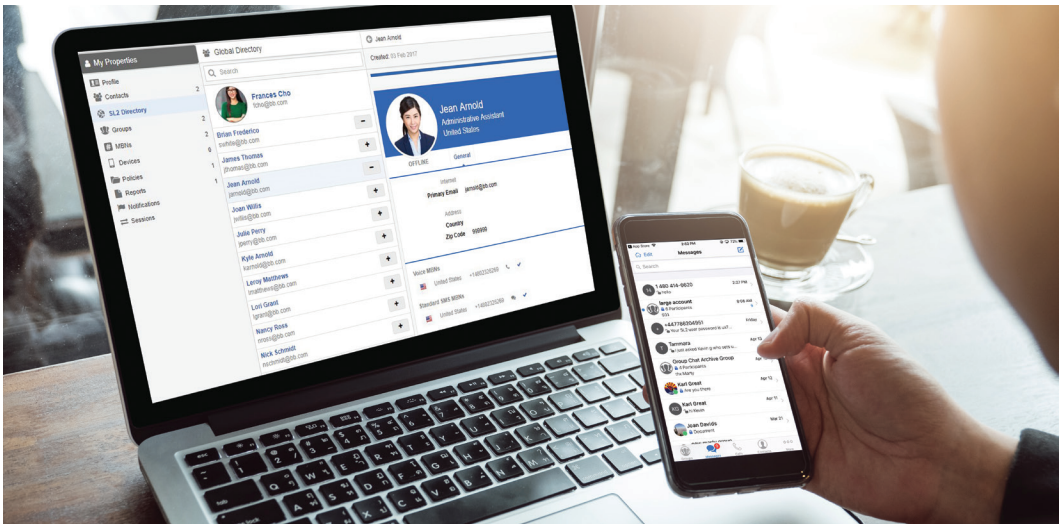
CELLTRUST®
SECURE & COMPLIANT MOBILE

Security, compliance and productivity with enterprise-grade mobile communication

Executive Summary:

A look at what makes a mobile communication solution enterprise-grade, and how investing now will protect your organization from cyber breach and compliance violations, while increasing productivity



Mobile messaging is the direct communication channel of choice

Customers around the world have spoken - and SMS text messaging has become the preferred communication channel for businesses and their customers. The “instant communication” which takes place between two people over a SMS text message exchange is very difficult to surpass in terms of speed, flexibility and productivity. In contrast to email communication, texting is also non-intrusive and direct, with almost immediate confirmation that the text was delivered and opened.

Highly productive people are often always on the go

There are situations which require a face-to-face sit-down type of meeting and others which, although virtual, require video connectivity so a visual presentation can be made. By far – the majority of customer exchanges are made through a quick phone call or text message backed up by an email. Busy personnel and their customers expect to be able to communicate effectively with each other while on the go. Business communications should support the organization’s key objectives and engage the customer/stakeholder, while remaining complaint with industry regulations - anytime and anywhere!

BYOD prohibition has failed miserably

Until recently, customer-facing personnel within highly regulated industries such as Financial Services and Government have been prohibited from using a mobile device to engage with their stakeholders. This was due to lack of an organization-wide mobile strategy or policy and the lack of mobile communication compliance technology.

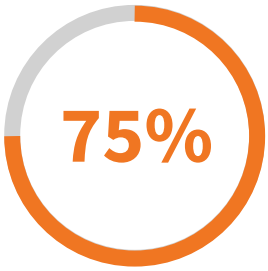
BYOD prohibition policies have failed as the use of BYOD and consumer-grade messaging apps continues to increase and is putting enterprises at risk. Often, personnel have had customers and other stakeholders tracking them down on their personal mobile devices, without the appropriate mobile communication compliance or security infrastructure to support them. Financial Advisors have expressed frustration with BYOD prohibition saying - “It’s quite awkward, inconvenient and time consuming to have to tell your client that you can’t communicate with them about their investment on your personal mobile phone (that they just called or texted you on), and then ask them if you can call them back when you return to the office or send them an email!”.

98% | 20%

SMS open rates are as high as 98%, compared to just 20% of all emails. Source: Campaign Monitor

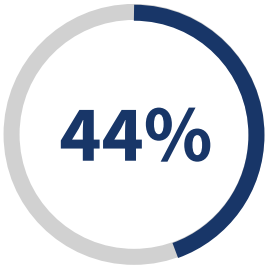
90 seconds instead of 90 minutes

It takes 90 seconds for someone to respond to a text and 90 minutes to respond to an email. Source: Campaign Monitor



Smarsh, Inc. 2019 Electronic Communications Compliance Survey Report.

Three-quarters (75%) of those surveyed allow employees to use personal mobile devices at work. At the same time…



Of respondents lacked confidence that their organizations were capturing and archiving all business communications via allowed mobile devices.

"It's quite awkward, inconvenient and time consuming to have to tell your client that you can't communicate with them about their investment on your personal mobile phone (that they just called or texted you on) and then ask them if you can call them back when you return to the office or send them an email!"

Source: Financial Advisor based in California, USA

Enterprise is at risk of non-compliance, potential fines and penalties

Without an enterprise-grade mobile communication solution which enables organization-wide administration of message and voice capture and archiving – the enterprise is continuously put at risk of non-compliance with the associated audit and potential fines, sanctions or penalties.

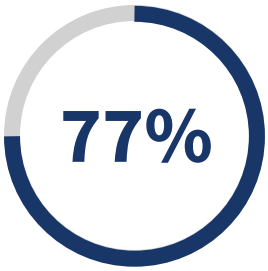
Sensitive data could be lost or compromised

The use of consumer-grade messaging platforms in the workplace, not only challenge the enterprise Compliance team due to lack of supervision and e-discovery, they also cause the enterprise IT and Security leaders serious concern. The majority of consumer-grade messaging platforms or text messaging on personal mobile phones offer little or no protection of customer data. Private conversations and sensitive customer information could be lost or compromised without enterprise-grade technical and physical mobile security protocols and safeguards in place.

"CFOs should recognize a new type of financial risk management related to cybersecurity risk as many finance activities are now conducted remotely. CFOs often perceive cybersecurity to be the responsibility of IT, but as more finance processes run remotely, CFOs need to develop security measures specifically for the finance function and not rely solely on the organization's blanket security protocols to safeguard financial data. "

Source: Smarter With Gartner, The CFO Cybersecurity Risk Checklist, October 2020, https://www.gartner.com/smarterwithgartner/the-cfo-cybersecurity-risk-checklist/

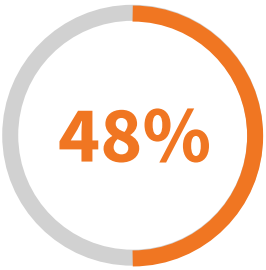
Smarsh, Inc. 2019 Electronic Communications Compliance Survey Report.



Of respondents perceive SMS/ Text messaging as the top communications compliance risk for their firms.

$8.19 million

Average total cost of a data breach in the U.S. in 2019. Source: Ponemon 2019 Cost of a Data Breach Report



Nearly half (48%) of employees sacrifice mobile security for the sake of speed and efficiency. Source: Verizon Mobile Security Index 2019

Verizon surveyed over 670 professionals, along with many leading mobile security organizations, to discover insights into the latest mobile data security threats and trends.

What makes a mobile communication solution Enterprise-grade?

Enterprise-grade mobile communication should protect the enterprise from cyber-attack or data loss, provide central administrative control, engage the customer, support productivity and meet regulatory compliance requirements. Below are some of the attributes an enterprise-grade mobile communication solution will have:

- Security (Zero Trust, Active Directory, SCCA Cloud, Cryptography best practice)
- Cloud based - Mobility as a Service (MaaS)
- Scalable and customizable
- OS agnostic (iOS or Android) on mobiles with a desktop version available
- Central administrative control (device and app deployment, compliance supervision)
- Archival integration
- AppConfig
- EMM and UEM
- Dedicated mobile business number(s)
- International mobile coverage

"Record work conversations drive change. By 2025, 75% of conversations at work will be recorded and analyzed, enabling the discovery of added organizational value or risk."

Source: Gartner Top 10 Strategic Predictions for 2021 and Beyond, October 2020, https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-predictions-for-2021-and-beyond/

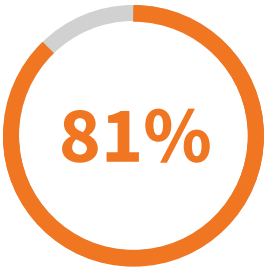
Security

Enterprise mobile users may access the network from anywhere, therefore Administrators are challenged to weigh productivity needs against security requirements.

Enterprise-grade secure mobile communication and messaging platforms, unlike consumer-grade apps, are engineered and constantly monitored with data loss prevention and cyber defense in mind. While consumer-grade solutions may provide some security features such as encryption, a form of multi-level authentication and remote wipe, they often lack the robust security rules, policies and processes an enterprise-grade solution has been engineered with.

It is also essential for mobile communication and messaging applications to be stored in a Secure Cloud Computing Architecture (SCCA) certified cloud environment where encryption key management lifecycle services with optional dedicated hardware security modules and transparent data encryption for encryption at rest are the standard. Best practices for all cryptography operations, including strong encryption for all data in motion and transmission across the Internet must also be applied.

Additionally, Zero Trust architecture, designed to protect by leveraging network segmentation, preventing lateral movement, providing layered threat prevention and simplifying granular



Of organizations said employees are now the greatest risk to mobile security. Source: Verizon Mobile Security Index 2019

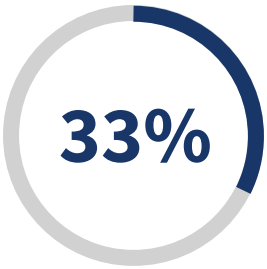
Five of six respondents said that their organization was at risk from mobile threats. 29% said that it was a significant risk. Source: Verizon Mobile Security Index 2019

$17.2 million

In 2016 FINRA Books and Records fines totaled $17.2 million across 13 firms. Source: FINRA.org

67%

Two thirds of organizations said they are less confident about the security of their mobile assets than other devices. Source: Verizon Mobile Security Index 2019



The percentage of organizations that admitted to having suffered a compromise involving a mobile device increased, and the impact of these attacks has been significant. A third said they'd experienced a compromise, up from 27% in the 2018 report. Source: Verzion Mobile Security Index 2019

user-access control, is best practice. The foundational building block for the Zero Trust network model is Active Directory (AD), which vastly enhances the network security and safeguards access to enterprise data through identity management and conditional access control for both devices and users.

Cloud based enterprise-grade mobile communication

Cloud based enterprise-grade mobile communication and messaging platforms help companies cost-effectively deploy and manage a scalable, secure enterprise-wide solution across multiple device platforms.

As already mentioned, sensitive customer or constituent information should be stored in a Secure Cloud Computing Architecture (SCCA) certified cloud environment where encryption key management lifecycle services with optional dedicated hardware security modules and transparent data encryption for encryption at rest are the standard.

Scalable and customizable

Enterprise-level solutions have been designed for performance and scalability so they can autoscale for dynamic and on-demand expansion of cloud services and resources.

For enhanced privacy and security, discerning enterprises can have a dedicated instance which offers isolation at the platform level, including advanced security features and flexible configuration.

iOS or Android and desktops

An enterprise-grade mobile communication platform provides clients for both iOS and Android mobile devices as well as desktop computers.

Organizations of all sizes were hit by mobile compromises:

100–249 employees - 33%
250–499 employees - 25%
500–999 employees - 39%
1,000–2,499 employees - 33%
2,500–4,999 employees - 30%
5,000–9,999 employees - 39%
10,000+ employees 31%

Average = 33%

Source: Verizon Mobile Security Index 2019

443 data breaches = 168,962,628 records

Since 2014 there have been 443 data government/military breaches involving 168,962,628 records. Source: Comparitech

"The future of work is here. CIOs must pay attention to three key trends: Hyperautomation, digital dexterity and the on-demand workforce. Around the world, corporate offices sit empty. In 2019, Gartner predicted that by 2023, fewer than one-third of digital workers would select the corporate office as their preferred place to work. Now, surveys show that 48% of employees will work remotely some or all the time post-COVID-19."

Source: Smarter With Gartner Digital Workplace Trends you can't Ignore, October 2020, https://www.gartner.com/smarterwithgartner/digital-workplace-trends-you-cant-ignore/

Central administrative control

For IT Administrators to deploy and manage mobile devices and applications across the organization they require a responsive platform. At a minimum, IT and supervisory staff must have near real time oversight of user activity, organizational units, devices, policies, Mobile Business Numbers, archiving, system logs and usage. Compliance teams should be able to filter and produce customized reports at the organization, group and user level on key data within their mobile communication network and control and configure the compliance features as required.

Archival integration

To help mitigate risk and respond to regulatory audits, enterprise-grade compliant mobile communication platforms can be integrated with archiving technology providers.

Leading edge archiving technologies can manage, validate, trace and archive voice, chat, text and multimedia messages in support of e-discovery and regulatory compliance. Enterprise-grade solutions provide comprehensive reporting, and administrative/operator activities are logged for server audit trails, and intrusion attempts are logged for intrusion detection reports.

In 2019 FCA fined two large firms £34.3 million and £27.6 million re MIFID I

In 2019 the Financial Conduct Authority FCA in the UK fined two large global financial firms for MIFID I £34.3 million and £27.6 million for transaction reporting failures. Source: FCA.org,uk

MIFID II regulations are even more stringent and require voice recording capture, archiving and retention.

Saved $1.35 million and gained $300 million annually

Cisco transitioned to a BYOD mobility strategy and saved $1.35 million annually on smartphone lease and management costs, gained $300 million annually in employee time and reduced support cases by 33 percent. Source: Cisco Public

"Our customers, some with users across 100+ countries, definitely require an enterprise-grade solution for SMS and Voice communication on BYOD/COPE deployments. We believe enterprise-grade mobile communication capture is the most risk-adverse and cost-effective way to leverage productivity and customer engagement while ensuring security and compliance."

Source: Sean Moshir, CellTrust Chairman and CEO

AppConfig

AppConfig is a community focused on providing tools and best practices around native capabilities in mobile operating systems to enable a more consistent, open and simple way to configure and secure mobile apps in order to increase mobile adoption in business. Users benefit with instant mobile productivity and a seamless out-of-the box experience, and businesses benefit with secure work-ready apps with minimal setup required while leveraging existing investments in Enterprise Mobility Management.

Enterprise-grade secure mobile communication and messaging applications engineered on the AppConfig platform recognize the importance of a standard approach to app management and leverage a common framework for enterprise app configuration and security based on native operating system standards and the AppConfig common schema. https://www.appconfig.org/members/

EMM and UEM

Over the last ten years MDM (Mobile Device Management and MAM (Mobile Application Management) evolved to EMM (Enterprise Mobility Management) which is now evolving to UEM (Unified Endpoint Management) to include phones, tablets, PCs and IoT (Internet of Things) devices.

Forward thinking enterprise-grade secure mobile communication and messaging platforms will have made the required investment and evolution from EMM to UEM integrations with one or more leading global providers such as Microsoft and BlackBerry®.

Dedicated mobile business number(s)

On personally-owned (BYOD) devices or corporate-owned personally enabled (COPE) devices, a dedicated mobile business number is required to separate personal and business mobile communication activity on the same device.

Many organizations have also marketed landline numbers to their customer/stakeholder base and want to be able to continue using them. Enterprise-grade compliant mobile communication can text enable and integrate those office landline numbers into the capture and archiving platform for compliance. The voice functionality of the landline and current service provider should remain the same and calls and messages can be forwarded to one or multiple mobile devices as required.

$9.67 billion

The market for unified endpoint management (UEM) is expected to grow from USD 1.43 billion in 2017 to USD 9.67 billion by 2023, at a compound annual growth rate (CAGR) of 37.48%.

Source: MarketWatch

In an employee satisfaction survey by VMWare: 61% of respondents admitted to being happier in their jobs if they could use their own devices and tools at work.

Government staff often need to remain anonymous for their own protection. An enterprise-level solution will be able to deploy a dedicated mobile number on a personally-owned (BYOD) or corporate-owned personally enabled (COPE) device to be used exclusively for such sensitive mobile communication scenarios.

International mobile coverage

Enterprise-grade mobile communication platforms support both domestic and international phone numbers on the same device with messaging and voice capability across many countries around the world.

Mobile-first rather than Mobile-as-an-add-on drives productivity

Mobile as the primary "instant communication" channel enhances near real time collaboration both inside and outside an organization. Mobile communication is traditionally approached as an add-on and this causes fragmented collaboration which limits productivity. Investing in a mobile-first strategy, not only drives productivity internally, it drives customer/stakeholder engagement by speeding up communication, reducing customer response times and building trust.

Enterprise-grade BYOD and soon BYOE. What is the ROI?

As enterprise and humanity transition to 5G connectivity and begin to embrace and rely upon the range of devices this wave brings with it, personal wearables and other work enhancement devices may soon join personal mobile phones in the workplace.

With UEM and SCCA cloud architecture, and enterprise-grade applications, many of the associated security costs for BYOD mobile-first strategies should become more predictable and manageable. Without the associated hardware costs, additional mobile phone data and voice telecommunication costs, and reduced IT training and help-desk costs, enterprise should spend less as compared to an exclusive COBO (Corporate-Owned/Business Only) deployment strategy.

While numerous industry studies have tried to, either demonstrate significant BYOD ROI or the lack thereof, each enterprise will need to make the calculation based on their unique UEM footprint and mobile communication compliance requirements.

COVID-19 has created an urgent need for organizations to accelerate their digitalization efforts.

69%

of boards of directors say that the effects of the pandemic crisis, the economic crisis and the social crisis are accelerating digital business initiatives, according to the Gartner Board of Directors Survey, conducted in May and June 2020. Source: Smarter With Gartner Covid-19 Accelerates Digital Strategy Initiatives, November 2020, https://www.gartner.com/smarterwithgartner/covid-19-accelerates-digital-strategy-initiatives

Organizations need to reimagine both the workforce and work design to be resilient — and to able to sense and respond to change, repeatedly and at scale.

As business strategies continue to evolve, organizations will need to take deliberate action to prioritize resilience and not just focus on efficiency if they want to succeed in their strategic ambitions. Source: Smarter With Gartner Build Organizational Resilience for Today and Tomorrow, October 2020 https://www.gartner.com/smarterwithgartner/build-organizational-resilience-for-today-and-tomorrow/

BYOD becomes BYOE

Industry Recognition:

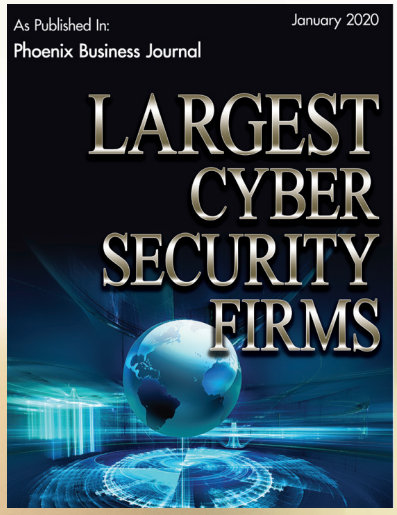
GARTNER
July 2021
Hype Cycle
for
Privacy, 2021

GARTNER
July 2021
Hype Cycle
for
Data Security, 2021

Gold
Microsoft Partner
Cloud Platform
Microsoft

APPCONFIG
COMMUNITY

www.appconfig.org



Reach out so that our experienced team can help you balance security, compliance and productivity with secure, compliant, enterprise-grade mobile communication. Let's get started!

+1-480-515-5200, sales@celltrust.com or **www.celltrust.com/SL2**

HEADQUARTERS
20701 N. Scottsdale Rd.
Suite #107-451
Scottsdale, AZ 85255 USA
+1-480-515-5200

CANADA
1500 West Georgia, 13th Floor
Vancouver V6G 2Z6
+1-778-375-3236