BYOD Policies – More than an IT Issue Part 5: Trust Model

Peter Silva, 2012-23-10

#BYOD or Bring Your Own Device has moved from trend to an permanent fixture in today's corporate IT infrastructure. It is not strictly an IT issue however. Many groups within an organization need to be involved as they grapple with the risk of mixing personal devices with sensitive information. In my opinion, BYOD follows the classic Freedom vs. Control dilemma. The freedom for user to choose and use their desired device of choice verses an organization's responsibility to protect and control access to sensitive resources. While not having all the answers, this mini-series tries to ask many the questions that any organization needs to answer before embarking on a BYOD journey.

Enterprises should plan for rather than inherit BYOD. BYOD policies must span the entire organization but serve two purposes - IT and the employees. The policy must serve IT to secure the corporate data and minimize the cost of implementation and enforcement. At the same time, the policy must serve the employees to preserve the native user experience, keep pace with innovation and respect the user's privacy. A sustainable policy should include a clear BOYD plan to employees including standards on the acceptable types and mobile operating systems along with a support policy showing the process of how the device is managed and operated.

Some key policy issue areas include: Liability, Device Choice, Economics, User Experience & Privacy and a Trust Model. Today we look at Trust Model.

Trust Model

Organizations will either have a BYOD policy or forbid the use all together. Two things can happen if not: if personal devices are being blocked, organizations are losing productivity OR the personal devices are accessing the network (with or without an organization's consent) and nothing is being done pertaining to security or compliance.

Ensure employees understand what can and cannot be accessed with personal devices along with understanding the risks (both users and IT) associated with such access. While having a written policy is great, it still must be enforced. Define what is ‘Acceptable use.’ According to a recent Ponemon Institute and Websense survey, while 45% do have a corporate use policy, less than half of those actually enforce it.

And a recent SANS Mobility BYOD Security Survey, less than 20% are using end point security tools, and out of those, more are using agent-based tools rather than agent-less. According to the survey, 17% say they have stand-alone BYOD security and usage policies; 24% say they have BYOD policies added to their existing policies; 26% say they "sort of" have policies; 3% don't know; and 31% say they do not have any BYOD policies. Over 50% say employee education is one way they secure the devices, and 73% include user education with other security policies.

Organizations should ensure procedures are in place (and understood) in cases of an employee leaving the company; what happens when a device is lost or stolen (ramifications of remote wiping a personal device); what types/strength of passwords are required; record retention and destruction; the allowed types of devices; what types of encryption is used. Organizations need to balance the acceptance of consumer-focused Smartphone/tablets with control of those devices to protect their networks. Organizations need to have a complete inventory of employee's personal devices - at least the one’s requesting access. Organizations need the ability to enforce mobile policies and secure the devices. Organizations need to balance the company's security with the employee's privacy like, off-hours browsing activity on a personal device.

Whether an organization is prepared or not, BYOD is here. It can potentially be a significant cost savings and productivity boost for organizations but it is not without risk. To reduce the business risk, enterprises need to have a solid BYOD policy that encompasses the entire organization. And it must be enforced.

Companies need to understand:

- The trust level of a mobile device is dynamic
- Identify and assess the risk of personal devices

- Assess the value of apps and data
- Define remediation options
- Notifications
- Access control
- Quarantine
- Selective wipe
- Set a tiered policy

Part of me feels we've been through all this before with personal computer access to the corporate network during the early days of SSL-VPN, and many of the same concepts/controls/methods are still in place today supporting all types of personal devices. Obviously, there are a bunch new risks, threats and challenges with mobile devices but some of the same concepts apply – enforce policy and manage/mitigate risk As organizations move to the BYOD, F5 has the Unified Secure Access Solutions to help.

ps

Related

- BYOD Policies – More than an IT Issue Part 1: Liability
- BYOD Policies – More than an IT Issue Part 2: Device Choice
- BYOD Policies – More than an IT Issue Part 3: Economics
- BYOD Policies – More than an IT Issue Part 4: User Experience and Privacy
- BYOD–The Hottest Trend or Just the Hottest Term
- FBI warns users of mobile malware
- Will BYOL Cripple BYOD?
- Freedom vs. Control
- What's in Your Smartphone?
- Worldwide smartphone user base hits 1 billion
- SmartTV, Smartphones and Fill-in-the-Blank Employees
- Evolving (or not) with Our Devices
- The New Wallet: Is it Dumb to Carry a Smartphone?
- Bait Phone
- BIG-IP Edge Client 2.0.2 for Android
- BIG-IP Edge Client v1.0.4 for iOS
- New Security Threat at Work: Bring-Your-Own-Network
- Legal and Technical BYOD Pitfalls Highlighted at RSA

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com