MOBILE WORKING WITHOUT CONSTRAINTS

HOW TO KEEP UP THE PACE WITH THE GROWING TRENDS OF BYOD AND REMOTE WORKING

Awingu.com

One Workspace. Any Device. Anywhere.

Gartner Cool Vendor 2017

01

INTRO

> *According to analyst firm, "Markets and Markets" the global market for BYOD increased from $67 billion in 2011 to about $181 billion by the year 2017. (*)*

Studies show that mobile working has grown by 50% over the past 20 years (**). This is a trend that is not going to stop anytime soon, for several reasons: traffic and its related pollution have become a global challenge, employee's productivity is constantly pushed to new limits, and adoption of broadband internet access has become the new default for many.

In addition, we are all used to working with multiple devices, a trend we bring into the workplace. Increasingly, employees are equipped with a desktop/laptop, a tablet, and a smartphone - devices which are not always company owned or managed devices.

Today employees want to work on their device of choice. As a result, a wide array of appliances are used in the modern workplace, be that a Microsoft Surface, an Apple MacBook, an Android tablet, a Google Chromebook, or an HP Elite X3s, to name a few. We all have our preferences, which is why companies are increasingly considering ‘Bring-your-own-Device” (BYOD)/ ‘Choose-your-own-Device’ (CYOD) policies.

The concept of BYOD was first introduced in 2009, and by 2011 had emerged as a trend, which studies suggest isn't leaving anytime soon.

* According to the analyst firm "Markets and Markets"
** Survey of Income and Program Participation, a sample with evolution remote workers in the US, 2010

02

HITTING THE WALL OF CONSTRAINTS

Despite the prevalence of mobile working, employees still face obstacles that often prevent them from efficiently going mobile, if they are able to do so at all. We've grouped these constraints into 3 categories:

LEGACY IT

Even with this rise of SaaS and cloud services, businesses still spend roughly 75% of application budgets on legacy platforms. These are typically not mobile and are considered a show-stopper in the evolution towards a mobile workspace by 61% of businesses.

SECURITY AND COMPLIANCE

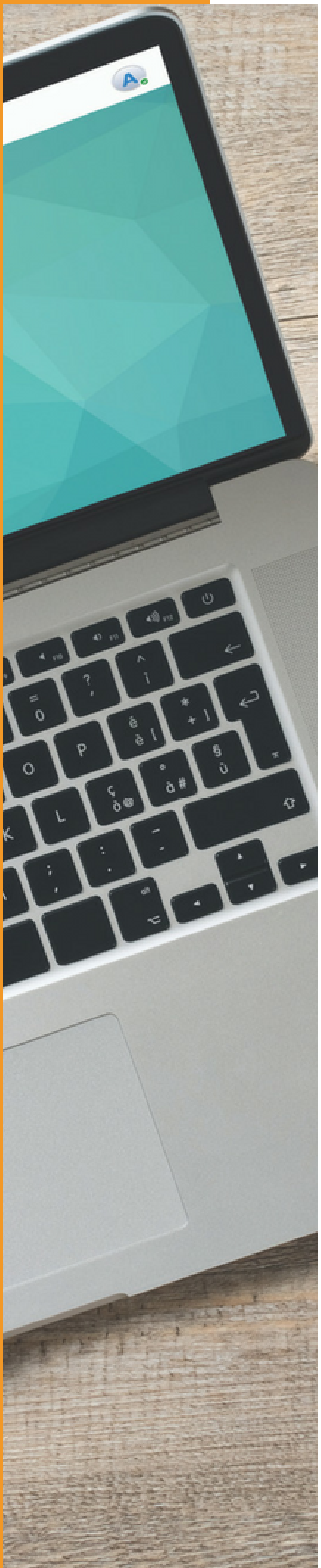
IT organizations are challenged by increases in security attacks, such as WannaCry, on one side, and compliance with new regulations such as the General Data Protection Regulation on the other side. This often forces IT departments to devote the bulk of their budgets to enhancing security and compliancy, resulting in a dearth of resources for mobile working and BYOD.

DEVICES AND OS PLATFORMS

Some IT organizations will require devices to be “managed”. Even "Bring-your-own" devices are entered into the perimeter of managed devices. This limits the actual adoption of any device policy as costs and resources are often just too limited to go as broad as employees desire/require.

A lot of companies struggle to keep all end-user devices on the same Operating System (typically Windows). This is often a heavy and costly process. At the same time, a lot of applications are only available on Windows, or even older version of Windows. This often creates a "catch 22": some applications won’t run on recent platforms, yet, we do want all platforms to be updated to the last version for manageability (and security).

03



WHAT IS THE SOLUTION?

Solutions offering a 'future-proof' perspective on workplace management should tackle "the wall of constraints" to mobile working while still reaping the benefits. They need to provide mobile access to legacy IT platforms and guarantee an optimal security and compliance, all while enabling employees (and contractors) to work from "any device".

It also involves breaking down some "old truths":

- Not all devices need to be managed
- Employees are empowered to choose their device of preference, including personal

04

JOCHEN MAERTENS,

CEO SYNERGICS, BELGIUM

> *Thanks to Awingu we can quickly and cost-effectively deploy the mobile workplace of the future to our customers without extra complexity.*

05

"BRING YOUR OWN DEVICE" WITHOUT APPROPRIATE TOOLING COMES WITH SECURITY RISKS

Today, almost 80 percent of BYOD is facilitated in a completely unmanaged fashion, according to SecureEdge Networks. This use-case is typically limited to email and agenda access (e.g. POP3, IMAP) on tablets and smartphones, but even with its limited scope, it shows that most current BYOD ‘policies’, if they can be termed as such, are not at all secure.

The global BYOD security market is expected to grow at a CAGR of 31.95% between 2013 and 2018 (as reported by MarketResearchReports.biz).

33%

of workers store their work passwords on their smartphone (according to SecureEdge Networks).

77%

of employees have received no instruction regarding the risks of using their own devices at work (from AllThingsD).

SCHEDULE
NOVEMBER 12 — NOVEMBER 18

RONNY HARTZEL

CEO TOOLBOX, SWEDEN

> *Finally, a solution that retains existing infrastructure and runs legacy applications in a browser. It increases security, mobility and the ability for Mac OS/iOS users to run distributed applications without the complexity.*

08

MOBILE DEVICE MANAGEMENT IS NOT THE (ONLY) ANSWER

One of the classic ways to ensure employees will stay productive and not violate corporate policies is “Mobile Device Management” (MDM). MDM is typically used by an IT department to monitor, manage and secure employees’ mobile devices that are deployed across multiple mobile service providers and mobile operating systems being used by the organization. Often MDM is used on company-owned devices. Mobile device management software is often combined with additional security services and tools, such as “Mobile Application Management”, to create a complete mobile device and security solution, labeled as ”Enterprise Mobility Management” (EMM). (*)

Initially, MDM was primarily focused on ensuring basic security measures (typically on-device encryption and adequate power-on passwords), and enabling organizations providing the ability to remotely wipe a managed device (e.g. if the employee left the organization or the appliance was lost or stolen). IT was adopted as a security solution for businesses. (**)

Although it seems like a great solution, MDM and EMM don’t provide coverage as adequate as that of a well-managed BYOD policy, as employees aren't very fond of giving their employers control over their personal devices. Furthermore, application and data access is typically limited to email, agenda, contacts and perhaps a CRM.

Finally, MDM solutions don’t help businesses "mobilize" their legacy IT platforms, as different tools, or, re-coding software, is still required.

* http://www.ingrammicroadvisor.com/data-center/23-byod-statistics-you-should-be-familiar-with
**. http://searchmobilecomputing.techtarget.com/ehandbook/BYOD-policies-should-balance-user-needs-and-mobile-security

WHEN THE US PRESIDENT DEFIES BYOD SECURITY MEASURES

While everybody is talking about the growing adoption of BYOD, President Trump has shown the world through his own example how this policy is very much a part of today's reality.

There has been a lot of fuss about the fact that the President still uses his personal Android device and all the potential security risks attendant with this. Android Central speculates it’s a Samsung Galaxy S3, which came out in 2012 and Google hasn't updated since 2015. “Mobile security experts agree that Trump’s Android phone poses a major security risk”, writes TechTarget. (*)

The revelation has some Beltway watchers worried. “A Galaxy S3 does not meet the security requirements of the average teenager, let alone the purported leader of the free world,” observed Nicholas Weaver, a security expert at the non-profit International Computer Science Institute, based out of Berkeley, California. Hacking that gadget is “the type of project I would assign as homework for my advanced undergraduate classes,” he said. (**)

We obviously don’t know for sure what the facts are regarding the President’s mobile device. What we do know is that using personal devices in a professional context has grown significantly over the past years. According to Markets and Markets the global market for BYOD will increase from by 170% from 2011 to 2017.)

BYOD involves every type of device, from iPad’s to Chromebooks, not just smartphones. A Gartner study from 2014 showed that 40% of employees in large enterprises use personal devices for work. “The lines between work and play are becoming more and more blurred as employees choose to ‘use their own device’ for work purposes whether sanctioned by an employer or not,” said Amanda Sabia, principal research analyst at Gartner. The same study also suggests roughly 40% of all BYOD is done without the knowledge or approval of the company IT department. (***)

Whether President Trump's use-case falls in the last 40% is up for debate, but this current group of shadow users is a growing reality faced by many companies. Businesses need to setup tools and policies to guarantee security and data confidentiality, especially on unmanaged devices.

* http://searchmobilecomputing.techtarget.com/blog/Modern-Mobility/Trumps-Android-takes-BYOD-to-the-White-House
** https://www.lawfareblog.com/president-trumps-insecure-android
*** http://www.securedgenetworks.com/blog/topic/strategy

HANS WILLEM VERWOERD

ICT INFRASTRUCTURE CONSULTANT, LANTECH BV, THE HETHERLANDS

> *“There is no need to install client software, connections are always secure and no complex VPN setup is needed, which means happier users and fewer support calls.”*

12

HTML5 CLIENTS ARE THE ANSWER

Awingu's HTML5 browser-based, unified workspace offers the required flexibility, manageability, and security to cover all these complex needs. By enabling access to your legacy (Windows) applications, SaaS apps, and files via our browser-based workspace, we eliminate the constraints imposed by IT platforms.

Awingu’s browser-based workspace has other benefits:

Any device
These days, almost any device runs an HTML5 browser, be it Apple MacBooks, iPads, Chromebooks, Windows devices, smartphones, or even ThinClients. As such, you can access your workspace – your applications and files – through any of all these devices.

Simplicity
Login via the browser. There is no need to install any agents or plug-ins, nor any of the costs attendant with the maintenance of such installations.

No local data
The workspace runs inside the browser. As such, there is no local data on the device (if you don’t want any). This is obviously a big benefit from a security and compliance point of view.

Better TCO
Given there is no need to manage devices from a deployment or security/compliance perspective, IT organizations can gain significant cost optimizations when adopting a browser-based workspace.

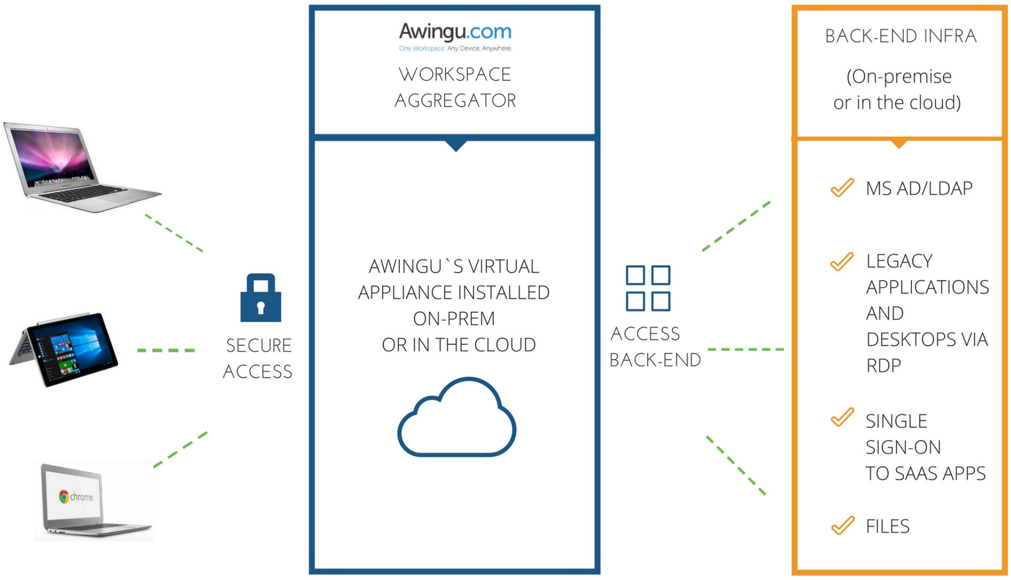
Context awareness
‘Smart’ online workspaces will optimize the user experience based on the user’s context, e.g. pushing a mandatory ‘strong authentication’ when logging in from outside the company network.

HOW DOES AWINGU WORK?

Awingu is deployed as a virtual appliance on any major hypervisor, in a private or public cloud. From there, Awingu will connect into a classic back-end environment.

- It will link with Active Directory or LDAP for user management.
- It will connect to application servers running Microsoft RDS for legacy applications, Windows applications and/or desktops.
- It will set up a Single-Sign-On with SaaS services.
- Finally, it will connect to classic file systems via WebDAV and CIFS and with cloud storage environments such as Microsoft's OneDrive.

For end-users, everything is available in a browser via Awingu's online workspace. No need to install agents, plug-ins etc. Any device with a recent browser can be used securely - this includes private or unmanaged devices.


Awingu.com
One Workspace. Any Device. Anywhere.
WORKSPACE AGGREGATOR
AWINGU`S VIRTUAL APPLIANCE INSTALLED ON-PREM OR IN THE CLOUD
SECURE ACCESS
ACCESS BACK-END
BACK-END INFRA
(On-premise or in the cloud)
✓ MS AD/LDAP
✓ LEGACY APPLICATIONS AND DESKTOPS VIA RDP
✓ SINGLE SIGN-ON TO SAAS APPS
✓ FILES
chrome

To put it simply, Awingu will (1) aggregate applications and files, (2) act as an HTML5 gateway for applications and desktops running on the applications servers and (3) act as an Identity Provider.

In terms of scalability, Awingu is 'stackable'. Our guidance is to host up to 100 concurrent users on one single Virtual Machine and simply add Virtual Machines for additional users. Finally, Awingu's software is multi-tenant, can connect with multiple Active Directories, can be branded, and is open API based. As such, it is also a Service Provider-ready solution.

MARC ALEN

SUB-COMMITEE ICT, BELGIAN FEDERAL POLICE, BELGIUM

> *When I look at the whole picture, going mobile with Awingu is a good solution and a great investment.*

TRIDENT
TRIDENT

ABOUT THE AUTHORS

ARNAUD MARLIÈRE

Arnaud is Chief Marketing Officer for Awingu. Prior to joining Awingu, Awingu worked at Belgacom (the Belgian incumbent Telco) and 'The Boston Consulting Group'.
During his time at Belgacom, Arnaud was heading the cloud product management activities and launched multiple cloud-based solutions: IaaS, Office 365, e-commerce, Dynamics CRM,...He has lived 'first hand' the challenges of bringing to market a SaaS service. At the Boston Consulting Group, he got involved in the firms' IT practice and the complexity of IT in large enterprises. Arnaud is passionate about cloud, mobile, ISV's and the indirect channel.

KURT BONNE

Kurt is Chief Technology Officer at Awingu and has more than 15 years experience in software product development. He bootstrapped and mentored various cross-functional teams and designed and implemented products in various domains, including Cloud Computing, Datacenter Automation, Distributed Databases, Security, Web and Mobile.
He is passionate about the intersection of product, technology and people.

ABOUT AWINGU

Awingu develops software to simplify enterprise mobility and liberate legacy applications. Our software aggregates all company files and applications to one secure online workspace that can be accessed from any device or OS using any HTML5-based browser. Awingu mobilizes all company applications without disrupting how you run your IT and works with any cloud service. No agent is required on personal or corporate devices, and collaboration and file sharing are as simple as sending a URL. IT assets remain centrally secure and no data footprint is ever left behind for a safe way to implement BYOD. Awingu is the fastest and easiest way to empower a mobile workforce. Awingu is headquartered in Ghent, Belgium with affiliate offices in San Francisco and New York. Gartner named Awingu as a ‘Cool Vendor’ when it released its “Cool Vendor in Unified Workspaces 2017” report.

Visit www.awingu.com or follow us on Twitter, Linkedin and Facebook.

Awingu.com

One Workspace. Any Device. Anywhere.

EMEA HEADQUARTERS

Awingu N.V.
Ottergemsesteenweg-Zuid 808 B44
9000 Gent
Belgium

+32 9 296 40 11

info@awingu.com
VAT NUMBER: BE 0832 859 222

US OFFICES

Awingu Inc.,
7th floor, 1177 Ave of the Americas,
NY 10036, New York
info.us@awingu.com

Awingu Inc.
620 Davis Street,
CA 94111, San Francisco
info.us@awingu.com