Ovum
TMT intelligence | informa

On the Radar: Samsung SDS EMM helps organizations secure and empower the mobile workforce

Publication Date: 23 Mar 2017 | Product code: IT0021-000254

Adam Holtby

Summary

Catalyst

Demand for capabilities that can help organizations manage and secure an estate of mobile devices is high. This demand is driving growth in the adoption of enterprise mobility management (EMM) solutions, and as a more diverse estate of devices enters the workplace, this traction shows no signs of slowing down. Samsung SDS EMM is a solution developed to help organizations secure not only a more traditional estate of mobile devices (tablets, smartphones) but also many new device types, including wearables.

Key messages

- Samsung SDS EMM can support organizations in enabling a mobile workforce.
- The technology enables organizations to enforce mobile device security and protect corporate data.
- Wearable devices running the Tizen operating system can also be managed via the solution.
- Broadening the appeal and relevance of the solution to enterprises represents a key objective for Samsung.

Ovum view

Enabling new levels of employee productivity and workplace innovation through mobility represents a significant opportunity for organizations. Increasingly, employees want to be free to use whatever devices and applications they wish in order to get work done. The challenge from an organizational perspective is how to support these behaviors in a way that does not place the business at great risk. As a result, technologies that can help organizations better enable and empower a mobile workforce, as well as manage the risks associated with mobile device utilization, are becoming an increasingly important business proposition.

Samsung SDS EMM is a solution developed to help organizations reconcile the enablement of mobile productivity with the appropriate security management. In addition to its device management capabilities, the technology also enables organizations to manage mobile apps. This is important as application management will be pivotal to enterprise mobility going forward. Ovum research shows that employees use apps for work purposes even when they are self-provisioned and not provided for by their employer. For example, a recent Ovum survey showed that 45% of employees are using an enterprise social networking app that they provisioned themselves (*Ovum Employee Mobility Survey, 2015/16*). This bring-your-own-app (BYOA) trend is gaining traction as employees continually look for ways to work more productively, even if it involves utilizing tools not provisioned by the IT department. Organizations must recognize and respond to such trends in a manner that not only optimizes user experiences but also safeguards corporate data. Tools such as Samsung SDS EMM play an important role in helping organizations achieve this balance.

In embracing standalone mobility management for Tizen-based wearable devices, Samsung SDS is also demonstrating a commitment to supporting organizations as the enterprise device landscape evolves. Ensuring that people can work efficiently and securely across multiple different devices is a key element of the digital workspace that many organizations are moving toward, so technology that supports this model will be increasingly important.

Organizations often struggle to understand where best to start with an enterprise mobility initiative. Beyond just the technological requirements, businesses must understand how mobility will impact current working practices. Samsung offers multiple mission bundles that provide a turnkey approach to enterprise mobility. These bundles have been developed around specific use cases, including tactical defense and law enforcement environments. This as-a-service approach embodies both the Samsung SDS EMM capabilities and implementation support services. As the company looks to increase its enterprise traction, a similar approach focused on specific enterprise use cases would represent a key strength.

Recommendations for enterprises

Why put Samsung SDS EMM on your radar?

Security remains one of the most important considerations for organizations looking to embark on, or further mature, a mobility initiative. The variety of devices being utilized in business environments continues to proliferate. Now, in addition to smartphones and traditional PCs, employees are increasingly looking to utilize a broader estate of devices in a bid to work more productively: tablets, wearables, and augmented reality and virtual reality headsets are just a few examples of devices now entering the workplace. Adopting an approach to managing this evolving device ecosystem is vital, and technology that supports such an approach is imperative to success.

Samsung SDS EMM offers mobile device management (MDM) and mobile application management (MAM) capabilities. The solution has been adopted by organizations in various sectors, including US government agencies. As one would expect, the technology also extensively supports Samsung KNOX, a well-adopted mobile container solution.

Samsung SDS EMM has a strong focus on meeting the high security requirements of modern organizations. Its security capabilities have been independently assessed and the solution has received US Common Criteria certification for both Android and iOS, which means the product has been independently evaluated and fulfilled criteria against important security properties. The solution is also compliant with National Information Assurance Partnership (NIAP) security requirements. NIAP oversees the evaluations of IT products for use in national security systems.

Highlights

Background

Traditionally, Samsung SDS has been more of a systems integrator; however, the organization is now on an effort to transform into a reputable enterprise solution provider. This strategy will see Samsung increasingly compete with the other well-known EMM solutions providers, including VMware AirWatch and MobileIron.

Samsung SDS employs more than 21,000 people across multiple global subsidiaries. Samsung reports that the EMM solution has strong traction across APAC, the US, and EMEA, especially with financial and government agencies (particularly Korean financial and government agencies). Samsung SDS EMM can be deployed as an on-premise solution only.

Samsung SDS EMM is one of multiple solutions Samsung is offering to market to support organizations executing an enterprise mobility strategy. Specifically, the Samsung Square collaboration suite of solutions, including Square EFSS and Square Meeting, can integrate with the EMM offering and support organizations in better connecting the workplace. At Mobile World Congress 2017, Samsung Mobile Security Suite, which includes SDS EMM and biometric authentication (Nexsign), won the GSMA Global Mobile Award (Glomo) for Best Mobile Security.

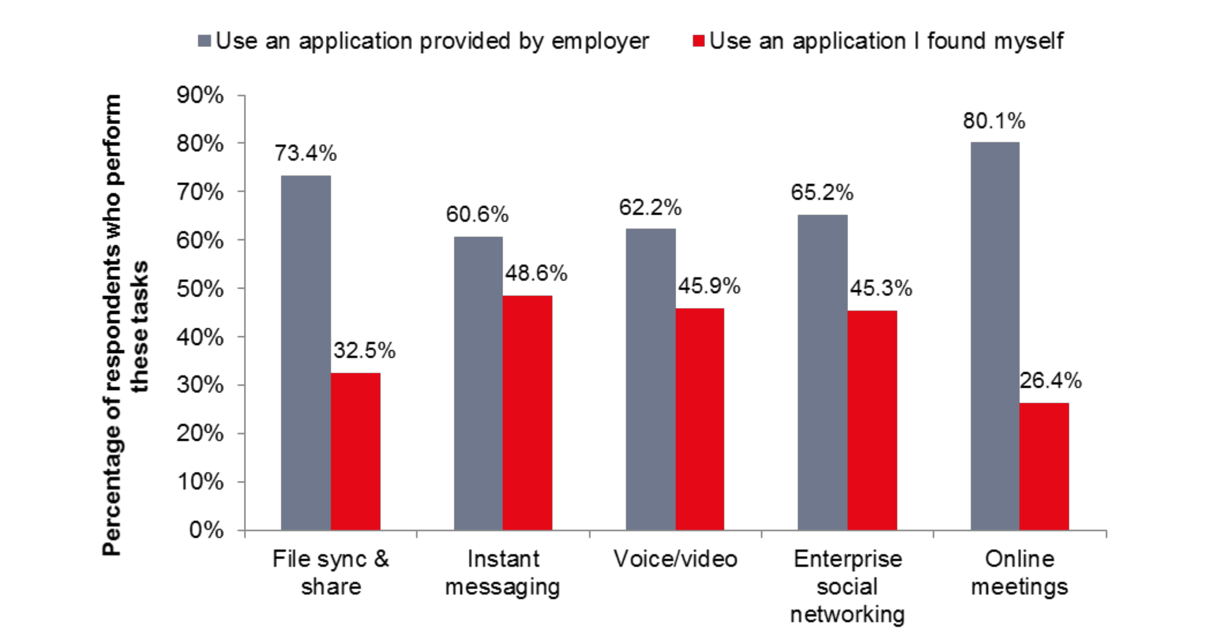
Current position

Samsung SDS EMM offers many of the features expected from an EMM solution while also aiming to differentiate through comprehensive Samsung KNOX support and the management of wearable devices. Samsung SDS EMM supports organizations in executing against both bring-your-own (BYO) and corporate-owned device management strategies. Policy management across both devices and apps is possible, as are various self-service options via a dedicated user portal. Administrators can monitor the compliance of apps and devices against defined security policies via a dedicated admin console. Data communications between devices and servers can take place over TLS-secured data channels, as opposed to over VPN. This can be beneficial in improving the user experience being delivered, because VPN systems can often be quite cumbersome to use. In terms of application management, organizations can distribute apps via a mobile enterprise app store and manage access to applications. Additionally, usage monitoring of apps is possible. Support for the Samsung Knox security platform is also strong, with SDS EMM supporting a total of 129 features out of a possible 142.

Early in 2017, Samsung SDS introduced capabilities that would enable the management of wearables running Tizen OS via the SDS EMM. With this functionality, organizations can use SDS EMM to undertake a variety of wearable device management tasks, including app deployment remote screen lock and factory reset, wearable device tracking, and the remote disabling of selected wearable system settings.

The device management and security capabilities of Samsung SDS EMM are well defined and communicated – this is positive, as organizations looking to embark on a mobility initiative attach great importance to this functionality. Mobile apps represent another area of significance for organizations, so communicating and demonstrating how the technology can help businesses realize value from mobile apps to modernize important business systems and processes is important. Employees are eager to leverage new technologies in a bid to work productively, even if these technologies are not officially provisioned via their IT department. Should organizations and IT departments fail to recognize employee needs relating to the utilization of mobile apps, then shadow IT activities will increase. In regard to mobile apps specifically, Ovum research shows that employees are using a combination of those provisioned by their employer and those they source themselves, as shown in Figure 1.

Figure 1: How people access cloud productivity apps



Source: Ovum Employee Mobility Survey

How to securely enable employee productivity through the provision and management of mobile apps must continue to be a strong focus for EMM vendors such as Samsung SDS.

Data sheet

Key facts

Table 1: Data sheet: Samsung SDS EMM

Product name	Samsung SDS EMM	**Product classification**	Enterprise mobility management
Version number	V1.6	**Release date**	17.3.31
Industries covered	All	**Geographies covered**	Global: APAC (51%), North America (37%), Europe (12%)
Relevant company sizes	Large enterprises, government agencies, financial institutions	**Licensing options**	Perpetual, subscription
URL	www.samsungsds.com	**Routes to market**	Direct sales, partnership with Samsung electronics, value-added reseller
Company headquarters	Seoul, Korea	**Number of employees**	21,900

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Author

Adam Holtby, Analyst, Enterprise Mobility and Productivity

adam.holtby@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.

Ovum
TMT intelligence | informa

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