging Apps: An alternative to public messaging apps is the use of private messaging apps. These apps are built specifically to solve the issue of security when communicating via mobile app. Private messaging apps offer a closed system which is specifically built for collaboration and messaging within a secure environment using encryption. Only people with access rights can access the communications. While consumer apps provide some level of protection, there are also enterprise-focused apps which provide military grade protection along with extended collaboration features.

ROUND-UP OF PRIVATE VS. PUBLIC MESSAGING APPS

	Public messaging	Private messaging
DATA PROTECTION	No encryption of data, with some exceptions. For example, whatsApp utilizes encryption, however if an employee leaves a company there is no way to delete messages , contacts, and / or files which could contain sensitive information.	Encrypted messaging and control of messages, contacts and files
LACK OF CONTROL	Lack of control of public apps means that company messages can be mixed with personal messages - this can cause fuzzy boundaries and a constant potential for sensitive information exposure	Ability to define roles and access control to ensure company messages are kept internal to the organization and completely separated from private messages
APP SECURITY	Highly attractive targets for malware attacks	Protected against vulnerabilities and regularly updated to provide continual protection
AUTHENTICATION AND ACCESS CONTROL	Usually no authentication required app access, or simplistic - for example 1234 code-based without underlying controls offered through policies	Ability to control access using passwords that can be managed via policies that comply with standards such as NIST
DATA PRIVACY	No emphasis on Privacy by Design (PbD) principles in app design External users can be added to private groups ad hoc (WhatsApp, for example, has an informal approach to groups, allowing at will addition of users, putting communications at risk of exposure) [16] Public messaging apps may not comply with EU privacy laws such as GDPR	Well designed apps will be built to PbD standards. Full control over groups and messaging is inherent in the design of the app
SECURE COLLABORATION	Usually no extended functionality, and relatively insecure even where features offered	Secure collaboration across a number of channels of communication, often including file sharing and enhanced features
INTEGRATION WITH EXISTING INFRASTRUCTURE	Not designed to integrate easily with existing infrastructure - at risk of be-coming part of Shadow IT	Ability to easily integrate with existing Infrastructure such as an existing Private Branch Exchange (PBX)

Compliance for Third Party Mobile Messaging Apps

Compliance issues and data security have improved, with updates in areas such as the EU's General Data Protection Regulation (GDPR), HIPAA in healthcare, and PSD2 in the financial space.

The mobile enterprise has some specific considerations to ensure that compliance targets are not adversely impacted by the use of mobile messaging. In a report by Lookout, they found that 84% of IT executives expected GDPR compliance to fall short when data was accessed via a mobile device [16]. The same report found that 63% of employees accessed customer, employee or partner data from a mobile device.

Privacy is a hot area in compliance at present usage and in particular is an area of mobile app which has issues. This was evidenced in the case of Consumer Financial Protection Bureau vs. Dwolla [17]. The payment platform Dwolla misrepresented the level of data security they offered for personal data and were found not to have fully tested the security of their mobile apps. Design of messaging apps need to take privacy seriously and build in a number of privacy features across the layers.

Data security too is a risk factor in data access and sharing. In the Lookout report they found poor employee behavior regarding app usage. This included employees downloading apps from unapproved stores, using unsafe links, and failure to install security patches.

All of these issues fall outside of the expectations of compliance requirements affecting all industry sectors.

THREE TIPS TO SECURING MOBILE DEVICES

MOBILE DEVICE MANAGEMENT (MDM)

MDM is a fundamental control strategy for the mobile enterprise. Using an MDM system can help you to identify endpoints across all devices, including smartphones. It can also allow you to put policies in place such as access control and patch management.

APPLICATION BLACKLISTING

A Ponemon Institute study [18] found that 60% of respondents had suffered a data breach as a result of an insecure mobile app. It is vital that mobile app installs are monitored and controlled.

USE SECURE MESSAGING APPS

The Open Web Application Security Project (OWASP) regularly creates a list of the top ten [19] greatest threats against mobile devices. In their 2016 analysis, they placed data security issues as the most pressing including:

- Insecure data storage
- Insecure communication
- Insecure authentication
- Insufficient cryptography

This magic quartet is intrinsic to the robust design of a secure messaging app like Adeya.

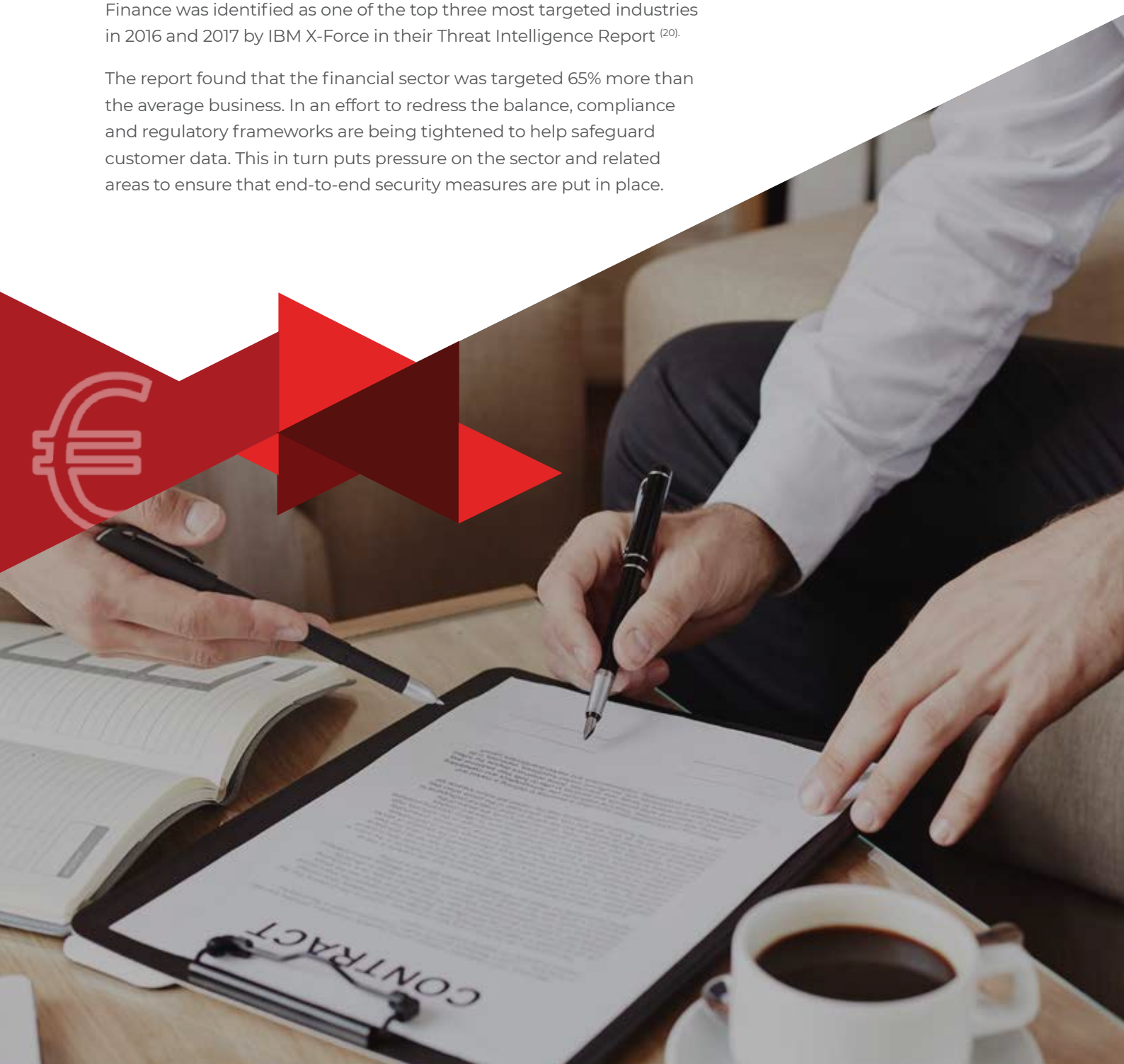
Part Two:

Mobile messaging in the financial sector

The financial sector is one of the most targeted industries when it comes to cyber threats.

Finance was identified as one of the top three most targeted industries in 2016 and 2017 by IBM X-Force in their Threat Intelligence Report [20].

The report found that the financial sector was targeted 65% more than the average business. In an effort to redress the balance, compliance and regulatory frameworks are being tightened to help safeguard customer data. This in turn puts pressure on the sector and related areas to ensure that end-to-end security measures are put in place.



FINANCE IS SEEN AS FAIR GAME BY CYBER CRIMINALS OF ALL PERSUASIONS. THE TYPES OF CRIME ARE WIDE AND VARIED AND INCLUDE:

WHALING:

This is an email fraud based hack which targets the financial departments of large corporations. The scam's aim is to trick corporations into paying large sums of money into the wrong bank accounts. In one such scheme, two large U.S. companies paid out over $100 million to one cybercriminal [21].

It is highly conceivable that messaging apps will be hijacked in much the same way as they start to be used as email adjuncts or replacements.

MONETIZING MESSAGING APPS AND SECURITY ISSUES:

A number of consumer messaging apps are starting to offer payment services. For example, the Japanese owner Line App used in China by 200 million customers, will be offering payment and money transfer services. The Open Banking Initiative, which is being promoted through PSD2, will see many banks expose APIs allowing payments and money transfers from mobile apps.

Unless apps are secured using reliable mechanisms including encryption and robust authentication, they will be exposed to attacks.

DATA PROTECTION:

The financial sector and finance departments have to deal with highly sensitive client and customer data. Information such as personal data, financial records, and client bank details are shared both internally and with external, often global, parties, across complex vendor webs.

Financial services have a mosaic of regulations from EU states, FSA, SEC, FINRA, FCA, and payment schemes. Data protection spans many vulnerable areas of mobile data and as mobile apps and secure messaging become ubiquitous, the data flow across these apps needs to be secured, without compromising collaboration

INSIDER THREATS:

In 2016, $81 million was stolen from Bangladesh Central Bank using stolen bank operator credentials to access the messaging interface connected to the SWIFT network. The attackers then installed malware which helped to hide their ongoing attack. Insider threats are a serious issue in financial sector - 58% of the attacks highlighted in the IBM X-Force Threat Intelligence Report were caused by insider threats.

Mobile messaging apps need to have robust access control policies and authentication measures. Auditing, and rules like geolocation controls are also vital in the war against insider threats.

The financial sector and finance departments are turning to secure messaging apps to help safeguard customer data and build a system of protected communications and secure collaboration.

Compliance in the Financial Sector

Compliance is often about the audit of processes and procedures used to protect data.

GDPR, for example, expects that an organization keeps records about their attempts to implement policies and tools that handle the data rights and encoruage consent expectations of the regulation. In financial services, the Financial Industry Regulatory Authority (FINRA) regulations set out requirements on the use of SMS-based messaging. The regulation specifically states that:

"...EVERY FIRM THAT INTENDS TO COMMUNICATE, OR PERMIT ITS ASSOCIATED PERSONS TO COMMUNICATE, WITH REGARD TO ITS BUSINESS THROUGH A TEXT MESSAGING APP OR CHAT SERVICE MUST FIRST ENSURE THAT IT CAN RETAIN RECORDS OF THOSE COMMUNICATIONS AS REQUIRED ..." (22)

The financial sector, like many others, is embracing the use of messaging apps agile working, collaboration, and always on messaging. As mentioned earlier, the lack of isolation between business and personal communications in public apps can cause a serious privacy and security gap. However, with compliance requirements, and data security issues, these apps must meet the security and privacy needs of the sector.

Private messaging apps are typically designeds to ensure two key criteria are met for financial services use:

CONTROL:

Having little or no control over the sharing of messages outside of the work/team context. Private messaging apps are built to enable secure collaboration and provide robust access control measures to keep conversations isolated.

FINANCIAL SECTOR USE CASE

The following is a real-life use case of the adeya messaging app in use by a globally reputed bank. It demonstrates the ease of use, seamless integration capability, and the secure approach of using the adeya private messaging app in a financial sector setting.

PROBLEM STATEMENT:

The bank has experienced a number of insider attacks. To insulate themselves from these threats they required a system that was easy to deploy and one that ensured that communications were fully controlled and protected.

In addition, the solution had be extended to enable file protection - as conversations typically included the exchange of files.

The system was required to be offered as an on-premise service to enhance sound quality, especially for overseas communications.

The service had to integrate easily with pre-existing infrastructure.

RESOLUTION:

After a comprehensive vendor review, Adeya was chosen as the best solution to solve the bank's secure communication needs by solving these problems:

CONTROL:
Adeya offered full end-to-end encryption of communications. Communication groups could be isolated and with controlled access to them - only authorized individuals could work within the communication groups.

FAST DEPLOYMENT:
Within hours of set-up, group members were able to make encrypted calls, and send encrypted messages and files using their own mobile phones.

SEAMLESS INTEGRATION WITH EXISTING INFRASTRUCTURE:
The bank had an existing IP communications system with which Adeya seamlessly integrated.

FILE CONTROL AND SHARING:
Adeya has an integrated and secure file management system allowing the bank to store and exchange files without requiring additional applications.

COMPLIANCE:

Public apps may not have the kind of attention to detail needed by the financial sector in terms of data security and compliance. Private, built for purpose apps will have Privacy by Design as a design foundation.

About Adeya

Adeya (ἄδεια): "freedom from fear" (Ancient Greek).

OUR MISSION: Securing communication, collaboration and business connections for your digital workplace.

Adeya SA, founded in 2007, is a Swiss cybersecurity company that has been providing secure mobile collaboration solutions for governments and enterprises since the onset of the smartphone era. The company conducts all R&D and product development at its Swiss headquarters and as a result, offers highest quality solutions that carry the prestigious Certified Swiss Made designation.

REFERENCES

1 **Statcounter**, *Mobile and tablet internet usage exceeds desktop for first time world-wide*: http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide

2 **MarketsandMarkets**, *BYOD & Enterprise Mobility Market worth 73.30 Billion USD by 2021*: https://www.marketsandmarkets.com/PressReleases/byod.asp

3 **Ericsson**, *Ericsson Mobility Report 2017*: https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-november-2017.pdf

4 **Statistica**, *Number of mobile phone messaging app users worldwide from 2016 to 2021 (in billions)*: https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/

5 **The Radicati Group**, *Instant Messaging Statistics Report, 2018-2022:* https://www.radicati.com/wp/wp-content/uploads/2017/12/Instant-Messaging-Statistics-Report-2018-2022-Brochure.pdf

6 **Aruba Networks**, *Mobility, performance and engagement:* http://www.arubanetworks.com/pdf-viewer/?q=/assets/EIUStudy.pdf

7 **Checkpoint**, *The Growing Threat of Mobile Security Breaches:* https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf

8 **Cisco**, *Cisco 2017 Annual Security Report:* https://www.cisco.com/c/en/us/products/security/security-reports.html

9 **SecureList**, *IT threat evolution Q3 2017. Statistics:* https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/

10 **Checkpoint**, *Preinstalled Malware Targeting Mobile Users:* https://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/

11 **WhiteHat Security**, *2017 Application Security Statistics Report:* https://info.whitehatsec.com/rs/675-YBI-674/images/WHS%202017%20Application%20Security%20Report%20FINAL.pdf

12 **Reuters**, *Apple moves to store iCloud keys in China, raising human rights fears:* https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060

13 **Ovum**, *Secure Enterprise Messaging in the Age of the Chat App:* https://ovum.informa.com/resources/product-content/secure-age-chat-app

14 **Financial Times**, *FCA fines ex-Jefferies banker over 'boasting' WhatsApp messages:* https://www.ft.com/content/7d0c204d-98d5-34b4-b2b4-d4c130434b9c

15 **Roseler, P., et.al.**, *More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema, Ruhr-University:* https://eprint.iacr.org/2017/713.pdf

16 **Financial Times**, *The perils of using WhatsApp at work:* https://www.ft.com/content/4fbf6c18-a501-11e7-b797-b61809486fe2

17 **Lookout**, *Finding GDPR noncompliance in a mobile-first world:* https://www.lookout.com/info/wp-gdpr-lp

18 **Consumer Financial Protection Bureau**, *Dwolla Inc.:* https://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf

19 **Ponemon Institute**, *2017 State of Mobile & Internet of Things (IoT) Application Security Study:* https://securityintelligence.com/10-key-findings-from-the-ponemon-institutes-mobile-iot-application-security-testing-study/

20 **OWASP**, *Mobile Top 10 2016-Top 10:* https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

21 **IBM X-Force**, *2017 Threat Intelligence Report:* https://www.ibm.com/security/data-breach/threat-intelligence

22 **Department of Justice**, *Southern District of New york:* https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme

23 **FINRA**, *Regulatory Notice 17-18, Social Media and Digital Communications:* https://www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-17-18.pdf

ADEYA

WHY CHOOSE ADEYA?

SECURE

Best-in-class encryption, closed circle access, and extensive management control capabilities.

CUSTOMIZABLE

Extensive customization options allowing adaptation to highly specific client requirements, including integration with custom cryptosets.

SWISS

Adherence to the highest privacy and data protection standards. Globally renowned product quality.

CONTACT US

Rue Saint-Louis 2,
Morges, Switzerland, CH-1110

+ 41 22 566 14 80

www.adeya.ch

contact@adeya.ch

KEEP IN TOUCH WITH US

Facebook

Explanations in video

LinkedIn