# Drama in the Cloud: Coming to a Security Theatre Near You

**Lori MacVittie, 2012-25-06**

#mobile #infosec #gdi Conflicting messages from various trends are confusing … should you care about the client end-point or not?


On the one hand, cloud:

> "Another key enabling factor for enterprise mobility is the cloud based delivery model for applications. With applications stored and delivered from the cloud, the endpoint device is largely irrelevant, with access allowed through smartphones, tablet devices or laptops. "

> -- Enterprise Mobility ranks highly for IT investment, 25% of businesses rate mobility as a priority in 2012, finds Frost & Sullivan

On the other hand, security:

> "If you want to secure the cloud, you need to secure your mobile devices," he explained. "They are the access points to the cloud -- and from an end-user perspective, the difference between the cloud and the mobile phone is lost."
>
> -- BYOD: if you can't beat 'em, secure 'em

> What's a data center to do? Lock them all out, let them all in. There doesn't seem to be a happy medium. This is comedy meets tragedy without the Greek mythology to make it a satisfying action film.

The conflicting messages are the result of security colliding with productivity, which is probably a lot like security colliding with performance. In other words, we know who all too often wins ***that*** confrontation, whether we like it or not. The problem is that many are approaching the conflict with an either/or perspective. They're trying to answer the question with an allow or deny policy based on the end-point, but ignoring the other end of the equation: the application or resource.

## SOLVE for X to DETERMINE ACCESS RIGHTS

Like the two halves of drama, comedy and tragedy, the client and the resource (whether application or file or otherwise), go together. Settling on a BYOD strategy should necessarily not be based solely on the answer to "do we allow X on the network" but on the answer to "do we allow X to access this resource". For example, in the case of many SaaS-styled applications, i.e. data is always stored in the database or on the server and never on the client, is there some other reason to deny an iPad or other mobile device access over any network?

Probably not.

However, attempting to download that confidential presentation with the latest roadmap of your product line … that may be something you don't want leaving the building on a mobile device, especially those over which you have no control and cannot wipe in the event of loss or theft. Perhaps even if you do have control, you don't want certain sensitive documents or data leaving the perimeter of the data center.

The thing is that a BYOD policy can be as complex or simple as you need it to be. You can solve only for X. You can add Y (the network) to the equation. You can add Z (the user) to the equation. You can even add A, B and C to the equation, if desired, where each represents different user, network, or device characteristics, i.e. is the end-point secured and accessing the resource via a VPN?

But it doesn't have to be the source of more drama than a Greek tragedy starring Oedipus and his ill-fated daughter, Antigone, that's so tragic it's nearly comedic (to those watching, of course).

With the proper tools and the right integration, you can implement a BYOD policy that works in the data center and in the cloud, without compromising security or productivity. Context-aware mobile mediation, in addition to providing developers with consistent identification of mobile devices, can also provide the means by which access rights to applications or resources can be determined. Context-awareness encompasses more than just device-type, it can provide network, user, and environmental variables that can be plugged in to your BYOD/Cloud policies and alleviate the frustrating one-off add-on rules that would otherwise overload operations.

If the context-aware mobile mediation is enabled via an intelligent intermediary, like an application delivery controller, operations is further empowered not just to deny access, but to explain why, in simple HTML, to the end-user so they aren't just frustrated by a failure to connect or a generic "403 Forbidden" status message. Give them an answer; explain to the end-user why they can't download that confidential, highly sensitive document to their personal iPad. Offer some rationale into the policy behind the allow or deny and it might engender understanding from the end-users (or at least eliminate some dramatic tech support calls asking Why oh WHY can't they get that file!?).

Right now the conflict between unfettered access to cloud-based and corporate resources and reality is causing a lot of unnecessary drama. The right tools can enable operations and security to implement more flexible, reasonable access policies that may reduce that drama and return some sanity to the data center.

---

- The Half-Proxy Cloud Access Broker
- Mobile versus Mobile: An Identity Crisis
- The Three Axioms of Application Delivery
- Cloud Security: It's All About (Extreme Elastic) Control
- Total Eclipse of the Internet
- The Cost of Ignoring 'Non-Human' Visitors
- Identity Gone Wild! Cloud Edition

---

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