Prepared by AmCham member

In cloud we trust

Top ways to securely implement BYOD

Cloud services, consumerization and bring-your-own device (BYOD) have forever changed the notion of information security. End-to-end IT control allows workers to make decisions about resources and how they're used. The arrival of the cloud era presents both risks and opportunities for the IT field.

By rethinking security to meet expanded requirements, you can empower workers to new levels of productivity and innovation while still maintaining information governance and managing risk. Fortunately, the progressively open model of enterprise computing doesn't have to be the high-risk proposition some IT professionals fear. The following suggestions will help you not only assure security in the cloud, but also enable the productivity and innovation that the cloud and BYOD make possible.

Design for your fears

IT needs to recognize the new requirements, threats and tactics that cloud computing brings. Traditional approaches to security are often not enough. Many resources are available to help you redesign IT for this new era. Some of the best are the National Institute of Standards and Technology, the Cloud Security Alliance and the reports from the CLOUD2 Commission of the TechAmerica Foundation. By implementing a secure-by-design architecture, you can optimize productivity and security for both IT and employees, while supporting the business imperative for agility and innovation.

Embrace consumerization

IT has long resisted the use of consumer technologies in the enterprise—and for just as long, people have used them anyway. Employees are often more productive with these tools. This is not surprising since consumer technologies are often more advanced and engaging than their corporate counterparts. Isn't it time we helped people work better?

Make IT personal

In the cloud era, the computing experience is tailored to the individual – not defined by IT's need for standardization and control. Allowing personalization in devices, applications and data enables a fit-to-purpose work experience that improves productivity and job satisfaction. A well-defined BYOD policy grants workers choice over their computing environment—not just the device used, but also the personal cloud through which they access resources—while maintaining control and governance over sensitive proprietary data. There is a need to refocus on networking. It's not enough for enterprise networks to be high-speed, highly redundant, resilient and secured against compromise. To enable full mobility and constant access to resources, it's essential to maximize secure portability as well. This includes using service virtual machines (VMs) to achieve network isolation between virtual resources and application-specific virtual private networks (VPNs) to match connectivity and security to the requirements of individual apps.

Refactor access

BYOD and the cloud don't have to destroy information security. In fact, they create both the need and the opportunity to make security much more specific and relevant. Instead of relying on a simple yes/no approach to network access, IT can gain greater control over complex data relationships by making access decisions based on the five W's of information access: Who (identity), What (device), When (situation), Where (location) and Why (usage case).

Define relationships

Relationships are the new networking. Viewing your network as a complex set of connections and policies for relationships between entities, not just simple ports and subnets, will help build and scale to meet the networking demands of the cloud era.

Virtualize to secure

Virtualization unlocks new opportunities and innovations to address business needs—including the transformation of security. Effective virtualization security protects mobility, collaboration and social computing through isolation of sensitive resources, which is essential to the success of BYOD. This protocol keeps sensitive data in the data center whenever possible and complements physical network security controls with virtual remote display protocols to keep sensitive data off unapproved devices.

Presume multi-tenancy

Shared-ownership computing architectures are an important part of the cloud, which has implications for ownership, management and security. A proven multi-tenant design that protects administrative, tenant and external services from each other is essential for maintaining security and compliance.

Own your own

Services-based cloud computing challenges the data center ownership model and BYOD shifts device ownership to the worker. As a result, IT must focus on what it needs to own and manage itself: data and encryption, yes; devices, perhaps not. While IT has traditionally emphasized managing end point devices, what really matters are user sessions and data, which may be accessed via multiple devices. IT can avoid encroaching on the ownership rights of BYO participants and still ensure security on any device by managing access to data and apps rather than the devices themselves.

Enforce end-to-end cloud trust

IT must build and enforce end-to-end trust in the cloud. This is done through security, privacy, transparency and accountability. People need to be able to pick up any device and know what kinds of work they can do securely on it, with an automated security experience for BYOD and cloud services. Servers need to have trust relationships that better protect the sharing and distribution of sensitive data. The network needs to automatically inherit and enforce policies appropriate to the sensitivity of specific data. By ensuring that people, processes and technologies support core principles of trust at every level from architecture to audit, IT can allow the organization to say, "In Cloud We Trust."

Thomas Huber, Director Channel Sales and Development, Eastern EMEA