# LOBSTER SHACK IT



good morning. Thank you all for coming. My name is Michael and this session is entitled “Lobster Shack IT: or how IT must change to support a BYOD world”. This session is designed to cover what i have learned through my various experiences, training, and efforts to prepare an IT environment for the BYOD revolution. A little background on me, I have been working in IT for over 13 years, and have been an Apple tech and administrator for most of them. I did a tour if duty as a Mac Genius for 3 years, which gives great incite into the products and how they work. I wanted to. Go beyond that and learn about integrating those technologies into corporate and education environments. I recently worked at a company in MA, who hired me to help implement Apple technologies into their environment. An environment that, up until that point, had be 100% Microsoft. Any of you who have gone through such an implementation knows how much fun that can be.

# BYOD



In fact, it is these types of integrations that has gotten me into the BYOD space. We have only recently seen the term “BYOD” become a catch phrase, but, in truth, it has been around for a while. A show of hands, how many people in the room own their own smartphone, doesn’t matter the brand or OS? And of those, how many have your phone, or know someone who has their phone configured to receive work email? How many of you have encountered these devices on your corporate network?keep your hands up, and everyone take a look around. You are all part of the BYOD revolution. It is all around us. IT is only now starting to catch on and catch up to it.

# BYOD

## Bring Your Own Device



This is the inherent problem with BYOD: consumers love the idea of “Bring Your Own Device”. They love that they can have their work and personal lives on the same device, or devices. Even with the threat of constantly having to work, they still want it... but for IT folk, BYOD is more like “Bring Your Own Disaster”.

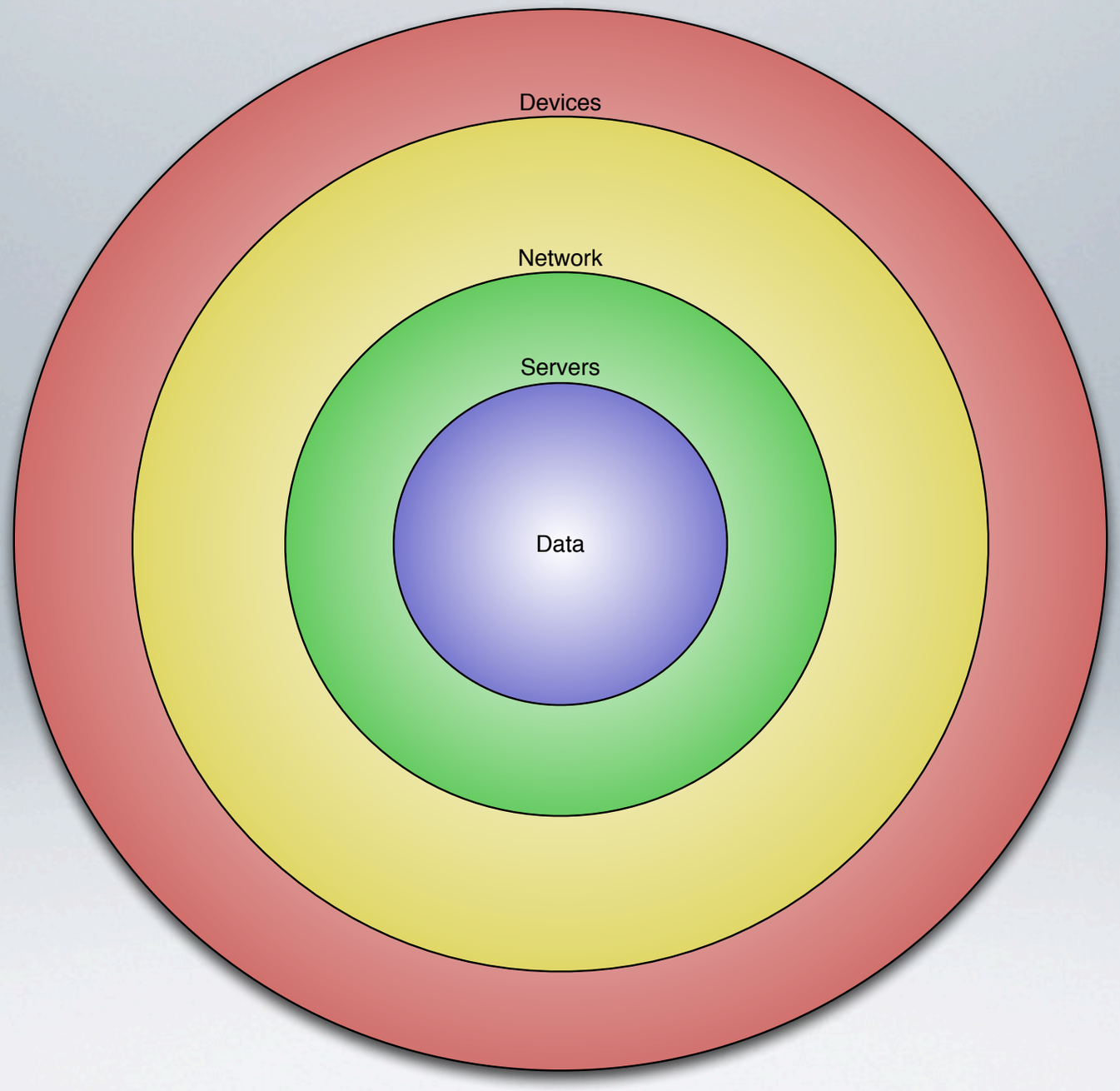
# BYOD

## Bring Your Own Disaster

MDM =BYOD



Why is this? Well, Part of that catching up to it is figuring out how to deal with the influx of devices that IT does not own. How many of you have implemented in MDM in your environment? This tends to be the typical knee-jerk reaction the many IT departments take as a response to the influx of people bringing in their own devices, their own smart phones, their own tablets and computers. Part of the problem with this response is that it is a addressing only a small part of a much larger issue. This solution is focusing on the device. And it is that mindset, device control, that causes IT more issues and drives many to try to stop BYOD. In order to better understand why, let's take a look at a chart that describes the traditional IT infrastructure.




Wednesday, May 22, 13

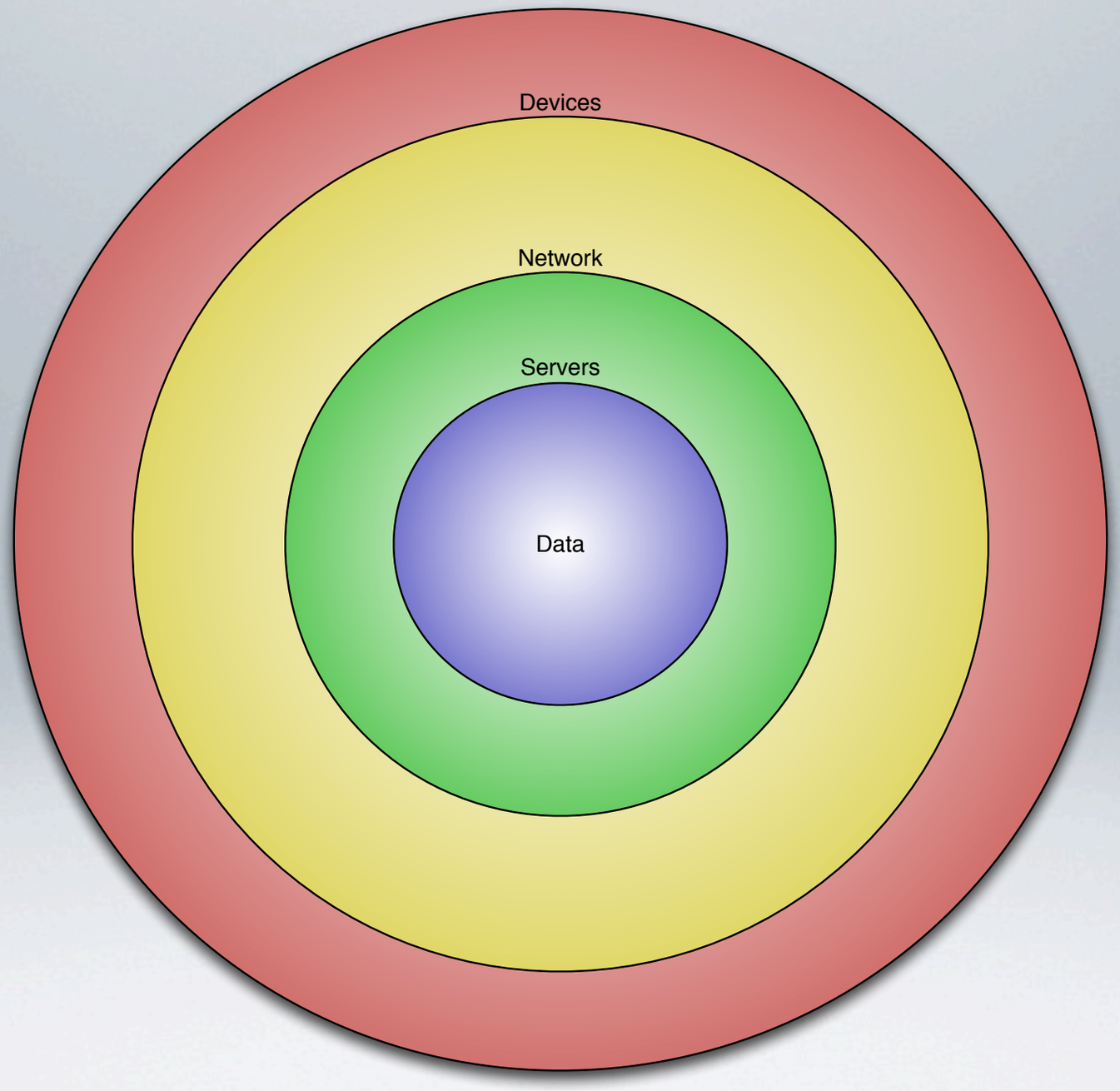
I made this chart for the director of IT at the last company I worked for. it was designed to simplify what was in my head. As you can see I divided up into four basic domains: the data, the server/applications, the network, and the end-user devices. I wrapped them inside each other because that is essentially how we work... the data is central, applications access, modify, and share data, and the network delivers the application and/or data to the end user devices, which are also controlled by IT. This is how traditional IT has functioned for years. It doesn't just reflect the technical side of things, but also the mentality IT personnel have. It is our comfort zone, because it allows us to control every single aspect of our infrastructure that we are responsible for, end-to-end. And let’s face it, IT people are control freaks. We want to control every thing! One needs only to take a look at the hundreds of Access Control Entries and group policy objects we can set for Microsoft products, to see the level of control we desire. It is the mentality that has been pervasive in IT for the past 30+ years.



In many ways, it is a bit like a traditional sit down restaurant. Think about it: from the moment you first arrive, you are shown where to sit, provided all the tools necessary to consume your meal, you are given menu with a pre-defined list of options to pick from, everything is brought out prepare for you, and all you have to do is enjoy your meal.
Traditional corporate IT is very similar. From the moment a user shows up, they are given a desk and chair, provided a computer with all the tools that they would need (and locked down as much as we can), they are given a small list of additional applications they can choose from, and all they have to do is start working. The devices are strictly (or not so) controlled.
But in the world of BYOD, this model begins to fail. after all, we can't take full control over these devices because we don't own them... our users do. And this is the most common argument most IT departments give when trying to dissuade upper management from allowing BYOD. But, there is another way...

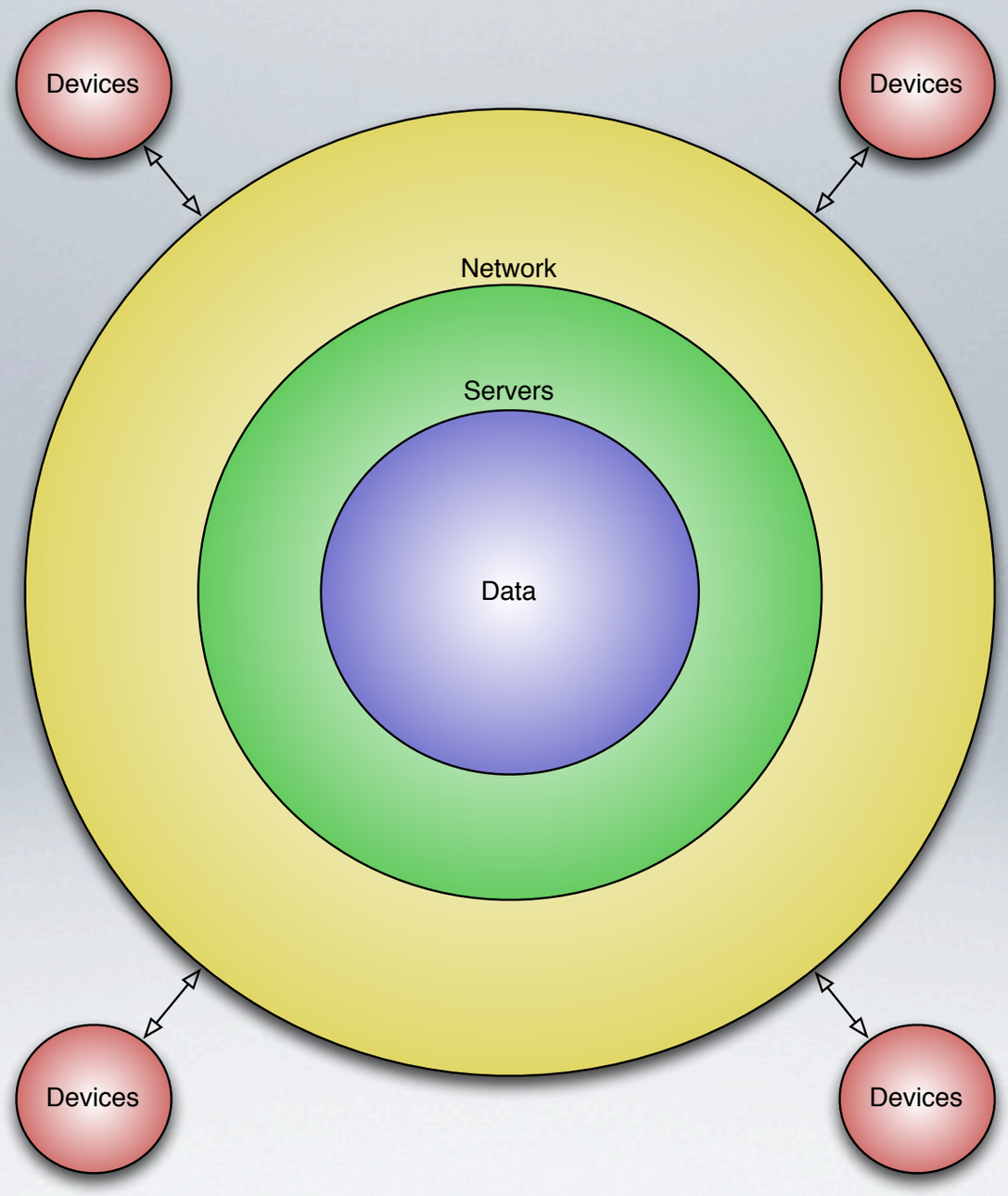



If traditional IT is like a sit-down restaurant, then then to continue the food analogy, an IT environment that supports BYOD could be likened to a Lobster Shack. Has anyone here ever been to a real lobster shack? Or any road-side stand? They actually fully support BYOD: Bring Your own Drinks. You bring the drinks, chips, whatever else you want, a blanket if you do not want to sit at a picnic table, and you are provided just what you need through a small window. You don’t go inside, you don’t see the inner workings, you simply get just and only what you need.






In IT terms you would wind up going from a model that looks like this...






To a model that looks like this. This is the new model for IT departments. The end user devices are all on the outside, they all connect up to the corporate network and systems and they only have access to just what they need to get their work done.

*The abstraction of data from the device*



This lobster shack IT model can be summed up in a sentence: “The abstraction of data from the device”. That is the one underlying goal, the one concept, the secret, to any successful BYOD implementation. If there is one thing you take away from this session, let it be that idea. Too many IT departments focus on the wrong idea of controlling the end user devices because they have data on them. And they continue to do so in the service of BYOD. Instead, we should think about controlling the data because it is on end user devices. When working in this mindset, BYOD no longer becomes the end goal, rather it becomes the inevitable result of a properly structured IT department.

Ask yourself this question: if an engineer looses his laptop in an airport, what do you care more about: the $1500 laptop, or the code he was working on for your next big product that could be work millions? The data, of course. So why are we so focused on the device? We should be focusing on the data. As we go through this new model of IT, keep that in your mind: everything is in service of the data.

# Data



So, since we are on the topic, and since everything is about the data let’s look at the subject of data first.


Wednesday, May 22, 13

What is data? More importantly, what is your data? Not the easiest of questions to answer. So let's break it down a bit. What kinds of data do you have? Now an Excel file, or an email, those aren't really "kinds" of data, so much as they are "types" of data or data formats. What is in them? Financial documents? Payroll, HR records, code, schematics, product documentation, sales figures, etc... These are all "kinds" of data. The first thing any IT department needs to do is to find out what "kinds" of data they have and perform a risk analysis of that data.

| Severity | | | | | |
|---|---|---|---|---|---|
| **Chance** | Insignificant | Minor | Moderate | Major | Severe |
| Almost Certain | | | | | |
| Likely | | | | Code | |
| Possible | | | | | |
| Not Likely | | | | | |
| Rare | | | Payroll | | |



This is an analysis that will rate the data a company has on two primary factors: the likelihood of data being lost, and the potential damage such a loss could incur. As an example, HR personnel files have an incredible amount of sensitive information in them, but if only 1, 2, or 3 people have access to them, and they do not work remotely, the actual risk of data being compromised is actually low. Source code, however, may be shared by a number of engineers and they do work remotely. In that case, the risk is much higher. This type of discovery and analysis is the first step to understanding your environment and will help guide your future decisions on your data.




The next step is to determine the “types” of data, or the “formats” that the data is in. Microsoft Office documents, email, databases, cloud services, etc. You might be surprised how much data is actually in email form, which I always find strange since email is neither a good repository, nor a good presenter of data. Yet, people seem to have the pension for sending other file types such as those Word Documents or PowerPoint Presentation via email, and keeping them there for reference. So, that data doesn’t just exist in a Word Document, but in an email as well. This type of discovery is equally as necessary as discovering what “kinds” of data there are.

*The abstraction of data from the device*



In order to reach our goal “Abstraction of data from the device”, we must embrace and work towards two principals:

*The abstraction of data from the device*

Device Independence

Vendor Neutrality



“device independence” and “vendor neutrality”. Now, what are these principals?

# Device Independence

*Data should be able to be accessed, viewed, modified, and saved using any device from any manufacturer*



Device independence means that data is accessible from any device, regardless of type or form factor. This concept is important: Data should be able to be accessed, viewed, modified, and saved using any device from any manufacturer.

# Vendor Neutrality



The second part, “vendor neutrality”, is equally important.

# Vendor Neutrality

*Data should not be locked in to a specific proprietary format*



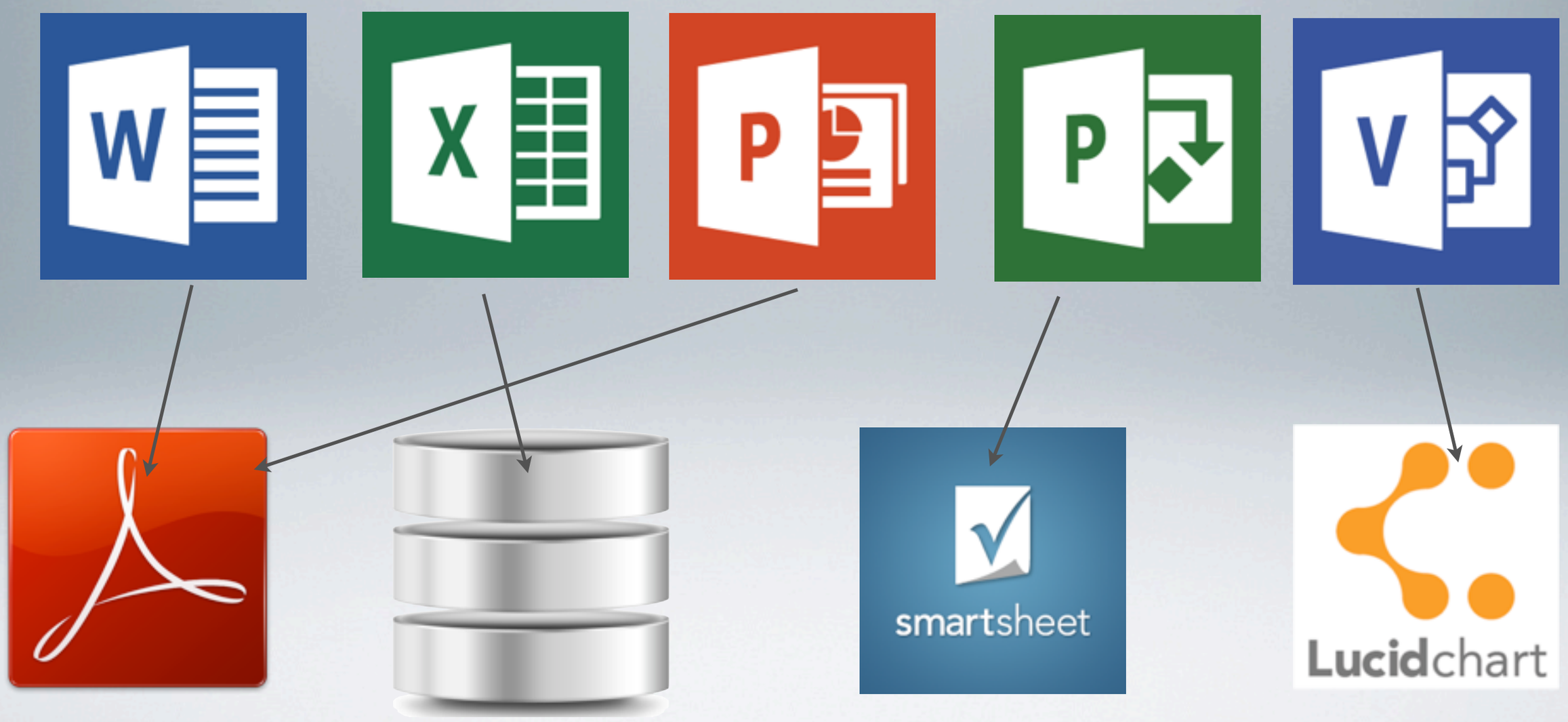
This means that data should not be locked in to a specific proprietary format. Now, this can become the subject of heated debate, so let me show you why this concept is important.


Wednesday, May 22, 13

Take Microsoft Office for example. Think about how many Word documents, Excel spreadsheets, and PowerPoint presentations a company might have. These file formats are, in fact, proprietary. They are owned by Microsoft. Now, in this particular case, The chances of this are slim, but consider the potential fallout if Microsoft simply shuttered it doors tomorrow, or even just stopped selling Office. That is the danger of proprietary formats, and why we must start looking at alternatives.




Now, before I get angry letters from Microsoft, I am not implying that everyone should stop using Microsoft Office. It happens to be the best, and de-facto office suite out there. But, in a world where Office doesn't run on every device, and there is a lack of feature and application parity on the devices and OS's it does run on, it would behoove us to at least consider alternatives for certain types of data.






Maybe that document can actually be a web form. Perhaps that Excel spreadsheet can become a database instead. Realistically, you will never completely eliminate every proprietary format out there. Even Apple is wrought with them, just look at iWork. However, companies like Google have been pursuing this very idea with Google Apps Suite, which can save to open formats like OpenDocument. As IT folk, by attempting to move as much data as we can to open standard formats, we protect our data, and make it more accessible.

While on the topic of data, one system you may want to start looking at, as it will play a crucial role, is a Document Rights Management System. A DRMS is designed to provide fine-grained control over files you have. They go far beyond read and write, to prevent or allow actions such as saving to a flash drive, printing, copying from, and emailing. It works in combination with permissions that are set by Active Directory, but are designed to add additional support. One such applicant is made by GroupLogic called ActivEcho and it's companion called MobileEcho for mobile devices. Microsoft makes one as well, that is integrated with their file server and works with SharePoint, and I believe Adobe makes one.

# Applications and Servers



Which leads right into ring two of our lobster shack IT model: Applications and Servers. Applications are the windows to our data. They are what allow us to see into our data, to create, manipulate, store, and share it. As we start to move our data and look at how we can make it more available we have to start thinking about access.







Again, the concepts of “platform independence” and “vendor neutrality” are still at play here. Let me ask, how many people here use Evernote? How about Dropbox or equivalent? How many have iWork on their iOS devices, or use Google Docs, or Roambi? The days of the full-fledged, fully integrated office suites that do everything and cook your breakfast are not the necessarily the only game in town anymore. They have not been so much replaced, as they have been augmented with all of these other, more specialized, applications and systems. We want to make sure that our data is able to be viewed on any device. And there are a few options for applications, depending on the “format” of the data:

hybrid clouds

Public clouds

The Cloud

private clouds

hosted clouds



The first is “The Cloud”. We have heard this term used ad-nauseum. Public clouds, private clouds, hybrid clouds, hosted clouds,

Wednesday, May 22, 13

# nimbus clouds

Wednesday, May 22, 13

# cumulous clouds

Wednesday, May 22, 13

its like a freaking rainstorm.




“The Cloud” is one of the more amorphic and difficult to define terms in modern day technology. And yet, it is more crucial than ever, because cloud-based applications are quite useful and can be quite powerful. An example: SalesForce. SalesForce, for those who have not used it, is a CRM suite that is completely based in the cloud. Companies use it for all of the sales, client management, reporting, etc. A lot of data can go up to SalesForce and it is completely customizable. At my last company, we used Salesforce, not only for sales, but as our Help Desk ticketing system. It is also open, with APIs that allow for developers to integrate and build on top of the SalesForce system, turning it from just an application, to a full-fledged software platform. And we are starting to see more and more software move to the cloud.

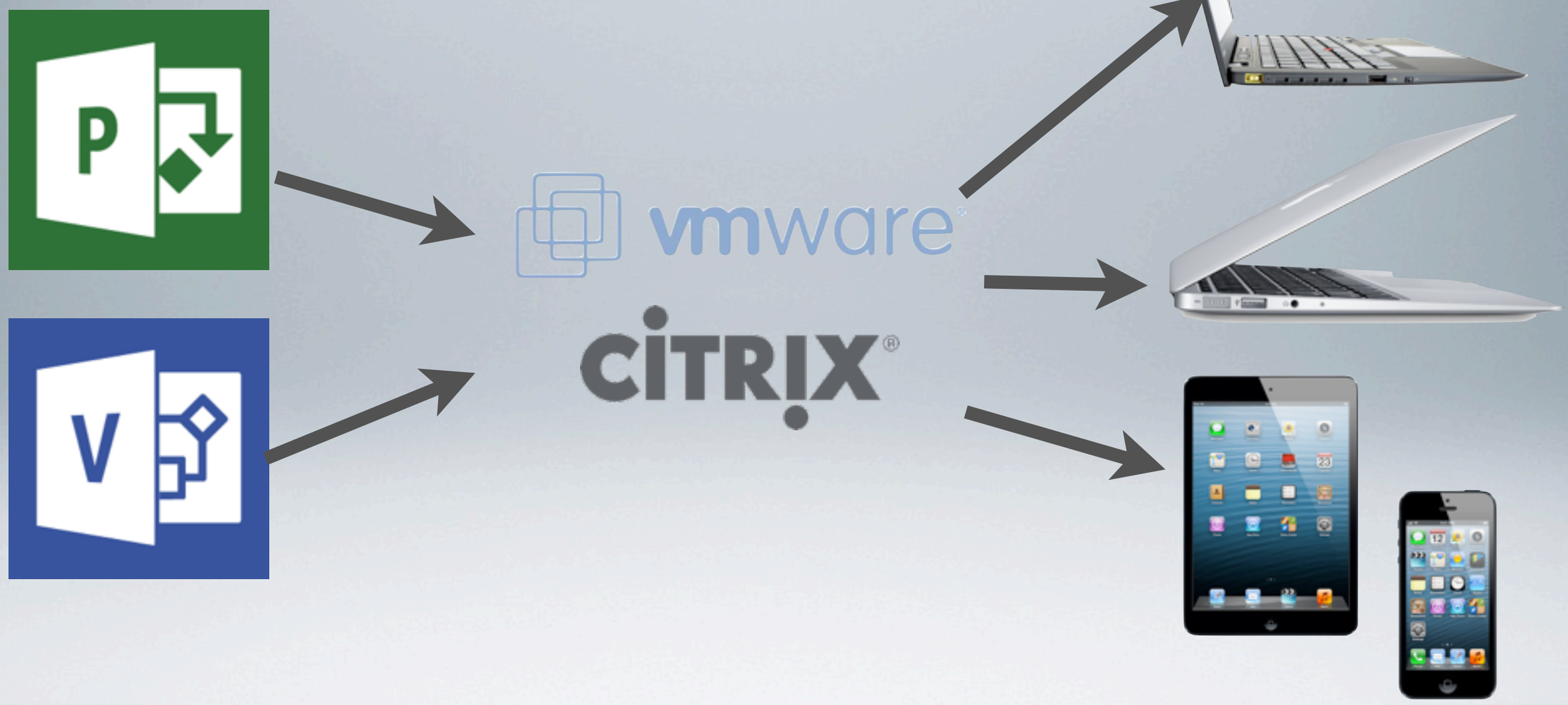
# Application Virtualization



When there isn't a cloud application available, or when data is in a proprietary format that locks it into a specific application, what do you do then? The next option is Application Virtualization. This is a really powerful way to deliver device or vendor specific applications and data to any device.



A prime example would be an application like Microsoft Visio or Project. There are no Mac or Linux versions of those applications, and their data formats are proprietary. So, what do you do when a Mac user needs to open a Project file, or a Linux developer needs to see a diagram?






Application virtualization allows for those applications to run on a server and be remotely streamed down to the user, regardless of the platform. Citrix has an excellent product called the Citrix Receiver, that works wonders on a Mac. Point and case, at a previous job, we actually virtualized LANDesk Management Suite. And anyone who knows this application knows that it is a beast. It is a Lifecycle Management tool that does everything from executing scripts and installing applications on remote machines, to remote control, to Inventory scans and more. The console is Windows-Only. But I had it running at near-native speeds on my Mac, thanks to Citrix Xen server and Citrix Receiver.

Taking virtualization to the next level, there is, of course the Virtual Desktop Interface, or VDI. Instead of an application, you virtualize an entire instance of an OS, and stream that to a machine. Now, what good is that? In a corporate environment, if everyone has to be in a locked down, Windows environment, you can do that, and still allow for your users to utilize their Macs. They can even access it from their iPads. There are cases for this, such as the need to work on ultra sensitive information, or having a complete Windows environment for development.

Now, many argue about the value of virtualization and the costs involved. Yes, there is a requirement for an investment of infrastructure. And, by itself, virtualization may not prove to be a worthwhile venture in traditional IT environments. But, taken in the context of the larger picture. The lobster shack IT model, there are added benefits and savings. First of all, you do have the savings on end user hardware. Second, you have the savings on licensing. In the traditional model, you would deploy a copy of Visio to every user who might need it for their job, regardless of whether they use it constantly, only once or twice, or not at all. If you have 400 users who might use it, that is 400 licenses. With a virtualized model and a little research, you can purchase just the licenses you need. In the case above, if there are 400 people who might use it, but only 50 at the most at any given time that do, you can by 75 or a 100 licenses for a buffer and save the cost of 300 unneeded CALs. And it means you can update everyone at once, in near real time. One patch applied in one place, and everyone has

# Local Applications



There is a third option as well. In some cases, there are equivalent applications on each different device that allows for the data to be cross platform without additional help.A simple example is Microsoft Word. As of the latest versions, Office for Mac and Office for Windows are essentially equivalent. The advantage of this scenario is that it allows for the data to be shared, while allowing each application to be built to take maximum advantage of that device and interface. Evernote is a great example, where a single platform has multiple versions of the application depending on the device and OS. This allows access to all of your notes, through the native interface you are used to: Mac Windows, Mobile, etc. Other applications, such as Roambi, are designed to re-format data to take advantage of the mobile screen space and interface. Custom applications can be developed in-house as well, allowing you to build just what you need for the devices you need it on... Bringing the data to the device, not the device to the data.

These application models: cloud, App Virtualization, VDI, and local applications, are what IT departments should be looking to implement, based on their data and what formats they can get their data into. And this is the general order of precedence that should be used.

# The Network



Now, once you understand your data, have it in the right formats, and have the applications in place to access that data, you need to get those applications and that data to your users. Which leads to ring three: the network. This can be an area of extreme pain for some, and for others, not at all.

The Network

Capacity

Encryption

VPN



There are three aspects to focus on: the strength and capacity of the network, Encryption and VPN

Capacity = Bandwidth



The first part: strength and capacity of the network is straight-forward. There is no way that 2 MB pipeline out and a 10/100 connection internally is going to handle streaming applications to 500 people. Ensuring that there is enough bandwidth internally and externally to handle the increase in traffic is the big key here. Ensuring that wireless networks are about to handle the increased number of connections and increased throughput. Ensure you are not clogging up your network by having GB ethernet everything running into 100MB phones for the last mile (my company did that).

# Encryption



The second part is encryption and segmentation.

Encryption

*SSL*

*802.1x*



Every connection to every device should support end-to-end encryption. There is no reason to not have intranet sites use SSL. There is no reason to not have proper certificates on your servers and for your services. There is no reason to not have proper certificates for wireless 802.1X. There is little reason to not encrypt or at least sign email traffic.

# Segmentation



Equally so, segmenting the network to ensure that a user cannot just plug in any device and get full access to everything is necessary.

# Segmentation

*The dividing of a network to allow or deny access to data or systems.*



Network configuration is black magic to me, but there are ways to route traffic as such that a device can plug in and only be allowed out onto the external internet until a user signs in, authenticated, registers a device, and then, simply based on their access, can get to just what they need. Cisco has some excellent implementations of this. In addition, Cisco and MDMs have way to setup geo-fences, allowing for various levels of control depending the location of a device.

# VPN



And finally, VPN. In the lobster shack IT model, VPN, like segmentation, is that window that you walk up to to order your food. It is what will give end users and their devices the ability to access the network from outside the building. We want to keep this window as small as possible. But we also want to make sure that any device can connect. Once again, “device independence” and “vendor neutrality” plays a role. We have a SonicWall setup at my work, which does not have a Mac client. It costs an additional $99 a node for every Mac we need to connect to the VPN because we have to purchase 3rd party software to jury rig them.

# The Devices



So, we have our data. We have it formatted. We have applications in the cloud and virtualized ready to be accessed. We have a strong network backbone, solid firewalls, certificates, SSL, and VPN at the ready. The stage has been set. And we are now almost ready for BYOD. There is just one more thing... (sorry, I couldn't resist). What about the end user devices!

# Governance



Here is where it gets a little touchy with IT folk. We cannot take total control over an end user's machine. Aside from any legal or ethical issues, doing so would completely defeat the purpose of what we have done up to now anyway. But if we cannot fully control and manage it, what do we do? This is where the concept of "governance" comes into play. Governance is the idea of "controlling by not controlling" (a very Zen-like concept). If you think about it, we don't really need to have control over the device, because we have control over the data. Over our systems. They aren't coming in and sitting down at our restaurant where we control the entire environment. We simply control what they have access to and make sure their system can't do anything to harm us. So, what is involved? Well, first, we need to come up with an end user agreement. Essentially, this is our SLA with the user. It doesn't specify what they can and cannot do with their computer, just what they can and cannot do on our network and to our data. It does not grant us control over their device, but sets requirements that the device must meet in order to gain access to our systems (compliance), and gives us the ability to remove that device from our network should it ever fall out of compliance. And, it defines what IT is responsible for and what it is not. Part of the benefit of allowing BYOD is that: they are not our devices! Your hard drive breaks, it is on you to fix. IT is responsible for our data, and our systems, and our network. If you are having a problem with one of our applications, call help desk. If you are having a problem with your computer, call your manufacturer. Now this is a bit of a change, and obviously your policy must be tailored to your environment. But this allows for IT to focus on what it is good at. I am an Apple Certified Mac Technician, I can repair any Apple computer at my company. Most places don't have ACMTs on site, or Dell techs, or IBM techs. Nor should you have to. Your company will never be able to repair those machines as well or as efficiently as their manufacturers can. Your IT department should be focused on your data, your applications, your network, a.k.a. The things you are there to focus on that those companies cannot fix for you.

# Device Management



On the technical side, you will need a combination of Profile Management for mobile devices and Macs, and group policy for Windows machines.

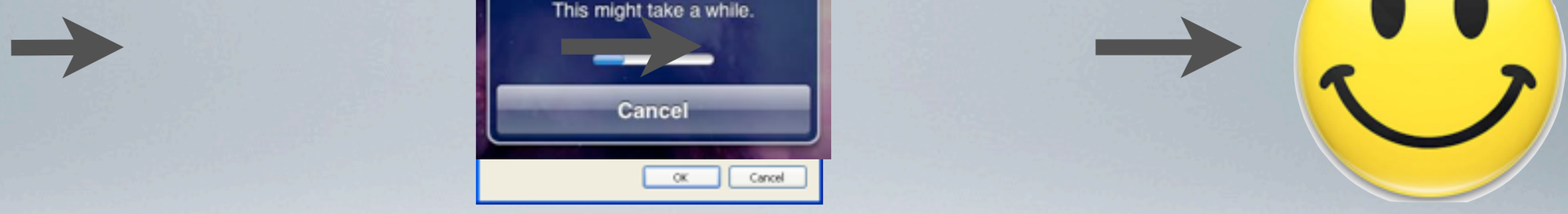
# Device Management

## Group Policy

## Profile Management



If you have never had the opportunity to look at Apple Configurator or Profile Manager built into OS X Server, take a look. They are pretty powerful, and they are designed for BYOD environments. You can see that most of their settings are not invasive. They don't take control away from users, but rather apply settings and configurations that augment the user experience and setup any special settings, such as VPN configs, automatically. The user has the ability to remove these profiles at any time... And so does IT. A balanced approach. That is governance in a nutshell.






So what does this all look like to an end user? Well, let's take a look at it from their perspective. A new user can come in with their own computer, sit down at their desk, and plug it into our network. They only have access to the internet at the moment. They open their browser and are prompted to log into a website using their AD credentials. The system verifies that their device meets the criteria we set, it deploys policy and/or profiles to that device, auto configures their system to access our internal systems, pushes down any applications and bookmarks needed, and the user is now ready to work.

# MDM

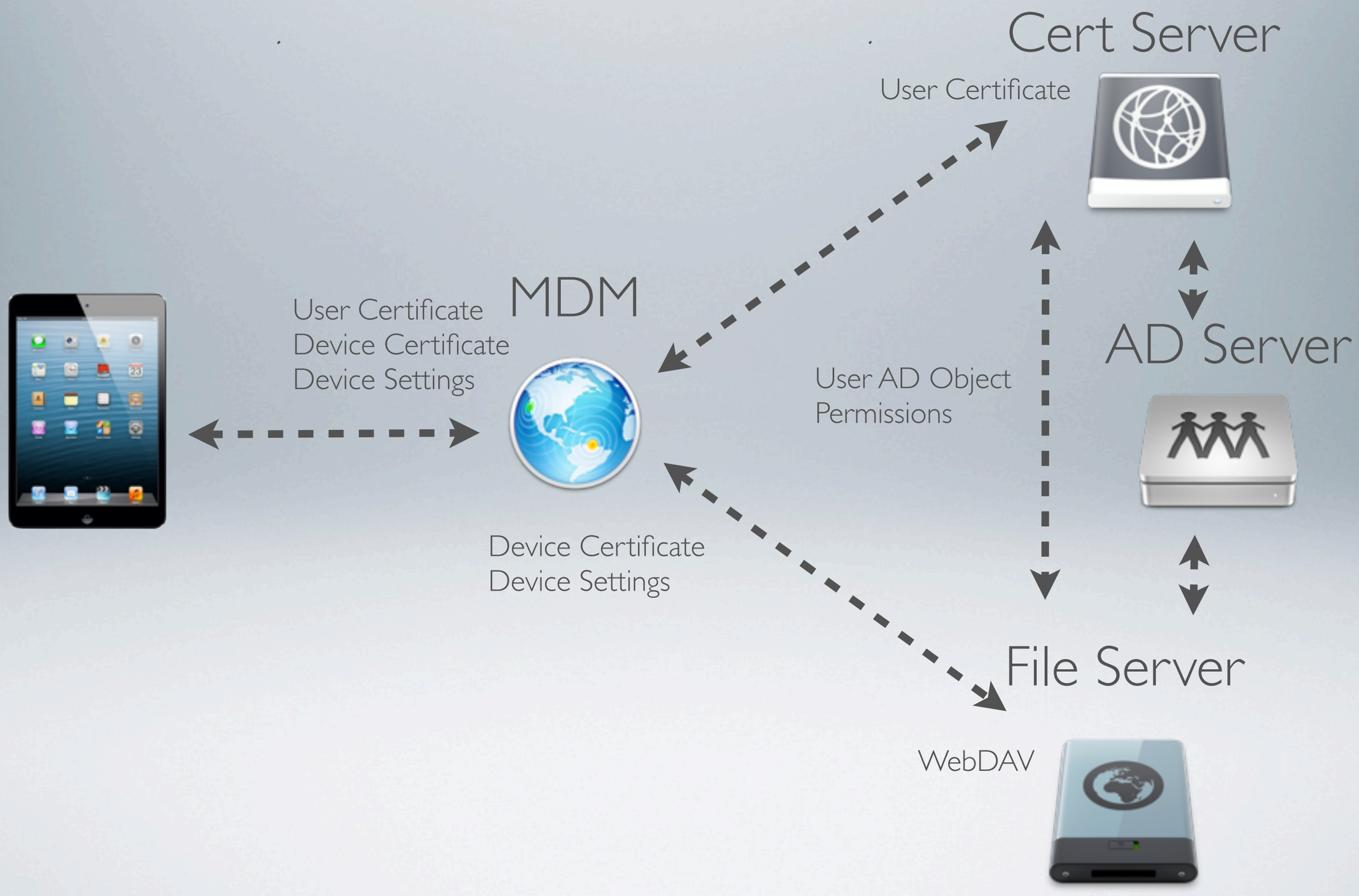


Now, you may ask, how does this all work? You ma also have a Windows admin saying “umm, I am not allowing any of these devices because they don’t work on active directory and group policy”. And you can confidently turn to them and say, “Well, as a matter of fact they do!” An MDM is a great solution, but it is only part of the solution for end user management. But, how can you use group policy and AD permissions on devices that don’t support binding to AD?

Certificates



The answer: Certificates.




Wednesday, May 22, 13

Certificates are the the future. Certificates is the word, the concept you should memorize, learn, master, love... Certificates are how it is all done. Now, how do they work? Well, ideally, what you want to do is this: use a certificate to spin up: an Microsoft Certificate Server. This a free, yes I said free (if you have a Microsoft license), server that you can spin up that will act as a certificate authority for your site. Now, you can use a certificate from an actual CA first, which is fine. But, even without that, you can spin up a CA for your company. What does this give you? If you have that CA, you can generate a certificate for each AD User and for each device... So, when a user downloads the profile from your MDM, they are also getting their certificate. What can this certificate do? Well, VPN works with them. File Shares work with them. Web shares (which is how iOS devices access files) work with them. And, guess what, group policy works with them! You can grant access to all of your systems, control who has access to what, all using certificates! No more manual logging in, no more password reset and AD account locking nightmares! Certificates are your friend. Certificates are the future! Use them!

# BYOD



All of the steps I have talked about, all of the work and configuration is being done to attain one ultimate goal: “the abstraction of data from the device” If you were to follow everything I just talked about, your IT department and infrastructure would be fully prepared for the BYOD revolution. However, it does not mean that you have to implement BYOD. And that is why I said at the beginning of all of this: “BYOD is not the end goal, but an inevitable conclusion”. You could do all of this and still continue to provide machines to all of your employees. You could do what most companies do and offer a choice. Either way, the process is now the same. No more complex and time-consuming imaging. No more 500 group policies. No more user complaints about not being able to get to YouTube or listen to iTunes. The flexibility is there. The security is there, the infrastructure is there. BYOD is only a natural extension of your layout. But, no matter what you choose to do, the device is largely irrelevant.

# LOBSTER SHACK IT



With lobster shack IT, your systems, your network, and most importantly, your data, is under control.

Thank you.