From the Magazine: Centrify CEO Tom Kemp on Samsung KNOX Making Security Easier in the Enterprise

Ben Munson

When Samsung made its KNOX security software available to all during the announcement of its Galaxy Note 3, the enterprise already understood the benefits. It comes down to Samsung's partnership on KNOX with Centrify, a California-based identity management firm. Centrify CEO Tom Kemp told us recently that the secret sauce in his company's unified identity service is working across data center, cloud and mobile and extending Microsoft Active Directory out to mobile devices as well as PCs. Kemp went into further detail on securing Android and finding a happy medium for personal devices and corporate networks.

Wireless Week: Given the proliferation of Microsoft across the enterprise, why hasn't someone extended the reach of Active Directory before?

Tom Kemp: There are people that will extend Active Directory to maybe some SaaS applications or they may extend it to Unix or Linux, but no one's really taken it whole-hog and extended it across on-premise and cloud. And I think part of the reason is most people were not thinking globally; they were thinking, "Hey, I need to scratch an itch to get a Mac system joined into Active Directory," or "I want to have Active Directory integration with Salesforce." They weren't thinking, because of consumerization of IT, there are just a flood of applications. We're all familiar with BYOD but at the same time there's BYOA with departments deploying SaaS applications, etc.

So most people would focus not on the grand vision, number one, and number two, it's hard. For systems on-premise, you need an agent-based approach to integrate those but with devices and applications that are out in the cloud, you need a cloud service to act as a gateway into your Active Directory. To have an end-to-end solution across data center, cloud and mobile, you have to have both software and cloud services. It's hard to find a company that can do both well and we think that we're that company. This is the problem that we want to solve and we think we need to solve the problem in a comprehensive manner.

WW: How does KNOX work at keeping personal and work information separate for an end-user and on the IT end?

Kemp: One of the dings against Android—obviously Samsung is the leading provider of Android-based smartphones—but one of the dings against Android is that it's not secure, there's a lot of malware, etc. There's always been a push to make Android more secure, that's the first thing. The second item is that most smartphones, unlike tablets that tend to be more corporate purchased and given to employees, most smartphones tend to be purchased by the end-user. I saw one study that said two-thirds of smartphones in the enterprise are personally owned while in the case of tablets, it's two-thirds corporate-purchased. Clearly, on the smartphone, most of it's personal.

There's a problem between end-user and IT in that, the second that phone starts accessing corporate information, IT wants to lock it down. They want to apply policies to it, they want to be able to wipe it if someone leaves the organization, etc. But the problem you have is that it's a personal device where people have their own personally owned music, games, videos, photos, etc. So you have this basic conundrum. This concept of a container is you, with your personal device, allow IT to set up this virtual environment, this sandbox, called a container where inside it I'm going to access work-related things and they can apply policies to that container. But they don't control the rest of the phone because the problem historically has been the mobile device management is kind of all or nothing. You either wipe the device or not, apply policies or not. And what was happening to consumers is that their kid would use the phone and lock out the device by entering three bad pin codes, or the employees could not get Angry Birds because the policy was no games on the phone. But it's their own phone so by having this separation inside the container, it makes it perfect for BYOD where you can lock up the work information and inside the container, work will not leak into the personal and personal will not leak into the work.

One of the concerns is that, on iOS you can set up multiple email accounts and you can simply just move an email from work into your personal. Well, you don't want that so it's pretty cool with this container technology where you can even use the camera app inside the container, flip back to personal and you don't see the photo, and vice versa. IT can apply policy and wipe the container when the person leaves but it has no impact on the rest of the phone.

So what KNOX is, it's two things primarily. First thing, it's a more-secure version of Android and they've licensed some technology from the NSA so it's Android with security enhancements or SE. Linux has this concept of Linux SE. This is now a much more secure operating system overall and it significantly reduces the malware aspect of it. The second component of KNOX, besides the enhancements to the Android operating system, is the container that provides the separation of

work and play.

WW: Besides working with Android, what benefits does KNOX provide over similar offerings like BlackBerry Balance?

Kemp: First of all, KNOX actually has a consumer version. You can actually put into a separate container or vault, your personal information. The second thing, there are lot more enhancements and management capabilities associated with KNOX that you don't get with BlackBerry and a lot of those come through this OEM relationship with Centrify. Samsung realized that with these devices, they're going to compete with BlackBerry and BlackBerry was really known for really good exchange and Active Directory integration. So what Samsung wanted to do was provide better enterprise integration of Active Directory so they called upon Centrify to provide that. What we allow people to do, and this is actually what you get with KNOX, is that you can have both the device and the container join the Active Directory domain and you can manage the device and the containers just like you manage your Windows system by using the native Active Directory tools. This is not something you get with Balance, where you have to use a separate management tool.

The second thing that's a differentiation, provided by Centrify, is that inside the container, it's a business container and you're going to run business applications. Part of the value proposition that we also offer is not only the Active Directory-based management but the Active Directory-based single sign-on. So inside the container, if there are rich mobile applications, the end-user will click on the actual application and silently authenticate. We call it zero sign-on. Similarly if it's a web-based application like Salesforce or Google apps or Marketo, we provide an app launcher where you get the single sign-on experience.

In addition, the other obvious difference is that it's Android, these enhancements and capabilities on top of Android so you get the benefit of the Android ecosystem but in a secure environment. Samsung really saw the value proposition in Centrify in terms of the fact that we can make these Samsung devices and the KNOX container drop seamlessly into an enterprise.

WW: Is the Active Directory incorporation what is going to take the most pressure off IT?

Kemp: Absolutely, I think it will. The cool thing is that whenever you adopt a new technology, the last thing that IT wants to deal with is yet another management tool, yet another pane of glass and having things separated. IT is so used to creating a new user in Active Directory and knowing how to reset their password,

applying policies and knowing how to lock down the environment. Basically what Centrify provides is we make a Samsung device just as manageable and configurable as a Windows PC to IT by using the exact same tools. SAFE (Samsung For Enterprise) provides APIs for both the device and the container, like 800 policies for the device and at least over 100 for the actual container. And we support all those policies so now IT has literally hundreds of group policies it can apply to a phone and container, which is almost parallel to the number of policies it can apply to a PC. Because of Active Directory covers users, devices and computers, than IT can apply policies in bulk and it will allow the help desk that, if someone gets fired in the company, you just need to go into Active Directory and disable that user. And the cool thing is that you can set it up that based on a user being disabled in Active Directory, their container automatically gets wiped of the business-related information. So the second Bob is fired and walks out the door, it's a big easy button for IT to hit and they can be guaranteed that the container is blown away and they don't have to worry about a lawsuit with Bob complaining the company blew away 5,000 photos of his kids.

WW: How easy is KNOX to use from an end-user standpoint?

Kemp: It's kind of toggle switch. It's like dual persona. You push a button, it goes into work mode. You push a button, it goes into personal mode. The nice thing, you're at a restaurant and your kid wants to play a game on your phone, five minutes later you don't have to be in a situation where your kid is going through your email and clicking.