Embrace & adopt a mobility strategy: Enabling technologies

The innovation and introduction of new technologies over recent years has significantly changed the way enterprises embrace and adopt a mobility strategy. Let's look at some of the technologies that enable an enterprise to adopt a mobility strategy.

Virtualization and centralization

From an infrastructure perspective, it's obvious that a traditional workplace approach to mobility – with a strong interdependency of hardware, operating systems, applications and user environment – is not suitable. However, virtualization makes the individual components independent from each other and enables IT to move applications, data, the user environment or even entire workplace environments from the device into the data center. The user's device will then just serve access to the data center. The only thing that is needed on the device is a virtualization client or just a browser. As the virtualization client is from a major vendor and web browsers run on any device platform, a centralization approach is device-agnostic.

By having corporate applications and data in the data center, a separation of the business from the private environment is achieved. Management is simplified for the IT department as their focus is no longer on the device, but just on the corporate applications and data over which they have full control. Software can be easily deployed and updated, and patches become effective without touching end user devices or disrupting the end user. The level of application and workplace availability is significantly increased; even disaster recovery concepts can be applied. By having all the data hosted in the data center the risk of data theft is minimized. To achieve this, encrypted communication, firewalls, anti-malware and granular role-based access controls are applied to applications and data. Data backup no longer depends on whether the device is turned on or whether it's connected, and compliance requirements are more easily managed and satisfied. Centralization enables end users to access their applications and data anywhere from any device – applications and data follow the user, which is helpful when individuals are using more than one device.

Workplace delivery options

When it comes to centralization, there's not just one optimum concept for every situation. User types, their requirements and economic aspects are also important. Hosted Shared Desktop This is ideal for workers who use and share the same limited set of applications every day on a terminal server, and provides a very low Total Cost of Ownership. But its restrictions – multi-user capable applications, limited individuality and separation from other users – mean it's not applicable for real knowledge workers who need the highest levels of flexibility and individuality.

- Hosted Virtual Desktop

VDI or Virtual Desktop Infrastructure is the best solution for knowledge workers. It features individual desktops with different types of operating systems run as virtual machines on servers in the data center. They are isolated and protected from each other, and can be personalized to each user's needs. Unlike the 'Hosted Shared Desktop,' applications don't need to be adapted.

- Central Hosted Desktop

If centralization is demanded for power users with extremely high demands in terms of graphics performance, the Central Hosted Desktop with graphics workstations in the data center is the only useful alternative.

- Local Virtual Desktop

All delivery options discussed by now require a connection from the access device to the data center. With a Local Virtual Desktop even mobile users can be involved who occasionally have no network connection but want to work offline. By running a hypervisor on their local device users have access to exactly the same virtual desktop locally which is centrally used in a Hosted Virtual Desktop scenario. This means the IT department can manage these mobile users in the same way as stationary workers. The virtual desktop is delivered once from a central image to the mobile device. All work done offline will only have an impact on local copies. Once connected to the corporate network, updates are automatically synchronized with the data center's virtual desktop environment. Synchronization eliminates the need to backup mobile devices, and automatic updates ensure users always work with the latest software and security patches.

Virtual desktops are encrypted and fully isolated from each other and the private host environment, while additional security ensures policies can be put in place. For example, if a device hasn't re-connected to the corporate network for a certain period of time the image will lock itself down. Likewise, data leakage can be prevented by disabling printing or access to local disk drives and USB storage. If the device gets lost or stolen, the corporate virtual desktop can be remotely wiped.

- Local Streamed Applications

An alternative for offline usage is Local Streamed Applications in which business applications are downloaded to the mobile device and run in a sandbox. Data used or generated by the applications can be totally isolated and separated from whatever else is on the device. The rest of the security mechanisms from the Local Virtual Desktop are also available.

- Web Desktop

In the last couple of years the internet has become the main workspace for many users as more and more applications become web-based or at least accessible through the web. The Web Desktop becomes the aggregator for these applications, and to access them a HTML5 compatible browser is needed, which is available on any device no matter which operating system is deployed.

The Web Desktop is most suited to task workers, but knowledge workers and to a certain extent, even power users can take advantage of it. This is true for both stationary and mobile. Due to the local caching feature, minor disruptions of the connection can be bypassed, but this might not be the optimum approach for mobile users, who can have no network connection for any length of time.

The new formula: EMM = MDM + MAM + MIM + TEM

While accessing the web, devices can get infected by malware, which exploits vulnerabilities and then looks for security holes in other systems or business-related containers on the private device. It's true that for all delivery options discussed before, there are solutions in place that protect corporate applications and data. However, it's likely that attempted attacks generate traffic on the network and use up significant system resources of the device itself, in turn causing a negative impact on end user productivity.

Mobile Device Management

This can be significantly reduced by deploying anti-virus/anti-malware software and by running the latest security patches. With a Mobile Device Management (MDM) service all necessary security software and the virtualization client can be provisioned, monitored and regularly updated over the air, without disrupting the end user. MDM can be used to enforce device passwords, application blacklists or whitelists, jailbreak and rooting detection, remotely wipe all critical contents in the event of theft or loss, and helps IT organizations to meet regulatory compliance.

Mobile Application Management and Mobile Information Management

Certainly more important than having a defined level of control over end user devices is the control over corporate applications and data. This is what experts denote as Mobile Application Management (MAM) and Mobile Information Management (MIM). By separating business-related content from private content on the device, business content can be secured and controlled without having to interact or interfere with private content. This means things like business emails and attachments can be restricted from being sent from personal email accounts.

MAM and MIM include the automated enforcement of usage policies based on a number of factors that include the type of device, the type of network and user, and a selective lock and wipe of the isolated, secured environment, without touching the private sphere of the user. Enforcing a password for the container could, from a company perspective, even make the device password superfluous. This might improve the user experience and acceptance in many cases, as not every user is happy if their smartphone needs to be unlocked every time they want to take a picture.

Telecom Expenses Management

Telecom Expenses Management (TEM) is used for managing connectivity, data volumes and time to optimize communication costs. Alongside MDM, MAM and MIM, TEM is another important building block for a comprehensive Enterprise Mobile Management strategy.

This is an extract from Fujitsu's White Book of Mobilizing the Enterprise: Your ultimate guide to Mobility driven innovation. Download the full version from here.

Contact
FUJITSU
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Straße 8, 80807 Munich, Germany
www.fujitsu.com
www.fujitsu.com/contact
2014-06-01 INT EN