BYOD and the Death of the DMZ

Lori MacVittie, 2012-17-09

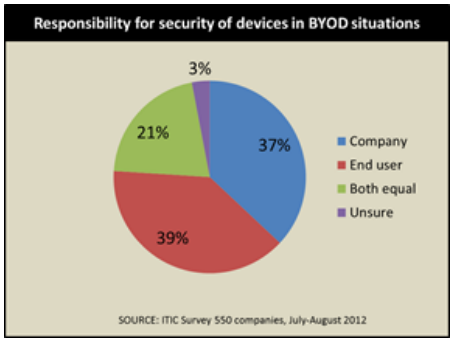
#BYOD #infosec It's **context** that counts, not corporate connections.

BYOD remains a topic of interest as organizations grapple not only technologically with the trend but politically, as well. There are dire warnings that refusing to support BYOD will result in an inability to attract and retain up and coming technologists, that ignoring the problems associated with BYOD will eventually result in some sort of karmic IT event that will be painful for all involved.

Surveys continue to tell us organizations cannot ignore BYOD. A recent ITIC survey indicated a high level of BYOD across the global 550 companies polled.

> 51% of workers utilize smart phones as their BYOD devices; another 44% use notebooks and ultra books, while 31% of respondents indicated they use tablets (most notably the Apple iPad) and 23% use home-based desktop PCs or Macs.

It's here, it's now, and it's in the data center. The question is no longer "will you allow it" but "how will you secure/manage/support it"? It's that first piece – secure it – that's causing some chaos and confusion. Just as we discovered with cloud computing early on, responsibility for anything shared is muddled. When asked who should bear responsibility for the security of devices in BYOD situations, respondents offered a nearly equal split between company (37%) and end-user (39%) with 21% stating it fell equally on both.



From an IT security perspective, this is not a bad split. Employees should be active participants in organizational security. Knowing is, as GI Joe says, half the battle and if employees bringing their own devices to work are informed and understand the risks, they can actively participate in improving security practices and processes.

But relying on end-users for organizational security would be folly, and thus IT must take responsibility for the technological enforcement of security policies developed in conjunction with the business.

One of the first and most important things we must do to enable better security in a BYOD (and cloudy) world is to kill the DMZ.

[Pause for apoplectic fits]

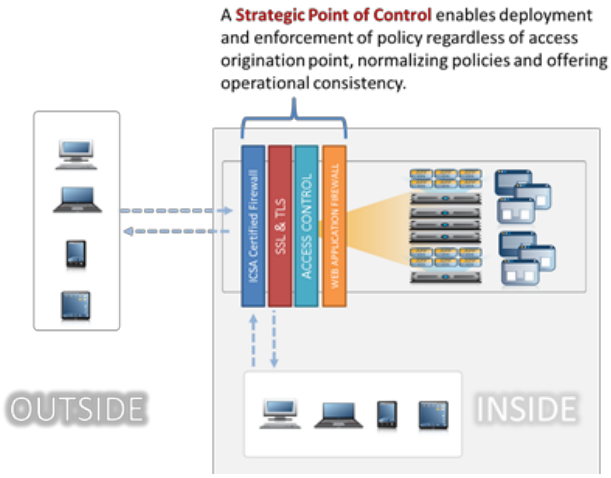
By kill the DMZ I don't mean physically dismantle the underlying network architecture supporting it – I mean logically. The DMZ was developed as a barrier between the scary and dangerous Internet and sensitive corporate data and applications. That barrier now must extend to inside the data center, to the LAN, where the assumption has long been devices and users accessing data center resources are inherently safe.

They are not (probably never have been, really).

Every connection, every request, every attempt to access an application or data within the data center must be treated as suspect, regardless of where it may have originated and without automatically giving certain devices privileges over others. A laptop on the LAN may or may not be BYOD, it may or may not be secure, it may or may not be infected. A laptop on the LAN is no more innately safe than a tablet than is a smart phone.

SMARTER CONTROL

This is where the concept of a strategic point of control comes in handy. If every end-user is funneled through the same logical tier in the data center regardless of network origination, policies can be centrally deployed and enforced to ensure appropriate levels of access based on the security profile of the device and user.



By sharing access control across all devices, regardless of who purchased and manages them, policies can be tailored to focus on the **application** and the **data**, not solely on the point of origination.

While policies may trigger specific rules or inspections based on device or originating location, ultimately the question is **who** can access a given **application** and **data** and under **what** circumstances? It's **context** that counts, not corporate connections.

The questions must be asked, regardless of whether the attempt to access begins within the corporate network boundaries or not. Traffic coming from the local LAN should not be treated any differently than that of traffic entering via the WAN. The notion of "trusted" and "untrusted" network connectivity has simply been obviated by the elimination of wires and the rampant proliferation of malware and other destructive digital infections.

In essence, the DMZ is being – and must be - transformed. It's no longer a zone of inherent distrust between the corporate network and the Internet, it's a zone of inherent distrust between corporate resources and everything else. Its design and deployment as a buffer is still relevant, but only in the sense that it stands between critical assets and access by hook, crook, or tablet.

The DMZ as we have known it is dead.

Trust no one.

Referenced blogs and articles:

- If Security in the Cloud Were Handled Like Car Accidents

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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113