BLUE COAT

Security
Empowers
Business

FIVE STEPS TO SECURELY EMBRACING MOBILE DEVICES

SOLUTION BRIEF

Enable BYOD Without Sacrificing Network Security

The use of personal devices to access corporate networks enables employees to achieve an unprecedented level of productivity and flexibility, but how do you protect your data and network and their devices? And how do you balance the need for control and accountability while ensuring users have the access they demand? Embracing employeeowned devices in the corporate environment doesn't need to be an all or nothing approach. Instead, your business can take incremental steps to protect the network while still giving your employees the access they want to be productive in an always-on work environment. Get started with this step-by-step guide:

❶ **Secure your corporate network:** First and foremost, ensure that you can protect and consistently enforce policies across all devices on your network – whether they are corporate or employee owned. This means being able to control and set policy around not just the web applications accessed by desktop and laptop users, but also the native and mobile web applications users access on their mobile devices. Creating a policy that blocks uploads to Facebook is pointless if mobile users can use the native Facebook app on their smart phones or tablets to work around the policy.

❷ **Extend malware protection to mobile devices:** Regardless of where your employees are or the devices they are using, malware protection should be a priority. It is never a good idea to leave devices that have access to the corporate network exposed to potential threats. Fortunately, both employees and IT managers agree that threat protection for users on mobile devices is critical, regardless of who owns the device. In a recent Global Mobility Study by IDG Research Services, 50 percent of employees and IT managers agreed that businesses should be able to provide malware protection for employee-owned devices.

❸ **Close the mobile app security gap:** Mobile web applications are effectively applications within an application – the native browser on a mobile device – and there are hundreds of thousands of them. While some security solutions give IT the ability to block or allow native applications, they do nothing to provide controls for mobile web applications, creating a mobile app security gap that leaves users vulnerable to risky or dangerous applications on mobile devices. Closing that gap with application and operational controls is a critical step on the path to fully embracing BYOD in the enterprise.

❹ **Set contextually aware policies:** A "one size fits all" policy approach simply doesn't work for BYOD because the needs and expectations of users and IT vary dramatically. Although employees generally accept that IT sets the rules on the corporate network, they are far less open to following the same rules on their own devices off the corporate network. As a result, it is imperative for businesses that are embracing BYOD to intelligently apply security policies based on the user, their location, the device they are using and the network they are on.

❺ **Report, adjust and repeat:** To maintain effective security and appropriate policy controls, it is essential to adjust corporate policies based on real-time data collected from all users and devices. Use reporting tools to not only understand how policies are impacting users and your network but also to quickly identify and remediate infected corporate- and employee-owned mobile devices.

What to look for in mobile security solutions

Although industry best practices are still developing for mobile security, you can begin implementing an effective BYOD strategy today. Look for a solution that can extend threat protection and policies from your corporate network to users in any location, whether they are working on laptops in the office or mobile devices in a café. Your mobile security solution should also offer granular control over both native mobile and mobile web apps. This will allow you to give employees the access they want with the security you need across any location, on any device.

With these simple steps, you can move from a policy of containing mobile devices to fully embracing them in the corporate environment.

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000