Barracuda Mobile Device Manager Now Supports Android Operating Systems

Cloud-Based Mobile Device and Application Management Service Allows Customers to Easily Extend Network Security Policies to Mobile Users

Campbell, Calif. (March 17, 2015) – Barracuda Networks, Inc. (NYSE: CUDA),

Press Release Highlights:

- Barracuda Mobile Device Manager (MDM) now supports Android operating systems.
- Barracuda MDM enables organizations to easily manage mobility initiatives and extend security policies by centrally administering and monitoring both iOS and Android devices.
- Barracuda MDM is part of the company's Total Threat Protection initiative, aimed at providing powerful, integrated security protection across multiple threat vectors at an affordable cost, **simplifying information security for resource-constrained organizations.**

Barracuda has updated its MDM solution, a free cloud-based mobile device and application management service. Barracuda MDM is part of the company's Total Threat Protection initiative, and now includes support for Android operating systems. With this announcement Barracuda is offering customers more choices to manage various mobility initiatives across a wide range of industries.

"We first released Barracuda MDM with iOS support targeting our K – 12 customers rolling out 1:1 iPad initiatives," said Stephen Pao, GM Security, Barracuda. "By extending Barracuda MDM support to the Android operating system, we look forward to extending support to help our corporate customers manage their BYOD environments that span both Android and iOS."

Barracuda MDM simplifies management of Android and iOS devices, enabling organizations to safely implement BYOD policies. Barracuda MDM is managed through a centralized console integrated into the Barracuda Cloud Control portal. Highlights include:

- **Security -** Configure mobile devices to include passcode policies, functionality restrictions, email/Exchange Active Sync, authentication credentials, and wifi/vpn/proxy access.
- **Application Management** - Manage app store access, enterprise applications, and integrate mobile devices into the Apple VPP program. Installed applications can be monitored and unauthorized applications can be flagged for follow-up.
- **Remote Management -** Wipe or lock stolen devices, un-enroll devices when employees leave the company, and change security and access policies with an easy to use, intuitive user interface.

“Barracuda MDM enabled our organization to easily manage our mobile education initiatives,” said Ray Stemmer, Technology Director, York School District 1. “With Barracuda MDM we are able to centrally administer, monitor and set policies for the tablets being used by our students. It has greatly improved our productivity across the board – our small IT staff is able to spend less time on MDM and more time working with students and teachers.”

Barracuda MDM integrates with a number of Barracuda solutions and is accessed in Barracuda Cloud Control, which provides a single-pane of glass for customers to manage their security infrastructure. Barracuda mobile applications such as Barracuda Safe Browser, Barracuda Copy and CudaSign by Barracuda can be pushed down to mobile devices, allowing IT administrators to enforce browsing policies, improve workflow, and manage the document signing process.

Barracuda Total Threat Protection

Barracuda Mobile Device Manager is part of the Barracuda Total Threat Protection initiative, which is aimed at providing powerful, integrated security protection across multiple threat vectors at an affordable cost. Barracuda Total Threat Protection is designed to protect multiple threat vectors including email, web applications, remote access, web browsing by network users, mobile Internet access, and the network

perimeter itself. It includes the combination of award-winning security solutions, a common management interface, a single point of support, and affordability. For additional information on Barracuda Total Threat Protection, visit http://cuda.co/ttp

Pricing and Availability

Barracuda Mobile Device Manager is provided at no cost for existing Barracuda customers and can be accessed through the Barracuda Cloud Control portal. Once a service account is provisioned, mobile devices can be easily enrolled with the service from any location. Administrators can send users an email invitation with enrollment information through the service. Optionally users can download the Barracuda Mobile Device Companion app from the iTunes App Store (https://itunes.apple.com/us/app/barracuda-mobile companion/id806338672?mt=8) and Google Play Store (https://play.google.com/store/apps/details?id=com.barracuda.mobilecompanion.The service also supports zero-touch enrollment and inventory management through the Apple DEP program.

About Barracuda Networks, Inc. (NYSE: CUDA)

Barracuda (NYSE: CUDA) provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

This press release contains forward-looking statements, including statements regarding the functionality, performance, and benefits of Barracuda Mobile Device Manager and its compatibility with Android operating systems. You should not place undue reliance on these forward-looking statements because they involve known and unknown risks, uncertainties and other factors that are, in some cases, beyond the Company's control and that could cause the Company's results to differ materially from those expressed or

implied by such forward-looking statements. Factors that could materially affect the Company's business and financial results include, but are not limited to customer response to the Company's products, as well as those factors set forth in the Company's filings with the Securities and Exchange Commission. The Company expressly disclaims any intent or obligation to update the forward-looking information to reflect events that occur or circumstances that exist after the date of this press release.