How Financial Services Faces New Data Security Challenges with BYOD and Increased Mobile Device Use

A record number of financial services employees now work from home using personal devices in response to the COVID-19 pandemic. A remote workforce will become the new normal for many organizations despite data security concerns prohibiting them in the past.

This growth in remote users means a larger attack surface for cybercriminals. As a result, cybersecurity teams face a perfect storm of issues. According to Modern Bank Heists 3.0, from February to April 2020, amid the COVID-19 surge, financial sector cyberattacks increased by 238%.

Remotely securing devices can be complicated, and Bring Your Own Device (BYOD) programs present unique security-related challenges. With Europe's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other US privacy laws raising concerns, finding the best bank data security solution can be daunting.

Mobile Device Management

Many organizations use Mobile Device Management (MDM) software solutions to implement BYOD and secure enterprise data and networks. MDM is a popular option to deliver apps to user-owned devices and to secure enterprise apps and data. The MDM market is expected to grow from $4.3 billion in 2020 to $15.7 billion by 2025, so clearly, installations are growing.

For financial services institutions, an MDM BYOD solution can maintain employee productivity— for financial services institutions, particularly with today's new remote workforce, to secure enterprise data and ensure regulatory compliance. MDM segregates corporate data, secures documents, enforces corporate policies, and integrates and manages devices making it a sound choice for banks and other financial institutions.

However, there are some concerns with MDM solutions. First, once enterprise data resides on an employee's device, that data is challenging to secure. It's something to consider, particularly concerning personally identifiable information (PII).

Second, inherent in MDM is full employee device management, making it an employee privacy concern and company liability. If a device is lost or stolen, the company will likely do a remote wipe, leading to the potential loss of end-user personal data. Since MDM gives employers full device control, employees may feel spied on. Unfortunately, these end-user concerns can cause corporate security issues as end-users may circumvent or reject IT policies, creating risk vulnerabilities.

Drawbacks aside, the numbers don't lie. The global MDM market is significant and growing, and many financial institutions will likely consider it for their BYOD solution.

Virtual Mobility Solutions

Another option is a Virtual Mobility Solution (VMS) delivering BYOD to today's financial institutions. A VMS is a "mobile-first" thin client experience that keeps all apps, data, and management on enterprise servers rather than on endpoint devices and maintains complete separation of personal and corporate data. The market is rapidly growing and is expected to grow from $113 million in 2019 to $173 million by 2024.

A VMS for a financial institution BYOD program makes sense and is a quickly adopted solution. The virtual mobility platform allows users to access a remote, secure company-owned virtual mobile device from their physical device. As with MDM, because employees use their own devices, they are more productive. However, with VMS, no company data ever resides on their phones, so privacy is not an issue, and corporate data

security is enhanced. Bad actors have no inroads via app downloads, email providers, text messages, or other typical end-user avenues.

For employers, VMS delivers enterprise network security, central management, cost-effectiveness, and regulatory compliance. IT doesn't have to manage individual devices, and compromised devices are remotely disconnected from the server, reducing costs and simplifying IT management.

A VMS is a BYOD solution whose time has come, and financial institutions are paying attention.

Conclusion

Financial institutions are increasingly concerned about and vulnerable to cyberattacks, particularly since COVID-19. Simultaneously, the industry is evolving to incorporate employee mobile device use and a remote workforce. Secure BYOD is imperative for financial services firms, and it's essential to implement the best solution for the job.

.