50 Years of Growth, Innovation and Leadership

The Case for Secure Communications Platforms

Overcoming Challenges Posed by 'Shadow IT'

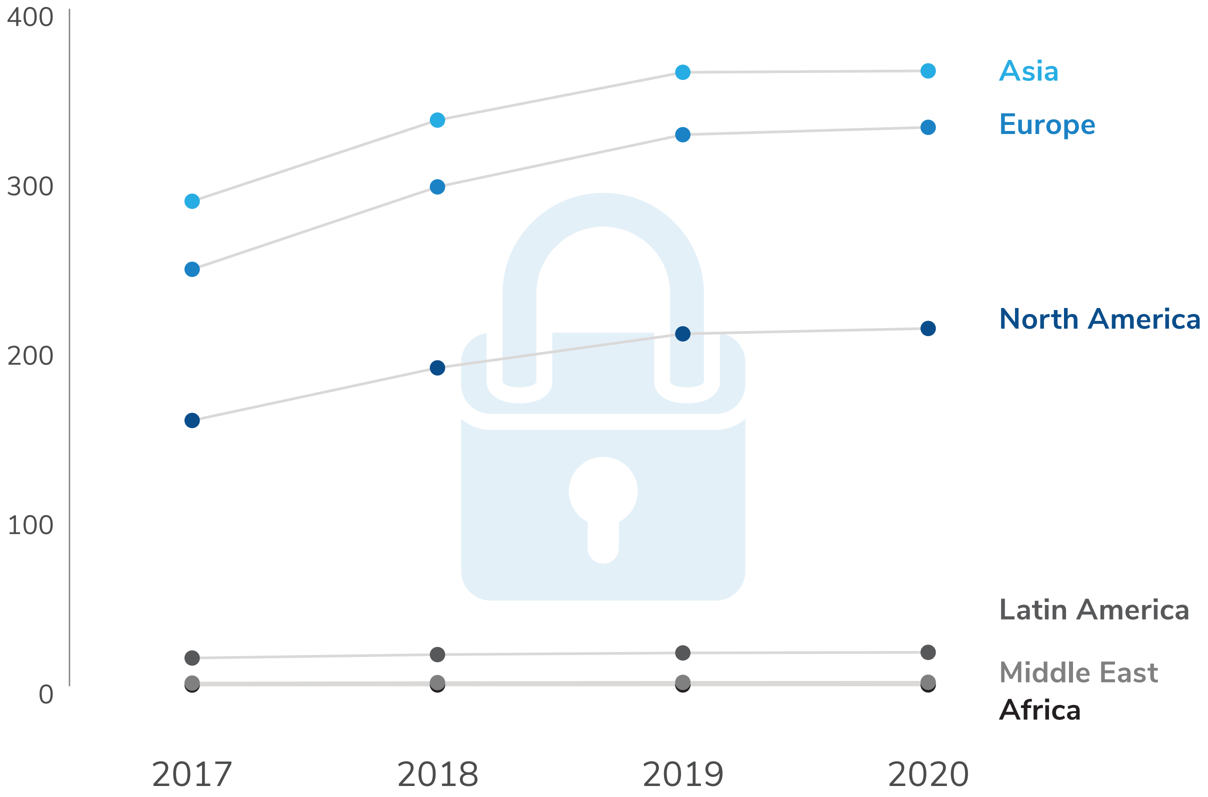
A Frost & Sullivan White Paper
Jason Reed, Senior Industry Analyst, Cybersecurity

FROST & SULLIVAN

THE SECURE COMMUNICATIONS MARKET LANDSCAPE

In the first half of this decade, revelations concerning the vulnerability of communication systems shocked the international community. The most famous of these revelations, brought to light by Edward Snowden, outlined widespread surveillance of communications by government agencies. Stories such as Snowden's caused a ripple effect that has driven governments, enterprises, and consumers alike to rapidly secure communication channels. The result has been the widespread adoption of encryption technologies, and the global secure communications market has seen significant growth. This growth and is expected to continue for the foreseeable future.

THE GLOBAL ENTERPRISE SECURE COMMUNICATIONS LANDSCAPE, 2017–2020



Source: Frost & Sullivan.

The reasons for adoption of encrypted messaging are varied; in some industries it is a matter of regulatory compliance, whereas for others secure instant messaging is more convenient than traditional emailing. Regardless of the motivation, the need for secure communications will no doubt increase as digitization envelops more and more business processes. What is also clear is that encryption is as critical for C-Suite executives managing confidential business transactions as it is for assistants who might occasionally handle communications.

While many companies are working to enhance their overall mobile security, not enough are taking a holistic approach to securing voice, instant messaging, file sharing, and collaboration—each a communication vectors that has been compromised in the past. Whether in voice, text, video calls, file sharing, or other modes of communications, enterprises must take care to secure all of their communications or risk a catastrophic breach that threatens their business, whether by fines, or loss of sector specific licenses.

KEEPING MODERN ENTERPRISE COMMUNICATIONS SECURE

A recent study found that a majority (72%) of enterprises either permit or plan to permit some kind of bring-your-own-device (BYOD) model for their business operations.[1] In such an environment, where users exert a significant degree of control over the applications they install and use, if an employer does not provide a comprehensive suite of communication tools that serve their employee's needs, users will simply install public applications for collaboration and communication. This gives rise to the so-called 'shadow IT' phenomenon, where employees are leveraging unauthorized external applications for business purposes.

There are a number of issues that accompany shadow IT. Firstly, public communication tools have a business model that is divergent from the aims of enterprises that strive keep their communications confidential—most often, these applications are monetizing data to generate advertising revenues. This fact renders these applications fundamentally misaligned with the aims of a high-caliber dedicated secure communications solution.

Public communication applications also carry other risks, namely around the issue of data sovereignty. Organizations have little to no administrative control over public applications, and, even by deploying MDM solutions, they cannot truly monitor their data security or control how that data is used. Furthermore, data from public facing applications may be housed outside of an organization's geographic region, meaning that the data privacy laws for the organization may be radically different from those where a public communication tool's servers are located.

> Organizations whose employees are deploying shadow IT face increased risks of penalties or fines if these applications violate data privacy regulations for their industries.

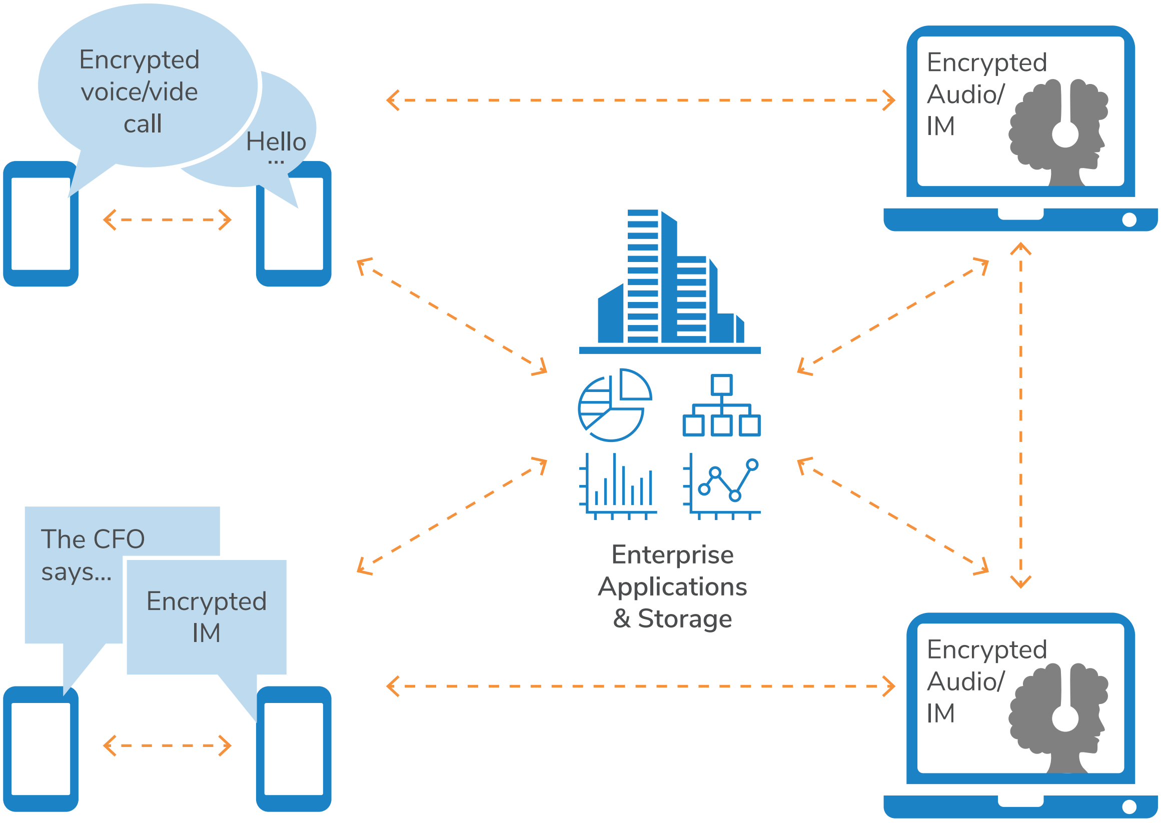
Finally, public communication tools may not adhere to industry regulations, particularly in heavily regulated industries such as financial services or healthcare. In addition to the elevated risks of a data breach (many public applications have suffered a breach in the past), organizations whose employees are deploying shadow IT face increased risks of penalties or fines if these applications violate data privacy regulations for their industries.

[1] http://www.techproresearch.com/article/byod-iot-and-wearables-thriving-in-the-enterprise/

OVERCOMING SHADOW IT

The emergence of shadow IT and its associated risks makes a strong case for adopting a secure communications platform that uses top-tier encryption to protect text messaging, instant messaging, voice calls, video calls, conferencing, file sharing, and collaboration tools. Vendors in the secure communication platform space offer 'white label' solutions that provide strong integration into existing company IT that will reduce or eliminate the temptation for employees to deploy shadow IT, while increasing productivity.

SECURE COMMUNICATIONS PLATFORMS



Source: Frost & Sullivan.

Providing employees the secure communication platform they need to communicate with one another, partners, and clients, has numerous benefits that address some of the challenges posed by the emergence of shadow IT. Notably, many solutions offer an on-premise deployment that allows organizations to own and house their data directly on site, thereby circumventing many of the problems surrounding data sovereignty. Furthermore, the customized expertise that a secure communications vendor brings to an organization will ensure that the solution is compliant with all relevant regulatory frameworks.

Finally, secure communications platforms provide uniform and scalable solutions that eliminate the patchwork of public applications that are sometimes used for business purposes in a BYOD environment. Scalability is critical, as too often organizations focus on securing the communications of executives, forgetting that lower-level employees may also encounter business-critical data in their tasks. Communications in an organization should be secure by default.

Moreover, these white label platform solutions integrate better into company workflows, and show employees a clear delineation between professional activities and personal activities, whereas public communication tools blur the boundaries. In light of the many benefits that a secure communication platform provides, there is no better way to ensure the continuing confidentiality of business communications. The need for secure communications impacts every industry and every employee, as the risks associated with a data breach pose a threat for all companies handling sensitive information.

CAN SECURE COMMUNICATIONS BE TRUSTED?

Enterprise grade security and military grade security are both marketing terms; But enterprise grade security adheres to no specific standards, whereas military grade encryption has a defined standard against which it is measured. Although enterprise grade security is often robust, the phrase can mean whatever a given vendor believes it means.

Military grade security means that a vendor follows an established standard that governments deploy to protect classified information. Secure communication providers who have worked with government agencies can, for the most part, be expected to have the most robust encryption and security standards.

It is essential, that an organisation knows the history and the reputation of a company in order to make an educated decision about trusting a partner to provide critical secure communication infrastructure without weakened security or creating back doors.

Geographic location also plays a role: Frost & Sullivan research identifies certain geographies as being more reliable for secure communication than others. The Swiss market, for example, has a strong reputation for data privacy regulations. Key players in this market include Adeya, Kudelski Group, and Wire. Organizations who handle sensitive data would do well to examine the Swiss vendors, as their solutions are second to none in this field.

FROST & SULLIVAN

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Floor 3 - Building 5, Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
TEL +44 (0)20 8996 8500 | FAX +44 (0)20 8994 1389

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?