The Network and The Cloud: Addressing Security And Performance

How Your Enterprise is Impacted Today and Tomorrow

UNITEDLAYER

Hybrid Hosting Experts

THE CLOUD: SECURED OR NOT?

IN A STUDY BY MICROSOFT, 51 percent of companies who moved to the cloud said that since moving to the cloud they spent less time managing IT overall, 50 percent said they used fewer internal IT resources, and 43 percent said they wished they had moved to the cloud earlier.

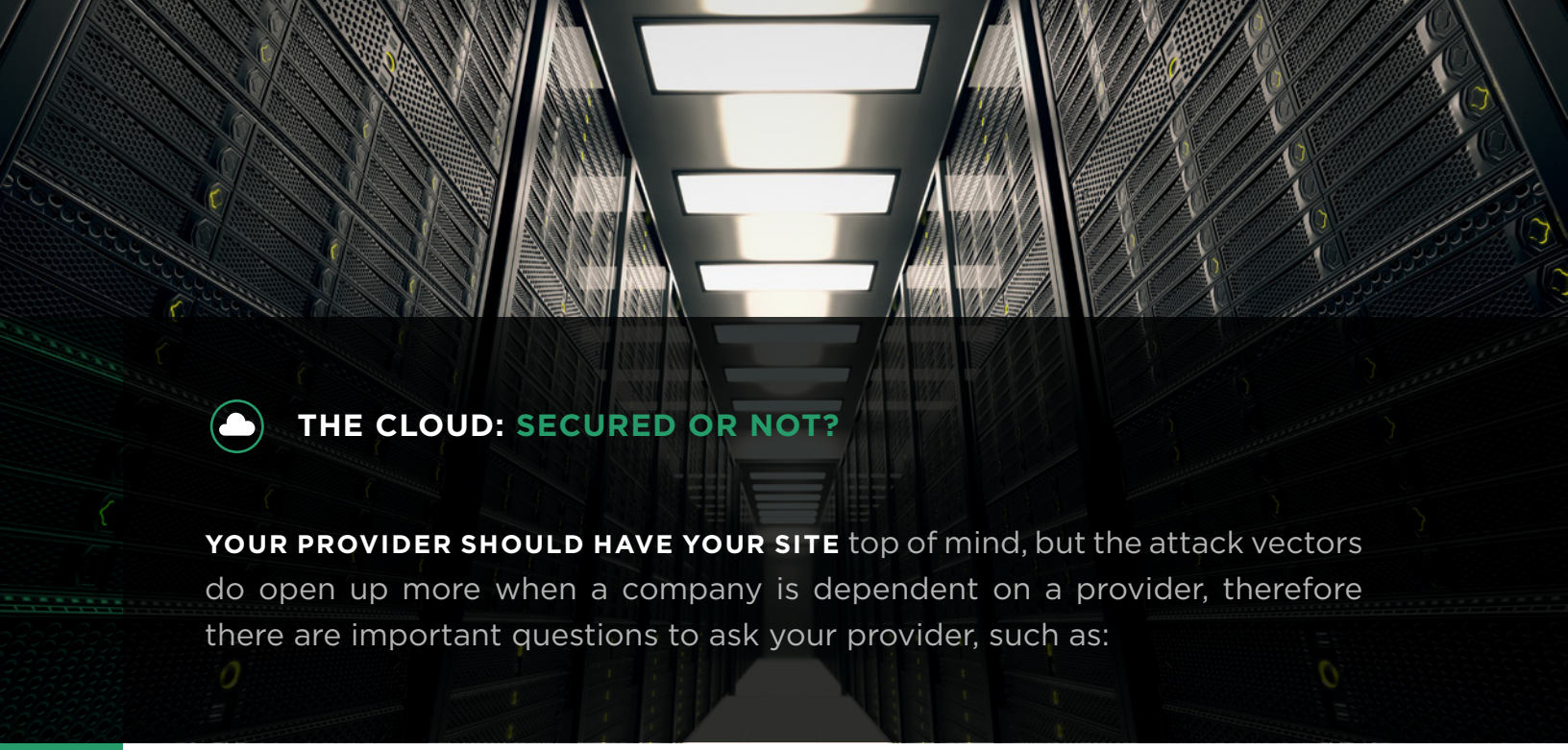
OF THE COMPANIES NOT currently using the cloud, 60 percent cited concerns around data security as an inhibitor to adoption. Of the adopters, 94 percent experienced security benefits in the cloud that they didn't previously have with their on premises service.

Security is the biggest concern – but also the greatest benefit of moving to the cloud.

For an organization considering moving to managed services or cloud based services, they rely on their provider for security.

WHILE YOU MIGHT BE at the mercy of your hosting provider, there are several things that you need to know to ask to ensure that you are properly secure.

Many enterprises may think about firewall security, application security, IDS (Intrusion Detection System) and IPS (Intrusion Prevention System), but there are things that happen physically that many companies aren't aware of – nor are they aware to ask. Issues like attestation of hardware, identifying a tampered compiler or knowing if your provider is using sniffing technology to identify any problems with your infrastructure.



THE CLOUD: SECURED OR NOT?

YOUR PROVIDER SHOULD HAVE YOUR SITE top of mind, but the attack vectors do open up more when a company is dependent on a provider, therefore there are important questions to ask your provider, such as:

1. **SECURITY POLICIES AND PROCEDURES** – What policies and procedures are in place? IPS, firewalls and compliance. What is their security infrastructure of their network like? What kind of technology do they use for security? Do they do continuous traffic monitoring, daily malware scans and protection such as denial-of-service mitigation?

2. **LAYERS** – Do they have several layers of protection and who has access to the application layer where your desktops run? Do the security policies apply for every layer?

3. **STORAGE** - How much storage do you currently have? Is there room to expand and grow?

4. **FREQUENCY OF UPDATES** – How often do they execute software updates?

5. **VIRTUAL MACHINES** – Does your system support virtual machines and what software is under virtual machine?

IMPROVING NETWORK PERFORMANCE

When working with your hosting provider to improve your network performance, **THE FIRST THING TO DO IS IDENTIFY WHAT PERFORMANCE MEANS TO YOUR ENTERPRISE.**

Is it:

1. Getting your application seen by as many people as possible?

2. Distributing it in a local geographic area? Will it stay on this continent?

3. Distributing it globally? Do you have two internal teams working in different countries who need access to the same information simultaneously?

A common challenge when distributing applications is the right synchronization point. If your enterprise has a team in Seattle and a team in India, where is the right synchronization point to ensure simultaneous updates?

The user's proximity to the web server has an impact on response times. If you are deploying your content across multiple geographical areas, a content delivery network (CDN) allows a collection of web servers to be distributed across multiple locations to deliver content more efficiently to users.

The server selected for delivering content to a specific user is typically based on a measure of network proximity.

This will allow for simultaneous update of information for both geographically disparate teams. If your team is on the same continent, it makes sense to have the server on the same continent as you are.

IMPROVING NETWORK PERFORMANCE

WHAT SHOULD YOU ASK YOUR PROVIDER TO ENSURE THAT YOU ARE PROVIDING THE BEST USER-EXPERIENCE FOR YOUR INTERNAL AND EXTERNAL TEAMS?

1. CAN YOUR APPLICATIONS BE VIRTUALIZED? – Do you have any legacy apps that can't be easily moved to the cloud? What apps can you virtualize to improve performance?

2. CAN THEY BE DISTRIBUTED? – Can your applications run on multiple computers within a network?

3. WHAT IS YOUR SINGLE-POINT OF WRITE ACCESS VS. READ ACCESS? – Are you set-up to provide a seamless experience for all members of your teams?

HOW DO YOU MANAGE SECURITY FOR NETWORKS?

MANAGING SECURITY FOR YOUR NETWORKS is a multi-faceted task. If your customers rely on you for their connectivity, not only are you protecting your own infrastructure against the global internet, without intentionally doing so, you may be also acting as a service provider. In this instance, you don't want to necessarily block traffic, rather provide a safe, open access internet for your customers.

Hosting Providers Must Understand Customer's Infrastructure

It's important that a hosting provider spends time understanding its customers' current infrastructure security and its needs. Also ensuring the enterprise is implementing security best practices, so that they contribute to keeping the enterprise free from security breaches. **Important things your provider should be talking to you about are:**

1. IPV6 SECURITY – Have they implemented the same security policies that existed for IPv4? If so, these may not be ideal once the company has moved to an IPv6.

2. ACCESS LISTS – Have you reviewed the permissions that are attached to each system? Do all parties still need access?

3. DENIAL OF SERVICE MITIGATION – Will your business keep running in case of an attack?

4. IDS AND IPS AND FIREWALL – Have you discussed the difference between the three and what is best for your business?

6. PATCHING HABITS – How often do they run security patch updates?

WHAT'S THE FIRST THING THAT PEOPLE SHOULD BE AWARE OF WHEN IT COMES TO NETWORK SECURITY?

It is wrong to assume that a network address translation (NAT) is protecting your infrastructure.

Enterprises generally use a small amount of public space and a great amount of private space. For sites with many hosts, using a NAT can allow them to access the internet through one single IPv4 address. Although a NAT does limit the number of public IP addresses used for economic and security purposes, it shouldn't be relied on as a security measurement; and unfortunately this is a common mistake many companies make.

Companies may rely on NAT for security and as a result, neglect to keep patching up to date. Another common problem is that companies fail to see that they need different security policies with the external facing infrastructure than its internal facing infrastructure. As a result, they rely on the NAT gateway to act as a firewall. This is dangerous.

NAT is an aspect of firewall security, as it conserves the number of public address within an organization and allows stricter control of access of resources on both sides of the firewall – but shouldn't be trusted to secure your infrastructure.

PAYING CLOSE ATTENTION TO BEST CURRENT OPERATIONAL PRACTICES

IT IS COMMON FOR ENTERPRISES to set up one set of standards 2 years ago, 5, or even 10 years ago and not have a review process in place to identify if they have the right hardware, software, patches and policies in place to keep their enterprise secure. It is important to review your security policies and procedures regularly to ensure that they are still in line with your operations.

Security Review Best Practices

1. CREATE USAGE POLICY STATEMENTS – Outline the users' roles and responsibilities in regards to security.

2. CREATE RISK ANALYSIS – Identify any risks of the network, network resources and data.

3. ESTABLISH A SECURITY TEAM STRUCTURE – Form a strong team of key stakeholders with the responsibility of reviewing and updating practices regularly.

4. PREVENTION – REVIEW SECURITY CHANGES – Regularly review any changes to the network equipment that have a possible impact on overall security of network. Changes include:

— Changes to firewall configuration

— Changes to access to control lists

— Changes to simple network management protocol (SNMP)

— Update in software that differs from approved software revision level list

UNFORTUNATELY THERE ARE common mistakes made by enterprises that can be easily mitigated. Ensure that you follow your best practices all year round, regardless of when your security review is, to ensure that you take the steps to avoid an internal/security breach.

Tips to Implement Year-Round

1. Change passwords to network devices on a routine basis.

2. Restrict access to network devices to an approved list of personnel.

3. Ensure that the current software re-vision levels of network equipment and server environments are in compliance with the security configuration requirements.

4. Review internal threats and physical security - Walk up Wi-Fi, port internal infrastructure guest vs. employee.

5. Review BYOD (Bring your own devices) policies and security.

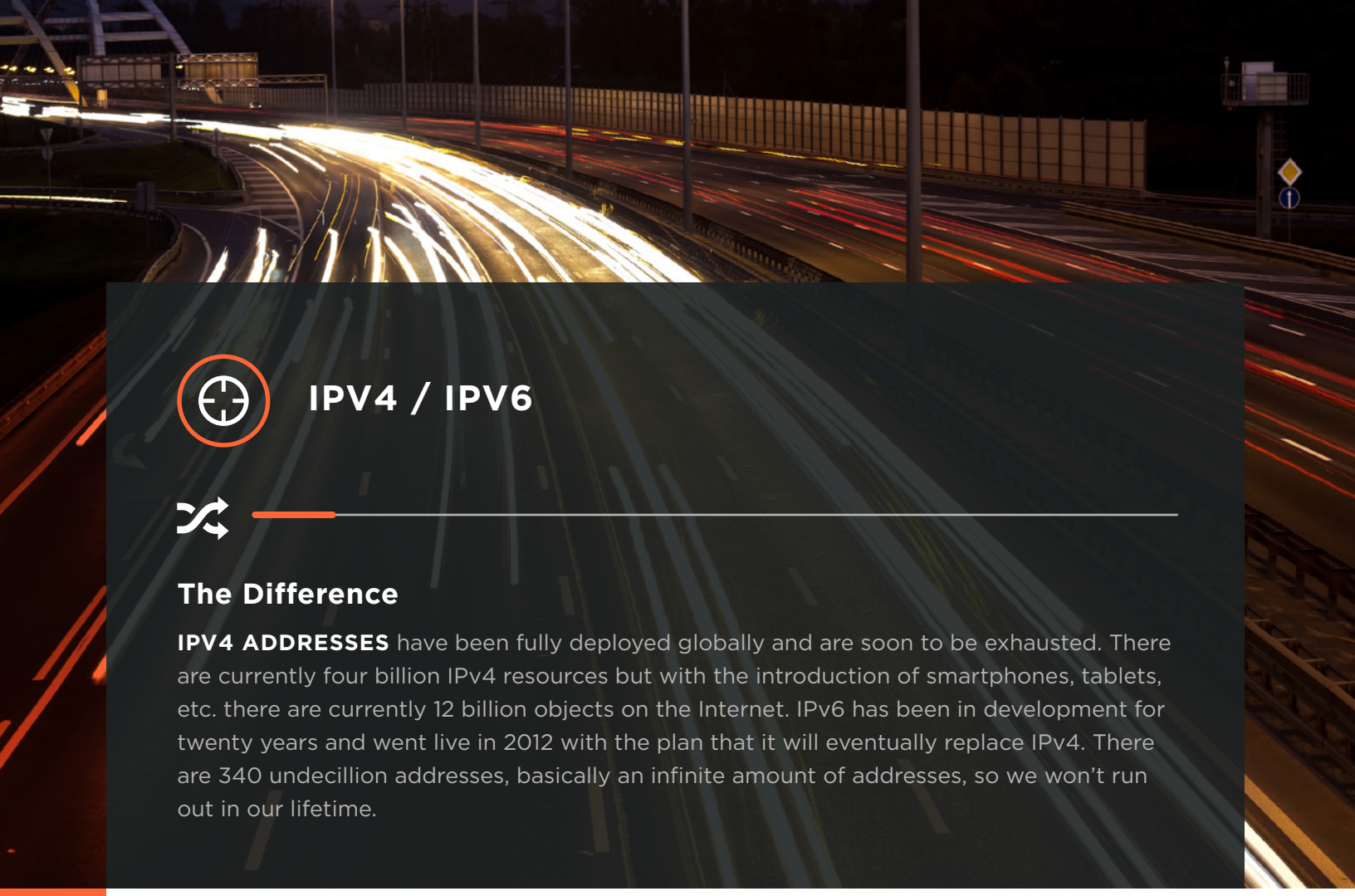
HOW SHOULD A COMPANY DEAL WITH BYOD AS IT PERTAINS TO MANAGING NETWORK SECURITY?

IT'S NOW QUITE COMMON for organizations to allow their employees to bring their own devices to their jobs, rather than purchasing devices for all of their employees. If your organization has BYOD (Bring your own device), security is going to be a risk. With the multitude of different devices, services and apps currently out there, it is hard for IT to manage and control the mix of apps, services and device types. It is also challenging to find ways to ensure the security on all the device types. If you have BYOD, the best thing to do is to separate your infrastructure from these devices. As a network administrator you can support the ability to connect to these devices for mail calendar but you have to treat them as they are not part of your infrastructure in order to protect your enterprise. These devices should be treated like they aren't part of your internal infrastructure and treated as though they are going to hurt your infrastructure and only allow the services that are mandatory.

IF YOU WANT TO HAVE more control and security is a concern, your organization may want to implement COPE (Corporate owned personally enabled), where an organization provides its employees with mobile computing devices and allows the employees to use them as if they were personally-owned.

WHAT APPLICATIONS ARE SUSCEPTIBLE TO NETWORK ATTACKS?

THE RULE OF THUMB is simply, whatever is being used the most is going to be attacked the most. For example, for the past ten years Windows has been the dominate player and as such, has endured the majority of the attacks to its operating system, over that of MacOS. People made the assumption that it was due to the fact that MacOS was safer, but that wasn't entirely true. There were more people on the Windows OS, so hackers targeted that system – simply because it was being used more. The attack vector changes over time, now with the increase in iOS phones, Windows and Android phones, the targets have changed. The fact of the matter is, nothing is safe – the hackers will always have a target. All we can do is look at the anomalies and understand.



IPV4 / IPV6

The Difference

IPV4 ADDRESSES have been fully deployed globally and are soon to be exhausted. There are currently four billion IPv4 resources but with the introduction of smartphones, tablets, etc. there are currently 12 billion objects on the Internet. IPv6 has been in development for twenty years and went live in 2012 with the plan that it will eventually replace IPv4. There are 340 undecillion addresses, basically an infinite amount of addresses, so we won't run out in our lifetime.

Security – What We Need To Know

IPV6 WILL BRING more numerical addresses as well as simplify address assignments, eliminate the need for NAT (Network Address Translation), allow auto-configuration and prevent private address collisions. Additional network security features include:

- Simplified, more efficient routing
- True quality of service (QoS), also called "flow labeling"
- Built-in authentication and privacy support
- Flexible options and extensions
- Easier administration (say good-bye to DHCP)
- Authenticity of each IPv6 packet is ensured through encryption
- Better at ensuring internet traffic gets to correct destination without being intercepted.

Options for Enterprise

PUBLIC FACING services such as websites can't survive on IPv4 only. What organizations don't realize is that without IPv6, parts of the internet aren't going to reach them. For example, in Asia residential users are coming up over IPv6 only and are using gateways to translate IPv6 into IPv4, which means that the performance for your application is going to degrade – something enterprises should be aware of.

Is it urgent to switch over?

ENTERPRISES NEED TO BE aware of IPv6 and make sure that any future PC, device, network infrastructure, or other IT purchases support the next-generation protocol. IPv4 should still be around long enough for most organizations to transition to IPv6 over time.

Why should your enterprise make the switch?

SOFTWARE AND ROUTERS have to be changed to support the more advanced network. Many routers and servers don't support IPv6 so connection between devices (or a device) with an IPv6 address to a router or server that only supports IPV4 is impossible. It's inevitable that iPv6 will be the only option for new devices or hosts on the internet. Transitioning to IPv6 now, rather than later, is a good idea and will avoid your enterprise having to worry about transitioning later on when IPv4 becomes obsolete.

WHERE IS THE FUTURE TAKING US?

WE WILL CONTINUE to see an increase in virtualization in the future. At budget time, more companies will look at virtualization as a cost savings over adding resources and purchasing expensive infrastructure. In addition, more enterprises will use virtualization to expand their footprint – as cost effectively as possible. We will continue to see the trend of companies moving away from keeping their servers as more companies will put their servers in the hands of their hosting providers.


UNITEDLAYER
Hybrid Hosting Experts
San Francisco Colocation Data Center | 200 Paul Ave Suite 110 (HQ) San Francisco, CA 94124
Los Angeles Colocation Data Center | 530 West 6thStreet, Los Angeles, CA 90014
Las Vegas | Toronto | Virginia | Vancouver
Sales (866) 291-4914 | LA Sales (866) 486-7908 |
Main (866) 395-5346 | Toll Free (888) 853-7733 |
Support/NOC (415) 349-2102 (available 24x7) | Fax (415) 520-5700
sales@unitedlayer.com
SSAE 16
CERTIFIED
TYPE II