COOLROCK

Whitepaper

Security and Privacy: Barriers to Mobile Device Management Adoption

October 2021

Security and Privacy: Barriers to Mobile Device Management Adoption

Summary: As the Bring Your Own Device (BYOD) market continues its growth trajectory, Mobile Device Management (MDM) has secured a position as the go-to mobile security software for enterprises. Whilst accepted as a security product, enforcement of security policy by enterprises within the BYOD environment continues to be a challenge. In addition, there are questions being raised as to the impact of MDM which is generally viewed as intrusive software allowing employers the ability to access an employee's personal communications or data on their mobile device, thereby compromising the privacy of the employee. This situation has led to an identifiable need within the BYOD market, which strives to preserve the privacy of the employee whilst ensuring compliance with the enterprise security policy. A need that is still yet to be adequately met by the market.

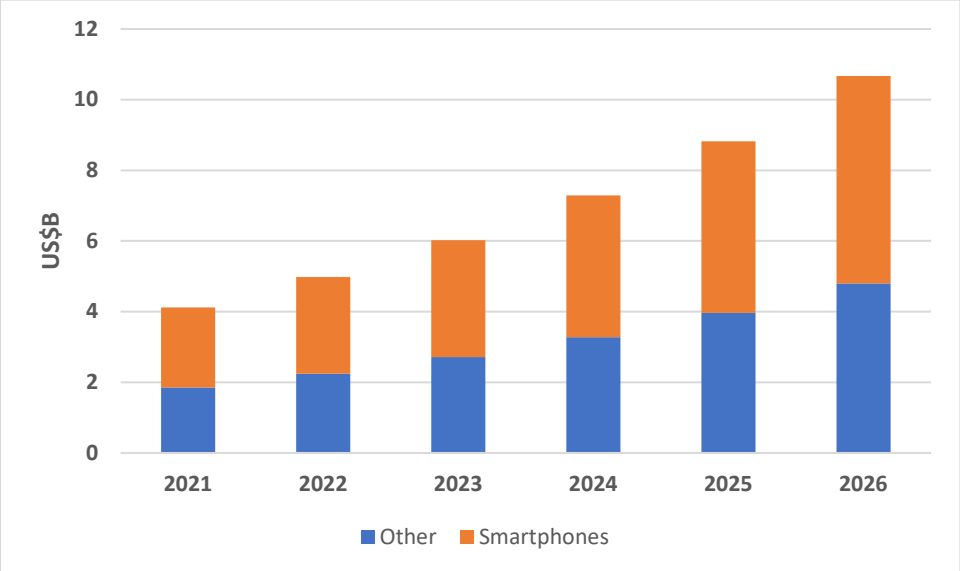
Market Growth

As part of the BYOD market which sees employees using personal devices (smartphones, tablets, laptops) to connect to their organizations networks and access work-related systems and potentially sensitive or confidential data, MDM software is used on devices to secure the corporate data, enabling IT departments to implement policies that secure, monitor, and manage end-user mobile devices.

The growth of BYOD, currently valued at cUS$70b and growing at 16% per annum, has enhanced the risks of data breaches and vulnerabilities to the company network, thereby increasing the focus of deploying advanced systems, such as MDM, to secure their corporate data. Due to the outbreak of COVID-19, firms are increasingly embracing a work-from-home culture. Any employee working remotely significantly increases the risk of a compliance deficiency and poses a risk to firms' most sensitive data. To mitigate these risks, firms are undertaking countermeasures like adopting MDM applications to increase supervision and security features, which will continue to drive MDM systems' market demand.

Currently, the MDM market is valued at cUS$4.1b and is expected to grow over the next five years to cUS$10.6b. Within the MDM market the largest and fastest growing segment is smartphones which currently accounts for cUS$2.3b and is forecast to grow at a Compound Annual Growth Rate (CAGR) of 21% over the next five years resulting in a market size of cUD$4.8b. [i]

MDM Market Growth – Global 2021-2025 (Projected)



Whilst the BYOD and MDM markets are forecast to grow quite strongly over the next few years, the deployment of the security software on devices has created significant issues in relation to the way software deals with the securing of the devices.

Whilst technically effective as a security product to a certain degree, there are questions being raised as to the real-world effectiveness of MDM, which is generally viewed as intrusive software allowing employers the ability to access an employee's personal communications or data on their mobile device, thereby compromising the privacy of the employee, resulting in very low rates of adoption and acceptance by employees. The result: low rates of penetration directly compromising the effectiveness of MDM as a security policy strategy.

Security

The ability to set and enforce security policy by enterprises within the BYOD environment continues to be a challenge. Enterprises are concerned as to the security of sensitive company information when using personal devices for work purposes.

According to Microsoft, regardless of the office's official "bring your own device" policy, two out of three employees use their devices at work. Even if it's forbidden, some people utilize their devices anyway, in one way or another.

A recent study by Trustlook found that 39% of companies have a formal BYOD policy. However, that leaves a majority of enterprises that don't precisely regulate BYOD. Furthermore, over 50% of employees haven't received any instructions for BYOD in the workplace. The lack of policy and its effective implementation imposes a security risk to companies that have embraced BYOD.[ii]

Not being able to control endpoint security as well as concerns with device management, are major reasons why almost a majority of companies do not adopt BYOD.[iii]

MDM solutions are also not perfect at protecting the data they were designed to protect. Once the data is moved to the device, it becomes harder, or impossible, to fully control it. In order to control this data loss vector, MDM solutions have become even more draconian.[iv]

Privacy

When an organisation enables BYOD, employees are able to use their personal devices to access data that can be used for work tasks. Naturally, the enterprise wants to secure these endpoints – with MDM as the security solution of choice. However, access to data is a two-way street with MDM, as IT teams are granted access to employees' devices. As such, there is increasing reluctance among employees to allow MDM agents to be installed on their personal devices.

While MDM solutions can help organisations prevent data breaches, they also raise significant questions regarding employee privacy. Many MDM tools let employers monitor all device activity – including personal calls and web traffic – at any given time.

In addition to this, MDM allows IT teams to perform a variety of remote actions such as locking devices, monitoring employees' locations through GPS and even wiping data from laptops, tablets and phones in the name of corporate security.

Traditional MDM requires the end-user (i.e. the phone/device's true owner) to cede certain rights and privileges over their devices to the company before the company data can traverses the device. Users are reluctantly willing to allow this intrusion into their rights for their own convenience.

Recent stories of data breaches, such as those involving Facebook, have intensified concerns about privacy, causing many to pay closer attention to the personal information their employers can access through MDM tools. Recent research suggests that MDM is facing a growing backlash, with only 44 percent of those questioned stating that they would allow MDM to be installed on their personal devices.[v]

ComputerWeekly reported that many businesses are experiencing pushback in bring your own device plans because employees don't want their personal smartphones and tablets to be controlled, in any form, by the business.

In some cases, people are choosing to carry around two phones rather than have a personal device used for work, the report said. Businesses must respect employee preferences, but in many instances, people want to still use their personal device for some functions in the office, such as sending an email via the corporate wi-fi network. This creates a precarious balancing act and businesses must plan carefully to create the right policies and controls for different device use cases.[vi] Employees have vital personal information on their devices and they typically don't want their current or past employers to have access to it.

A recent study found that 74% of organizations have visibility into emails in devices under BYOD. This potentially infringes on employee privacy, which is why 38% of organizations do not want to adopt BYOD. Other than privacy concerns, organizations do not apply BYOD because of resistance from employees.[vii]

When organisations mandate that MDM be installed on the personal devices of resistant employees, it inevitably leads to 'shadow IT'. Shadow IT refers to the unauthorised tools and applications that employees use in place of sanctioned options that are enabled by MDM. This practice creates a lack of visibility and control over data, demonstrating the need for a security solution other than MDM, one that preserves employees' privacy while protecting businesses' data.[viii]

The privacy issues associated surrounding MDM has caught the attention of regulators, privacy advocates, and others. The European Union's General Data Protection Regulation emphasizes the rights of citizens to privacy, and this focus on privacy has raised questions about MDM. The California Consumer Privacy Act (CCPA) and NYShield Act are raising the same questions in the US.

Conclusion

The growth of BYOD has magnified and highlighted the risks of data breaches and vulnerabilities in a organisations network, thereby increasing the focus of organizations on employing advanced systems, such as MDM, to secure their corporate data. The deployment of the MDM security software on personal devices has created significant issues in relation to the way software deals with the securing devices.

The ability to set and enforce security policy by enterprises within the BYOD environment continues to be a challenge and businesses are experiencing pushback in BYOD plans because employees don't want their personal smartphones and tablets to be controlled or monitored, in any way shape or form, by the business. The preservation of an individual's privacy within the BYOD environment will continue to grow as an issue and attract more attention from regulators.

There is an identifiable need within the BYOD market to preserve the privacy of the employee whilst ensuring compliance with the enterprise security policy.

Notes

[i] Verified Market Research - "BYOD & Enterprise Mobility Market by Security, by Component, by Deployment Model, by Vertical, by Region and Forecast" 2020, Market & Markets – "BYOD and Enterprise Mobility Market" 2019, Modor Intelligence – "Mobile Device Management Market Growth, Trends, COVID-19 Impact and Forecasts (2021 - 2026) 2020 , Grandview Research "BYOD Industry Trends Report 2020" and Company analysis.

[ii] Trustlook Insights – BYOD Trends and Practices

[iii] Greig, J. 2020, July 8. BYOD: A trend rife with security concerns

[iv] https://hypori.com/blog/mdm-drawbacks/

[v] https://www.theneweconomy.com/technology/protection-vs-privacy-the-problem-with-mobile-device-management

[vi] https://www.faronics.com/news/blog/enterprise-mdm-4-mobile-device-management-challenges-teams-face

[vii] Bring Your Own Device. Bitglass' 2020 Personal Device Report. San Francisco, CA

[viii] https://www.theneweconomy.com/technology/protection-vs-privacy-the-problem-with-mobile-device-management