Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Wavelink and Zenprise share ten 'must haves' for secure mobile device management

A security framework and evaluators checklist

July 30, 2012 – Wavelink, a value added distributor of enterprise mobility solutions, and Zenprise, the leader in secure mobile device management (MDM) share ten 'must haves' for secure MDM.

With an explosion of smartphones and tablets in the enterprise, employees can potentially gain access to the corporate network, proprietary business applications and sensitive data from anywhere at any time. The risks associated are high as employee habits and behaviours can lead to data loss, exposure of the corporate network and compliance breaches.

Ilan Rubin, managing director, Wavelink, said, "With the growing proliferation of mobile devices and bring-your-own-device (BYOD) in the enterprise, MDM is currently one of the hottest growth areas in the enterprise space. Organisations have to face up to the challenge of how to secure and manage the mobile devices used by workers while effectively protecting the entire mobile enterprise.

"Implementing a cost effective, automated MDM platform not only ensures a more secure environment, but also helps reduce additional management costs."

Ten "must haves" for securing the mobile enterprise

1. **End-to-end security across mobile devices, apps, the network and data**
   MDM solutions must proactively monitor, control and protect all layers of the mobile enterprise, providing both multi-layer coverage and checks and balances.

2. **The option to set dynamic, context-aware policies**
   Many employees use personally-owned devices for and at work. IT departments can't reasonably expect them to eliminate popular apps such as Angry Birds and Facebook and other functionality, but the MDM solution should offer context-aware security to block or lock access to specified resources or apps during work hours or while the employee is on premise.

3. **Grant granular access to mobile apps on a case-by-case basis and segregate critical business apps from non-compliant or potentially malicious apps**
   For many enterprises, giving virtual private network (VPN) access to mobile users means that access is an all-or-nothing proposition. Once the employee has mobile access, many corporate apps are open to that device. The MDM solution must provide additional app-specific layers of security that address corporate apps. This puts granular app access into the hands of the enterprise and protects critical business apps from non-compliant or potentially malicious apps on employees' devices.

4. **Monitor and profile mobile network traffic and user behaviour and ensure integration with Security Information and Event Management (SIEM) solutions**
   IT must have clear visibility of the devices and apps that access the corporate network. The MDM solution must provide real-time visibility into mobile network traffic and user behaviour, audit employee devices and block any that are unauthorised from accessing the network. To enhance real-time, proactive security, the MDM solution should integrate with SIEM solutions.

5. **Support employee devices remotely**
   IT has no way of ensuring that employees install the security patches and updates released by major vendors, which means remote management is a critical requirement. IT needs the ability to service devices, push compliance policies and perform diagnostics remotely.

6. **Architected for security with data residing behind a firewall**
   Many MDM solutions are architected so that the database housing the employee contact details resides in the DMZ, rather than behind the firewall, potentially exposing user and device details. All components of the MDM solution should be fully secured to the highest degree possible.

7. **Scale to support multiple locations and all of my employees**
   Mobility is on the rise, and all enterprises should plan for long-term scalability. The MDM solution provider should be able to support all employees, and multiple devices per employee, with little or no increase in management complexity. It should do so in a way that doesn't require multiple consoles or create a siloed mobile environment.

8. **Highly available at all levels including web, app, data, and, in the case of cloud, at the data centre**
   If the server a company relies on to protect their enterprise goes down, all company data and apps are exposed to risk. To prevent this, the MDM solution should protect against every source of potential failure. The MDM solution should offer high availability with load balancing and redundancy featuring active-active clustering at the web, app and data tiers, as well as global data centre redundancy in the case of cloud deployments.

9. **Flexible deployment options**
   Due to mobile device explosion, enterprises need a variety of deployment options, including on-premise, public cloud or hybrid cloud. The MDM solution chosen should have the flexibility to grow with the enterprise.

10. **Mobile data leakage prevention (DLP)**
    Mobile DLP is a serious issue for virtually every enterprise mobilising its business. Once an employee downloads sensitive data to a device, the organisation loses control and cannot get it back. The MDM solution should let IT set content and context-aware security policies for employee access to sensitive business data on their mobile devices, protect the data from being leaked and claw the data back when employees leave the organisation.

-ENDS-

About Zenprise

Headquartered in Silicon Valley, Zenprise is the leader in secure mobile device management. Only Zenprise protects the mobile enterprise end-to-end with the industry's easiest-to-use MDM solution. Zenprise MobileManager™ and Zencloud™ let IT say "yes" to personal and corporate-owned mobile

devices by safeguarding sensitive corporate data, shielding the network from mobile threats, maintaining compliance with regulatory and corporate policies, and making the administrative process simple and intuitive. This gives IT peace of mind, lets executives take their businesses mobile, and makes employees more productive on-the-go.

Zenprise's extensive list of global customers and partners spans a cross-section of countries and vertical industries including: aerospace and defence, financial services, healthcare, oil and gas, legal, telecommunications, retail, entertainment, and federal, state, and local governments.

For more information about Zenprise, please visit www.zenprise.com or follow us on the Zenprise blog (http://www.zenprise.com/blog), Facebook (http://www.facebook.com/zenprise), and Twitter (@Zenprise_Inc).

About Wavelink
Wavelink (www.wavelink.com.au) specialises in the supply, marketing and support of a range of leading edge enterprise mobility and UC solutions. Wavelink distributes a range of products from Meru Networks, Zenprise, Polycom, Digium, AirTight Networks, Nomadix and Bradford Networks. For more information please contact Wavelink on 1300 147 000.