VDI IN BYOD: BOON OR BANE?

Vinayak Sivanand
Storage Administrator
HP

EMC²

Table of Contents

Why VDI in BYOD 3

Architecture of Integration VDI into BYOD 7

VDI, BYOD in Health Care 9

Benefits of integrating VDI and MDM 12

Conclusion 15

Appendix 16

Disclaimer: The views, processes or methodologies published in this article are those of the author. They do not necessarily reflect EMC Corporation's views, processes or methodologies.

Why VDI in BYOD

Bring Your Own Device (BYOD) is not about individuals being allowed to connect their personal devices on to the company's network. BYOD is about giving them the ability to use technology they are used to, while ensuring that corporate data remains safe. Virtual Desktop Infrastructure (VDI) in BYOD devices does not access the corporate network, instead it should access the VDI infrastructure directly. The biggest concern for any Chief Information Officer (CIO) is if the company's data will be affected when BYOD users connect to corporate network. Well, the answer is no. In BYOD, there are three ways to protect data:

1. Authorization based on role through PIN, encryption
2. Removing access to data when appropriate
3. Either wiping clean any data stored in the devices or revoking access to fresh data.

For BYOD, VDI can be used for Mobile Device Management (MDM). VDI can be used for application security and user content, while management of device provisioning and user settings is handled with MDM. This balance will be an important thing to noticed and observe to help shape BYOD and VDI integration .

With the increase in the number of smartphones, hand-held device users want to use them to access the corporate data network to carry out their daily activities. IT Administrators can't test every type of mobile device to determine if it's up to par in terms of antivirus, performance, and security standards associated with their organization's environment. The approach below will be a great solution when VDI as a form of MDM is implemented

Without a VDI it's not easy to implement BYOD Strategy . Virtual desktops are the only method by which the end point can be completely removed from the corporate data thereby addressing data storage issues. VDI has a unique way to define business continuance problems by gaining control of the desktop at the server level. End users who connect to it via their hand held devices are simply establishing a connecting to a session running on the corporate servers, similar to a user connecting to a cloud-based application via the cloud.

By use of VDI, the risk of data loss is addressed at the server level itself. In BYOD devices, users generally connect to the corporate network using VMware View client or Citrix Xenapp thus the data remains on the server itself, not on the personal devices. Basically, end users are accessing a session. One could think of it as a cloud-based solution. Even if a personal device

is lost, the corporate IT team need not worry for the very same reason; the data was accessed from the server.

According to a Forrester report, personal devices will become the norm for enterprise computing. More than 70% of organizations will be using a BYOD program[1]. Their Workforce Employee Survey identified that 60% of those who use a smartphone for work and more than 50% of those who use a tablet for work have bought the device themselves

Since in BYOD, IT administrators cannot control what devices the end users would be using to connect to the network, business needs a centralized console /software which can manage any mobile connect Clients[2] like iPad, Android OS, iPhone or Windows OS. Also, the software needs to manage the existing desktop OS as well running on Windows, Linux, or Mac. Hence, the solution developed should be unique and be able to manage desktop OS and mobile OS.

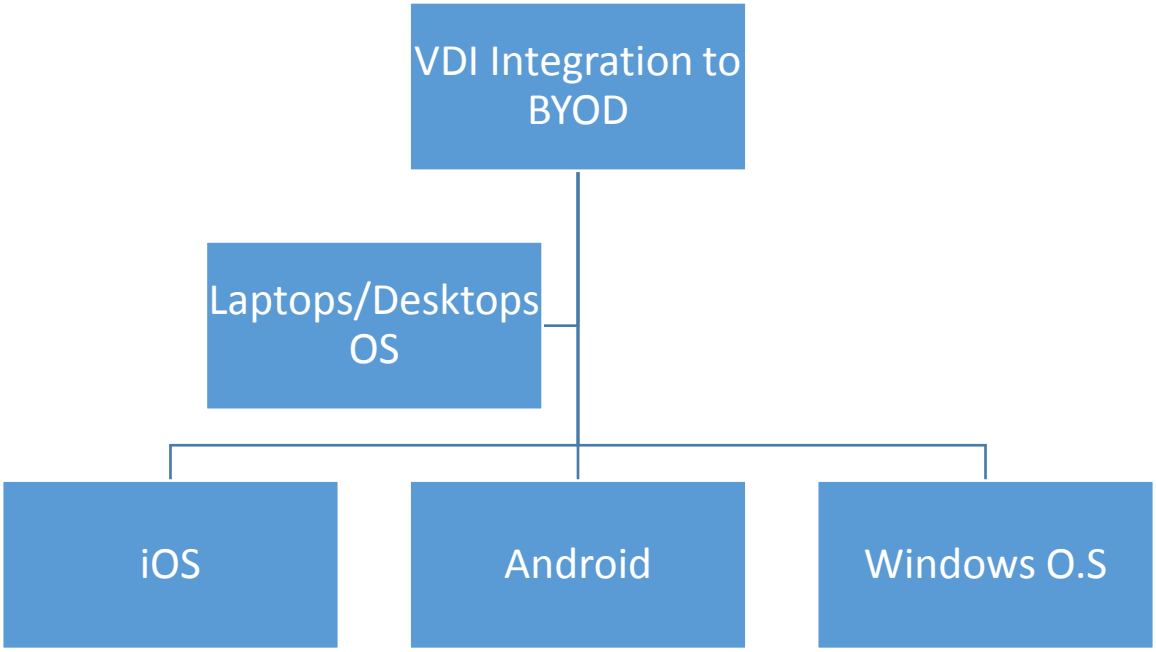


Figure 1: VDI Integration to BYOD

Traditional VDI has a reputation for storage inefficiency, is costly to purchase, and complex to manage. That often makes large-scale VDI deployments, in particular, too expensive and slow to be practical.

Administrators require software that could cache the I/O from each virtual desktop onto VDI compute nodes for common data reads and temporary data writes. This ensures that data is read /written on local storage VDI nodes, rather than remote storage on the storage area network (SAN), thereby reducing traffic and access to network storage as needed .

External storage costs such as Network Attached Storage (NAS) or SAN are the single biggest VDI deployment killers. Consider this scenario. An organization has 2000 users. On Monday morning, they are all logging on. All these users will be connected to access one image on the storage thereby causing a boot storm. This multiplies with more users in the organization.

IOPS are significantly greater when all users are booting Windows at the same time. To overcome this problem, more drives are added on external storage which increases the cost. Most storage vendors have introduced solid state disk- (SSD) based caching blades front-ending, which are very expensive.

What is needed is enough network bandwidth between the VDI servers and externally attached storage server. Cache I/O addresses these concerns by leveraging the local attached storage (which is less expensive) that is available on each VDI server. VERDE from Virtual Bridges is on such solution that is cost-efficient, can be centrally managed, and is very secure. The feature of this software is it provides desktop as a service, in turn reducing total cost of ownership

How do we protect Corporate Data? As discussed earlier, with BYOD, there are three ways to protect the data:

1. Authorization based on role through PIN, encryption
2. Removing access to data when appropriate
3. Either wiping clean any data stored in the devices or revoking access to fresh data.

To improve security, mobile applications need to have a policy enforcing PIN lock Capability. If enabled, the client requires PIN authentication once it is activated. This secures the data from scrutiny if the device is left open and there is no device-level lock configured which is an important feature, since many users would not prefer to use a PIN to access data[3]

Today, most virtualization software has all the above features. However, more important is how best to secure our corporate data without any fuss. The critical thing in this process is to ensure that the data never leaves the server or the data center when accessed using BYOD[4]

Most organizations require user to connect to a corporate network through some form of Remote Secures Access (RSA) which means a private tunnel is established between the client session and the remote server.

Architecture of Integration VDI into BYOD

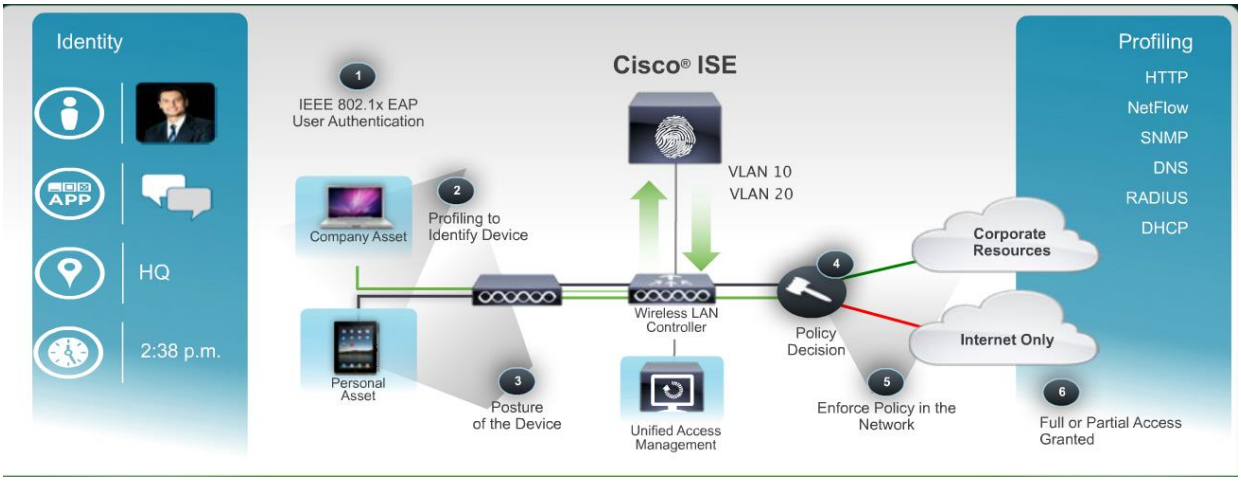


Figure 2: Source: Cisco Prime Unified Architecture

Figure 3 depicts how MDM is integrated into BYOD thereby making VDI more compatible to run on the end users' iPhone, Android devices, or any mobile OS. When a user connects to the corporate network, the following log on processes take place. First is the PEAP which is a more secure way of wireless access. That specific device then needs to be registered into the corporate network so that it can be managed by IT. Once that step is completed, a request certificate is issued which needs to be accepted by the device owner in order for the employee to be granted access to the corporate network. Once this is established, the MDM registration process takes place. The system then checks for compliance with set policies by the administrator for compliance. Once it meets the required criteria, full access is granted.

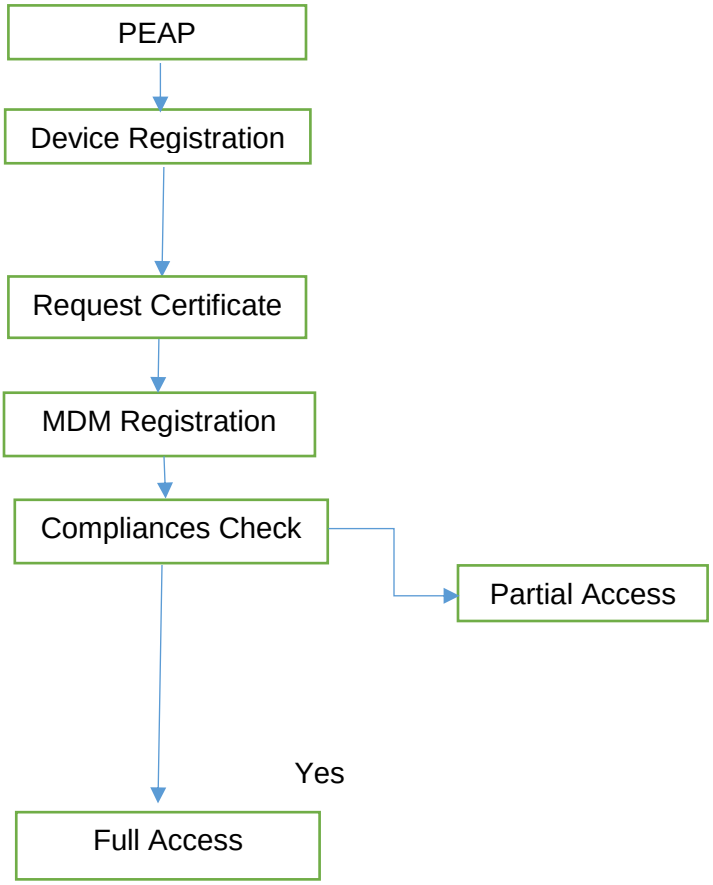


Figure 3: MDM integration into BYOD

The strategy above ensures there is a private tunnel between the mobile applications and corporate data network and that these specific devices are authorized are allowed to access the corporate data. This reduces risk of security issues and both the user and the IT administrator are assured of compliance .

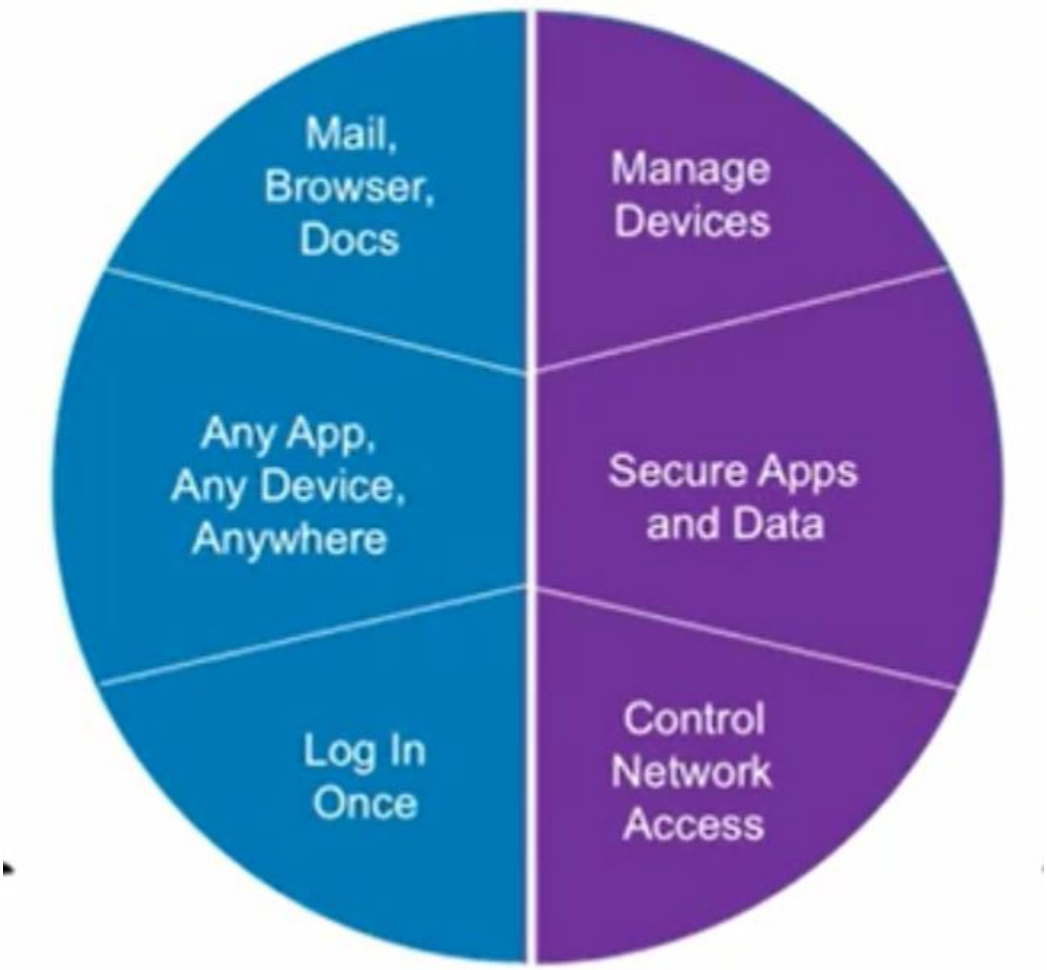


Figure 4: Managing mobile devices, apps, and data - Source: Citrix

VDI, BYOD in Health Care

Doctors and nurses sign in to their hospital IT network to access patient files, emails, their local desktops, applications hosted in their local desktop, and some amount of storage space. It becomes difficult for them to carry out their daily activities, i.e. having to come back to their workspace to update a patient file every time, if these are available on only one fixed system. Instead, having these applications and services available by just a click would increase their productivity. With a next-generation secured point architecture, Doctors and nurses can bring their iPads, iPhones, Android devices, etc. and have on-the-go access to their work-related information. This is made possible by technologies from VMware and Citrix which right now they provide access via unified web portal. The beauty of this method is that nothing is stored on the individual's device.

From the time that a user accesses data until the time that data is stored on the backend systems, the whole phenomenon is delivered to them virtually keeping the whole session secured. This is the concept of secure mobility. It could be thought of like Chromebook trying to access local desktops, apps, and other resources and giving the admin control of user data and resources. All these are achieved by developing the next generation secure endpoint architecture

Through clinical and business process improvements, along with technology, healthcare can achieve an interconnected, patient-focused environment. This provides all industries with assured business benefits of customer focus, cost optimization, quality of care, security, and compliance.

Figure 5 illustrates VDI in a HP BYOD healthcare architecture.

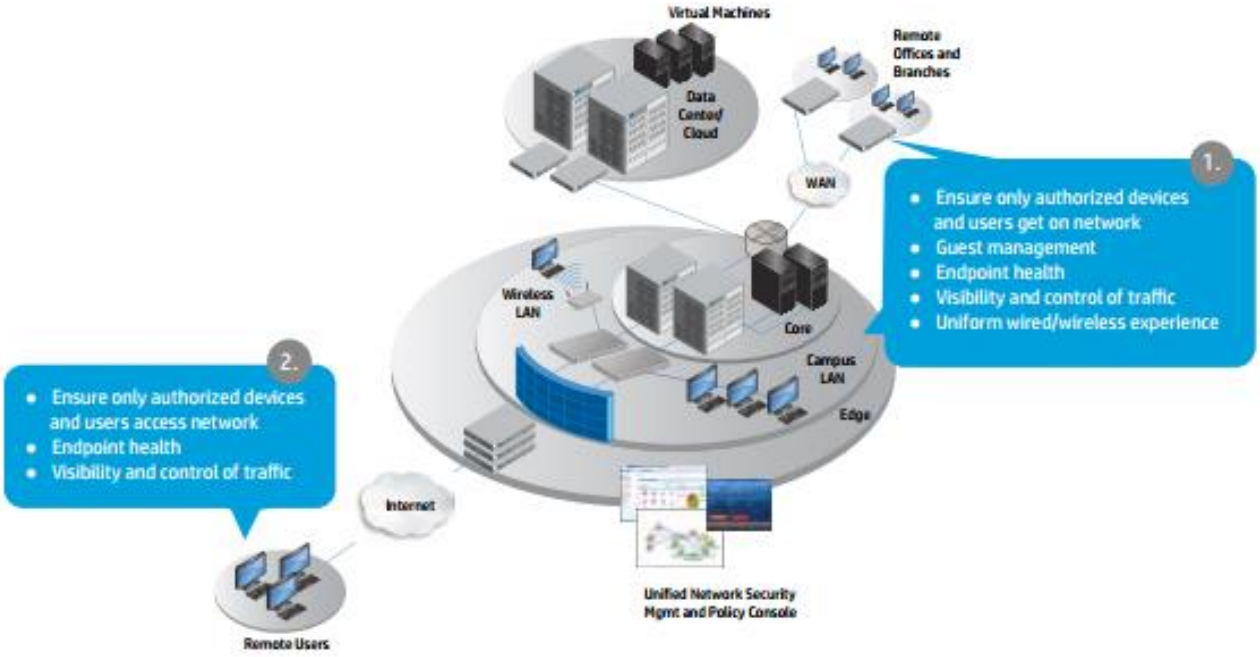


Figure 5: Source: HP BYOD healthcare[6]

Benefits of integrating VDI and MDM

In VDI, changes to the data occur at the backend while the client accessing the data communicates with the server. Only the differential changes to the data is transmitted and not the actual data itself is saved on the client. Subsequently, users can make changes to the data but its saved at the backend storage, ensuring that no data is left at the endpoint device. This is an important factor in which the data is always safe and secure.

Though diversity of mobile devices makes traditional IT management hard to unify, combining VDI and MDM can provide unified management of various mobile devices. Not having to develop management policy for different equipment and systems reduces management complexity.

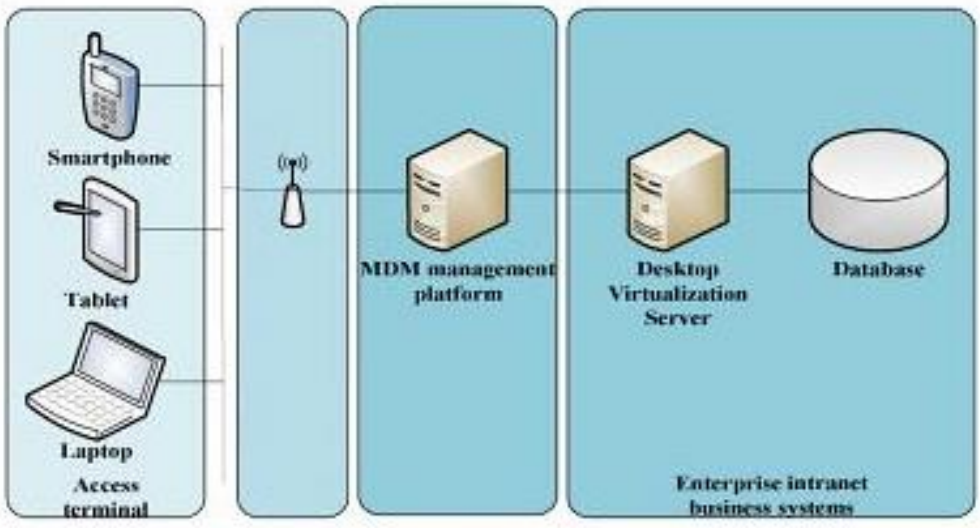


Figure 6: VDI and MDM integration – Source: Gary Lee

MDM can provide double network access control, prohibit unauthorized access, and also prevent user access through the network without enterprise certificates. Generally, MDM identifies the data and locates the specific mobile device using Global Positioning System (GPS), an important feature of using MDM. Desktop virtualization works with MDM to guarantee security of the data.

MDM isolates sandboxes in mobile devices where authorized application files are stored and can separate enterprise data from private data. Isolating desktop virtualization client and other office software not only reduces the risk of use of malicious software but also provides a preventive mechanism for any viruses being spread from a mobile device to enterprise data.[5]

MDM authenticates at each level and can execute different management policies like device identity, device type, application type, location. When the device is lost, misplaced, or stolen MDM has the capability to erase the desktop virtualization software

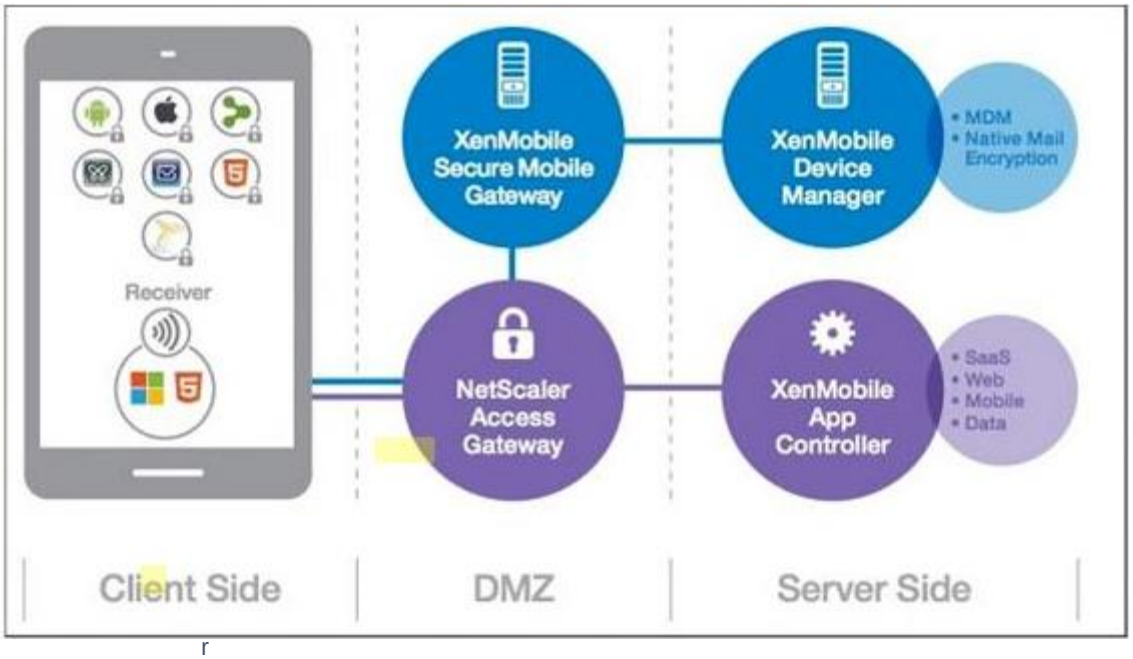
VDI on a mobile device is almost like accessing emails on regular desktop machines. Administrators are really not worried about which web browser or PC type the application is hosted on. They simply manage the backend server environment.

MDM solutions can complement VDI solutions. After all, the challenge of delivering the Wi-Fi settings and certificates to a smartphone is easily addressed with MDM solutions that allow administrators to perform activities by sending an email message or URL to the user. The user will click on the URL and automatically get their device configured for access without being concerned if they are downloading the right applications, entering the right settings, or any setup issues as these are addressed by the MDM

Basically, MDM is not a security component of a BYOD program as VDI offers full security capabilities. As such, both solutions work together well, and increasingly both are being used. What VDI addresses is how to handle application security and user content, while device management, provisioning, and basic user settings are addressed by MDM. It will be interesting to observe how VDI and MDM work hand in hand as BYOD and mobile productivity continue to capture the market.

Citrix provides mobile device management through Xenmobile, enabling corporate IT administrators to manage tasks on highly secured environments. Xenmobile helps manage BYOD and allows administrators to configure role-based management, i.e. automatically blacklist or whitelist apps, search for jail-broken devices, etc. This is a very important feature for a secure mobile environment.

Xenmobile also allows additional features like work mail, work web, and share file integration so that organizations can safely and securely access emails. There are other solutions available from different vendors which are container-based which limit native applications. Container-based solutions are applications that integrate corporate data, email contacts, and so forth. The disadvantage in such solutions is it limits the user specific to a native applications. XenMobile provides organizations the ability to automate most of the administrative tasks on mobile devices for both corporate and highly secured environments [11].



r

Xenmobile -MDM Architecture

Conclusion

With the help of supplier, it is important to get a clear picture of the current infrastructure, ways of working, and business needs before deciding how to manage BYOD. If it is decided that VDI is the right approach to drive BYOD for the business, you can look forward to cost savings, massive productivity improvements, and most important, a significant competitive advantage. VDI is an important solution for a true BYOD strategy from a data loss perspective. Virtual desktops are the only means by which the endpoint can be completely removed from the corporate network thereby eliminating concerns about data storage and data loss from a non-corporate asset.

This is an exciting time in the world of IT. By integrating VDI and MDM solutions, companies and employees are working together to shape MDM in the future. Over the next few years, MDM will play a larger role in providing a customer environment in the corporate world.

Virtualization and MDM are effective ways to address security threats. This article proposes a solution to combine virtualization and MDM to ensure endpoint device security management in the enterprise. Bringing a new technical reference to the enterprise can solve security problems when the enterprise deploys BYOD.

Appendix

1 “2013 Forrester Mobile Security Predictions” - Chenxi Wang

2 AirWatch by VMware

3 BYOD, MDM, NAC, DLP, VDI and Beyond – Shamoun Siddqui

4 VDI Answers Critical BYOD Challenges – Aamir Lakhani

5 Advances in Electrical and Electronics Engineering – Gary Lee

6 “Bring Your Own Device in health care” - HP Business White Paper

7 http://www.vmware.com/files/pdf/view/VMware-View-Datasheet.pdf

8 http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/xenapp-datasheet.pdf

9 http://vbridges.com/docs/VERDE6AdminGuide.pdf

10 http://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html

11 Instant Xenmobile MDM – Aamir Lakhani

VMware View[7]:

- Centralized administration and management
- Encryption using SSL tunneling
- Usability, security, centralized control, and scalability.
- Simplifies management of patches, updates
- High availability and advanced features in managing virtual desktops

Citrix Xen App[8]:

- Allows any mobile users to access their doc ,files on the run via P.C , netbooks, smartphones
- Simplified management of data which secures enterprise data
- IT management of devices using Xenapp is very easy
- Improved performance and reduces complexity leading to increase in user virtualization
- Achieves on demand application features

Verde[9]**:**

- Desktop management and provisioning is easier using this software
- Reducing VDI storage costs and improving performance with Verde Storage Optimizer Cache I/O Technology
- Works with cost efficient NAS storage and existing SAN's
- Improves the security by unifying desktop images making Administrators easier to manage
- An important feature of Verde is Integrate VDI and Verde LEAF(Live Environment Access Format) for online and mobile users
- Gold Master Image Provisioning model

Cisco ISE[10]:

- Identity based security feature from Cisco
- Creates and enforces security and access policies for endpoint devices
- Provides policy based access to the users of the corporate network and unified infrastructure
- It works with VPN, wireless network, or wired networks
- ISE collects the endpoint data and can deliver a device classification
- Cisco Prime is a network management tool which works with ISE which helps in providing devices and application security
- It helps secure network connectivity