Mobile Collaboration and Bring Your Own Device for Enterprises

Enhancements to the Avaya Networking portfolio will enable enterprises to maintain greater security and control of their networks as they adopt BYOD initiatives. Avaya Identity Engines 8.0, announced today at Interop Las Vegas, makes it simple and cost effective for organisations to provide employees and guests with secure, controlled access to wired and wireless networks from their personal devices.

Enterprises need to know who is accessing their network and how—whether it is with laptops, desktop computers, smartphones or iPad devices. Avaya Identity Engines 8.0 introduces two significant new capabilities that help eliminate the security risks of personal devices on a corporate network and enable enterprises to grant secure, flexible network access to individual users and their devices:

•Ignition Access Portal delivers a unified access experience for both wired and wireless users. It simplifies the administration of BYOD with auto-registration and device fingerprinting capabilities, providing IT staff with detailed visibility into the type and profile of devices on the network and allowing them to act accordingly. Access Portal can be customised and deployed throughout the network and across geographical locations based on the needs of the enterprise.

•Ignition CASE Client automates the configuration of devices for secure network access. It is a dissolvable client that helps ensure that devices meet specific security requirements before being allowed onto the network, and configures them without revealing the necessary certificates or shared keys to users. This is particularly useful when business partners with unmanaged laptops need secure but limited access to network resources, for example—the laptops can be configured automatically in seconds and the CASE client disappears from the user’s equipment.

These new capabilities build on Avaya Identity Engines’ existing security and policy features to deliver a cost-effective way for organisations to manage identity and network access for employees, guests and an ever-growing assortment of devices in the enterprise.

Avaya Identity Engines is part of Avaya Mobile Collaboration for Enterprise, an integrated solution for mobile workforces designed to provide business people with choices for where and how they can work. This solution makes applications and mobile devices work together securely, reliably and cost-effectively and provides new ways to leverage personal devices in the workplace using Avaya’s collaboration applications, unified communications infrastructure, networking technologies, and professional services.

This announcement highlights Avaya’s commitment to bringing The Power of We™

to every Avaya customer to help drive faster collaboration, smarter decisions and better business results.

“Given the funding cuts in education, it’s simply impossible to provide devices to every student. We are putting together a BYOD initiative that will solve this problem by allowing students to use their own personal devices to gain access to educational resources. Network security is extremely important to us and cannot be overlooked. Avaya Identity Engines’ ability to provide detailed visibility into the devices students will use to access the network will enable us to restrict the level of access as required. We will be able to retain security and control of our network at all times, and students will get to use the devices they want while they learn.” - Michael Papoulias, computer and telecommunication networks coordinator, Lester B. Pearson School Board

“Physicians and healthcare staff are increasingly bringing personal devices—from smartphones, to tablets, and notebooks—into work and requiring access to patient records. Hence they need to be provisioned onto the network and integrated into clinical workflows. The challenge is how to ensure secure, seamless connectivity across a diverse mix of devices. Avaya Identity Engines allows us to tailor the level of network access based on both the user and device, minimising the risk of security breaches and ensuring confidentiality of patient data. A physician can be given unrestricted network access when connecting using a hospital-owned PC, and restricted access when connecting using their personal Apple iPad.” - Mark Starry, chief technology officer, Concord Hospital

“IT consumerisation is creating a real headache for companies around the globe. Unfortunately BYOD has incorrectly become synonymous with mobile device management, which is only one part of the solution. Once a device has been on boarded, then what? How does one manage security, management, user experience, network flows? Avaya is the company that is stepping in with a true, holistic BYOD proposal that covers all the pieces.” - Zeus Kerravala, principal analyst, ZK Research

For more information please visit http://www.avaya.com/ [1].

Posted by Janine E. Mooney, Editor

May 08, 2012

Links:
[1] http://www.avaya.com/