FUND OPERATIONS

Mobile productivity touted as important as mobile security

Synchronoss offers tips to fund companies using a “bring your own” device policy

By Danielle Kane – June 1, 2016

As more investment management firms employ “bring your own device” policies, the need for strong mobile security and efficiency looms large.

However, some providers that offer the type of technology and applications needed to ensure a secure personal mobile device do not allow for maximum productivity at the same time.

Large financial firms and their employees are increasingly dependent on remote capabilities, including mobile, and are demanding the same amount of productivity and security one would have at a computer.

“Most mobile usability products today have a very simple utility approach—there’s not a lot of productivity to it,” said Dave Schuette, president of the enterprise business unit at Synchronoss. “Companies are challenged. Mobile users’ productivity is flattening because they don’t have the tools in place that they need.”

Most users access their mobile devices 60% of the time to conduct some level of work, whether it be via email, calendar, documents and spreadsheets or browsing functions. So while Schuette emphasizes the importance of security, he believes the rest of the focus from an operational standpoint should be on user experience and interfacing.

This is why Synchronoss partnered with Goldman Sachs last November to create the Secure Mobility Platform, which offers both security and a unique approach to accessibility and productivity.

The security container is important because it allows users of Synchronoss' platform to separate their mobile work-life from their mobile personal-life, which is becoming an issue inside many companies. Employees who work at financial firms normally are at risk for having their entire device analyzed and wiped clean—if needed—including personal information. However, within a container, all work related functions are separate.

"The big difference is we don't manage the entire device," Schuette said. "Most of our competitor's mange the device and secure the whole thing. We only secure certain applications. So we don't know your personal applications or what's happening outside that container. Our security container is called Lagoon, and what happens in Lagoon stays in Lagoon."

As for productivity, all integrated applications work within a solution called Orbit. This includes email, contact management, tasks, notes, file collaboration and more. Allowing users to have seamless access and an easy interface is crucial.

"We are currently building out a mobile application to support document sharing between the buy side and the sell side," Schuette said. "This would allow users to read, annotate, edit and collaborate internally and externally with certain parties but in a very secure way. And again, it would be done on a mobile device not a laptop."

Integration between certain applications is already available to some extent with the Secure Mobility Platform. But in general, these type of collaborative tools are more common on laptops and don't quite exist yet for mobile devices.

The final component to all of this is identity management. This is the most recent enhancement to Synchronoss' services, and increasingly an overarching theme within the mutual fund industry that more service providers are beginning to address. The company announced in February that it partnered with Verizon to deliver a user-authentication solution. The solution, Universal ID, is meant to provide a faster, easier and more secure way to manage employee identity in a digital world. Synchronoss plans to integrate Universal ID with the Secure Mobility Platform by the second half of 2016.

“It is really important that organizations understand that simple usernames and passwords aren’t good enough anymore,” Schuette said. “Even if your mobile platform is really secure, if you’re not managing the identity and credentials of your employees, that’s going to create a problem.”

Schuette suggests fund companies look at offerings that have multifactor identification capabilities, meaning that beyond a complex password, there should be a second form of factor identification. This could be one-time passwords for each login, PIN numbers, QR codes or Bluetooth authentication.