RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CXO-R04

THIS IS YOUR ENTERPRISE ON OFFICE 365

Tony Summerlin

Senior Strategic Advisor, FCC

Tony Summerlin

Senior Strategic Advisor, FCC/CIO

Senior Strategic advisor for the **FCC/CIO office of the Managing Director.** Seasoned industry leader with **30 years of security and government consulting experience**

Agenda

A Transformation Journey to Support O365

Outlining what to prepare for in regards to your network/ security architecture, the impact to your teams, and how to set expectations with your business

The Best Approach

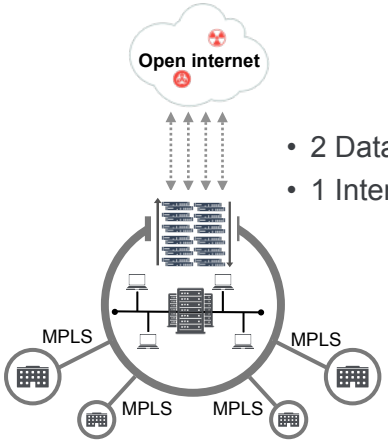
How to best follow Microsoft's guidance on connecting end-users to the Office 365 service and avoid the challenges common to Office 365 deployments within large organizations

Legacy Network & Security Architecture at the FCC

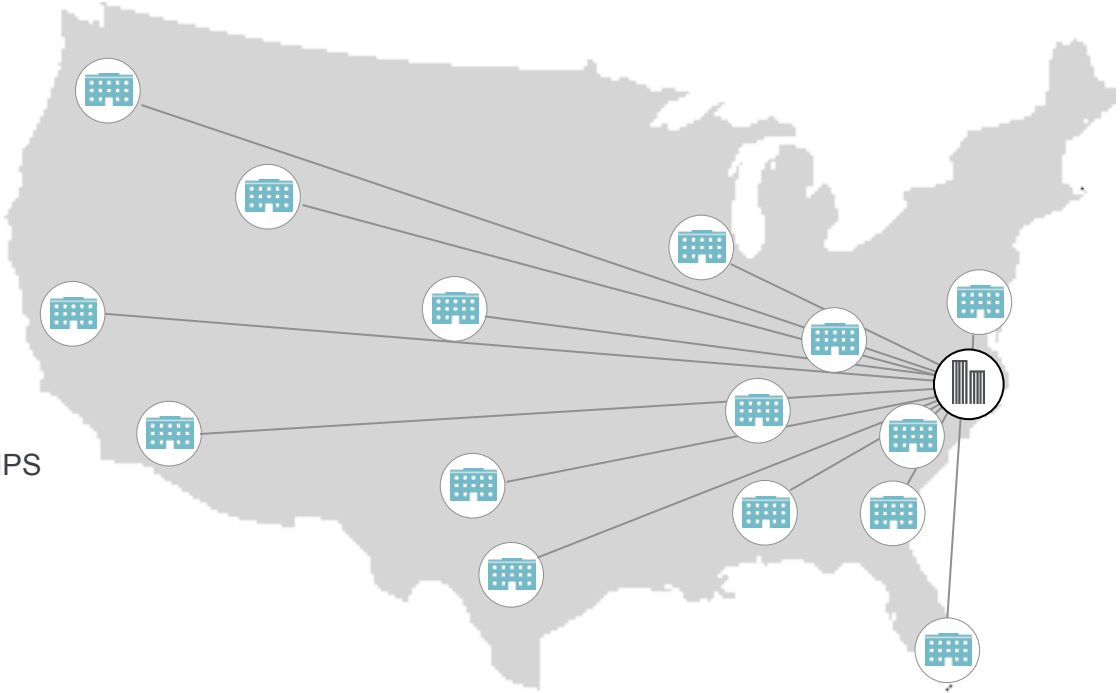
15 Locations

2000 Users

1000 Remote Users with VPN / Mobile Solutions



- 2 Data Centers in DC area
- 1 Internet egress point via MTIPS



The Rush to Move Email to Office 365

A Pending DC Consolidation Did Not Leave Time to Optimize Network & Security Architecture to Support O365

What You Need to Prepare For

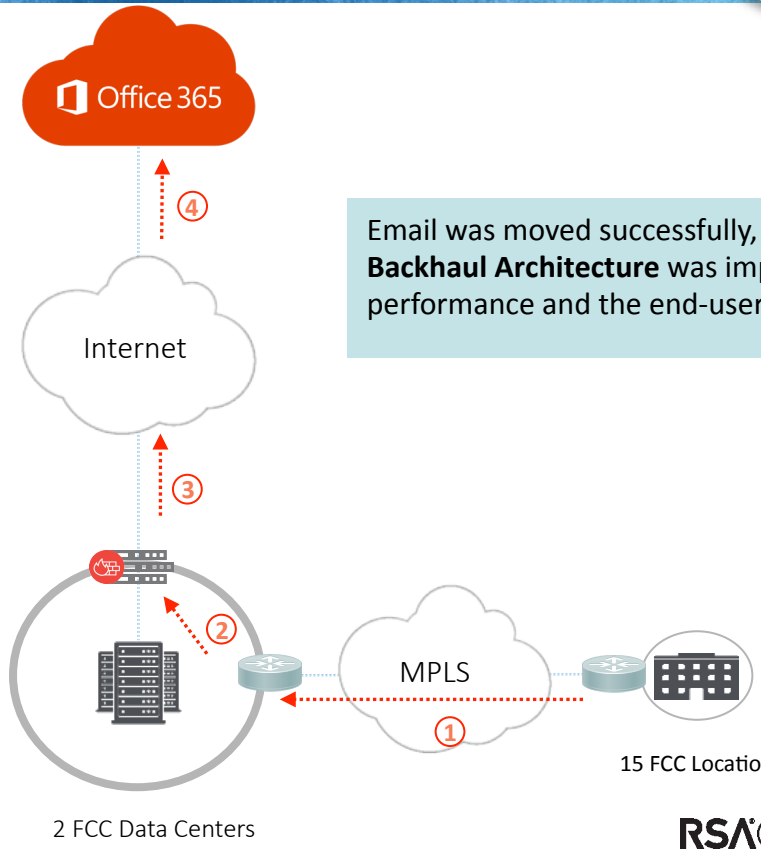
O365 not a normal project
Deployment will impact all users and work streams will overlap multiple IT disciplines

IT Culture Shift
"Office 365" means different things to different people. What apps do you plan on using?

How much bandwidth do you need?
Plan for 40% increase for internet traffic and find an aggregator

What metrics will you use to justify the additional bandwidth?

Session counts on your firewalls and proxies become an issue



Email was moved successfully, but the **Backhaul Architecture** was impacting O365 performance and the end-user experience

Prepare for the Increased Load on Firewalls and Proxies

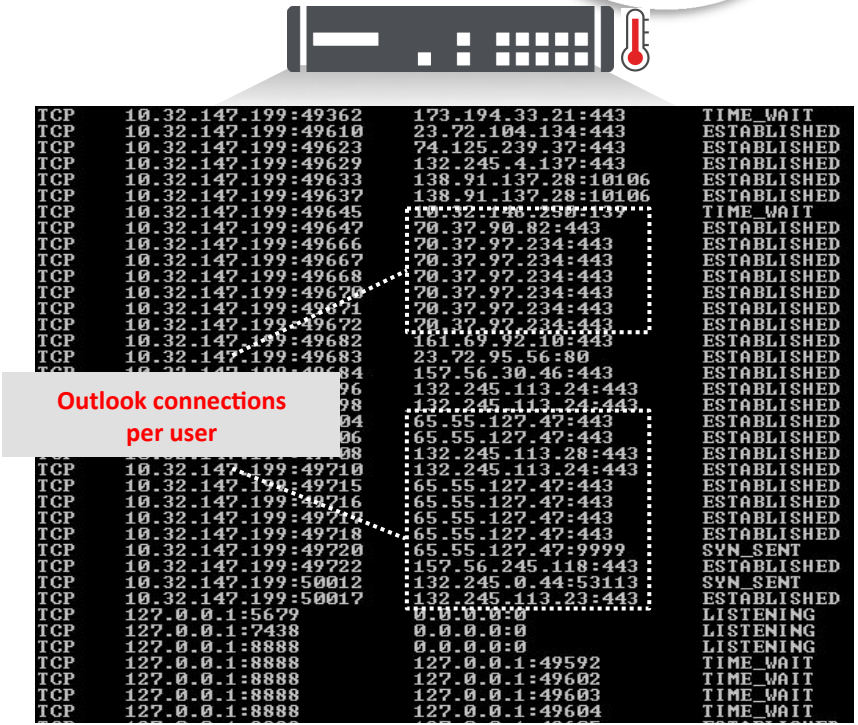
Bandwidth is Not the Only Problem – Session Counts & Non-Browsing Ports

Challenge Legacy Infrastructure

- Office 365 creates a high number of long-lived sessions that quickly exhaust firewall ports (we've seen 12-20 connections per user, per app)
- Around 4,000 clients can be supported by a single public IP safely (may require architectural changes)
- Some Office 365 apps use will require more than Web browsing (ports 80 / 443) – uses ephemeral ports

IMPACT ON THE USER EXPERIENCE

Random hangs and connection issues



TCP	10.32.147.199:49362	173.194.33.21:443	TIME_WAIT
TCP	10.32.147.199:49610	23.72.104.134:443	ESTABLISHED
TCP	10.32.147.199:49623	74.125.239.37:443	ESTABLISHED
TCP	10.32.147.199:49629	132.245.4.137:443	ESTABLISHED
TCP	10.32.147.199:49633	138.91.137.28:10106	ESTABLISHED
TCP	10.32.147.199:49637	138.91.137.28:10106	ESTABLISHED
TCP	10.32.147.199:49645	10.32.140.250:139	TIME_WAIT
TCP	10.32.147.199:49647	70.37.90.82:443	ESTABLISHED
TCP	10.32.147.199:49666	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49667	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49668	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49670	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49671	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49672	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49682	161.69.92.10:443	ESTABLISHED
TCP	10.32.147.199:49683	23.72.95.56:80	ESTABLISHED
TCP	[illegible]	157.56.30.46:443	ESTABLISHED
TCP	[illegible]	132.245.113.24:443	ESTABLISHED
TCP	[illegible]	132.245.113.24:443	ESTABLISHED
TCP	[illegible]	65.55.127.47:443	ESTABLISHED
TCP	[illegible]	65.55.127.47:443	ESTABLISHED
TCP	[illegible]	132.245.113.28:443	ESTABLISHED
TCP	10.32.147.199:49710	132.245.113.24:443	ESTABLISHED
TCP	10.32.147.199:49715	65.55.127.47:443	ESTABLISHED
TCP	10.32.147.199:49716	65.55.127.47:443	ESTABLISHED
TCP	10.32.147.199:49717	65.55.127.47:443	ESTABLISHED
TCP	10.32.147.199:49718	65.55.127.47:443	ESTABLISHED
TCP	10.32.147.199:49720	65.55.127.47:9999	SYN_SENT
TCP	10.32.147.199:49722	157.56.245.118:443	ESTABLISHED
TCP	10.32.147.199:50012	132.245.0.44:53113	SYN_SENT
TCP	10.32.147.199:50017	132.245.113.23:443	ESTABLISHED
TCP	127.0.0.1:5679	0.0.0.0:0	LISTENING
TCP	127.0.0.1:7438	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8888	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8888	127.0.0.1:49592	TIME_WAIT
TCP	127.0.0.1:8888	127.0.0.1:49602	TIME_WAIT
TCP	127.0.0.1:8888	127.0.0.1:49603	TIME_WAIT
TCP	127.0.0.1:8888	127.0.0.1:49604	TIME_WAIT

Internet Breakouts Make a Difference

Visibility, Cost Savings, and Improved Performance

What You Need to Prepare For

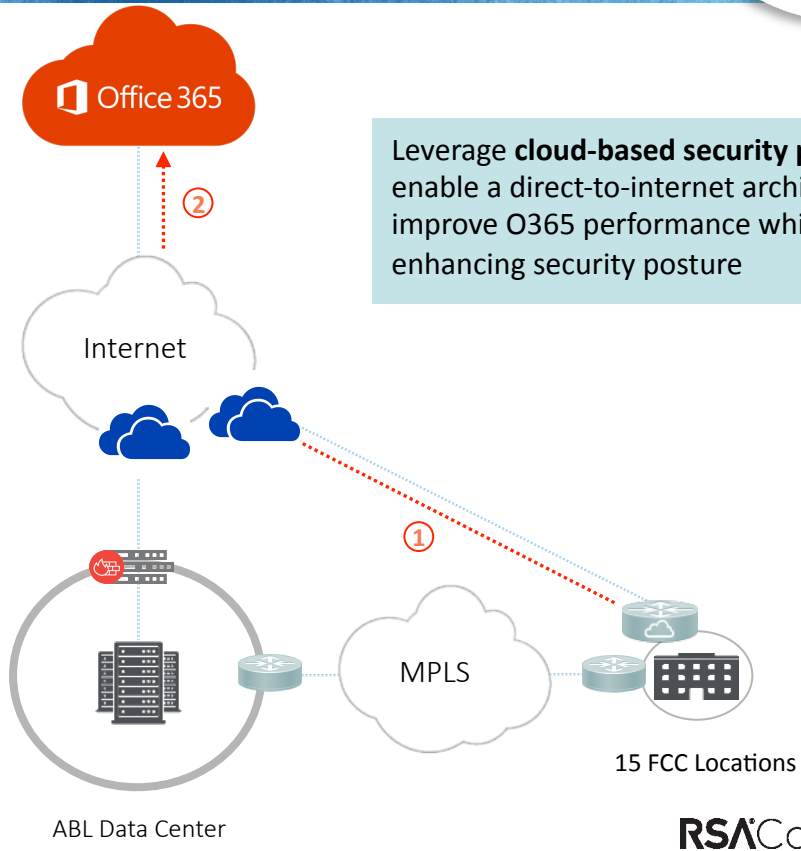
Inconsistent End-User experience: People will compare the experience at home vs. at the office

Fund local internet breakouts with MPLS savings: plan for 60% reduction in the DC

Distributed architecture policies Appliance sprawl is hard to manage and extremely expensive – Use the cloud and find an ISP aggregator

The end user is everywhere: Where are your monitoring tools deployed?

Perception is Everything Have metrics and data points ready to share



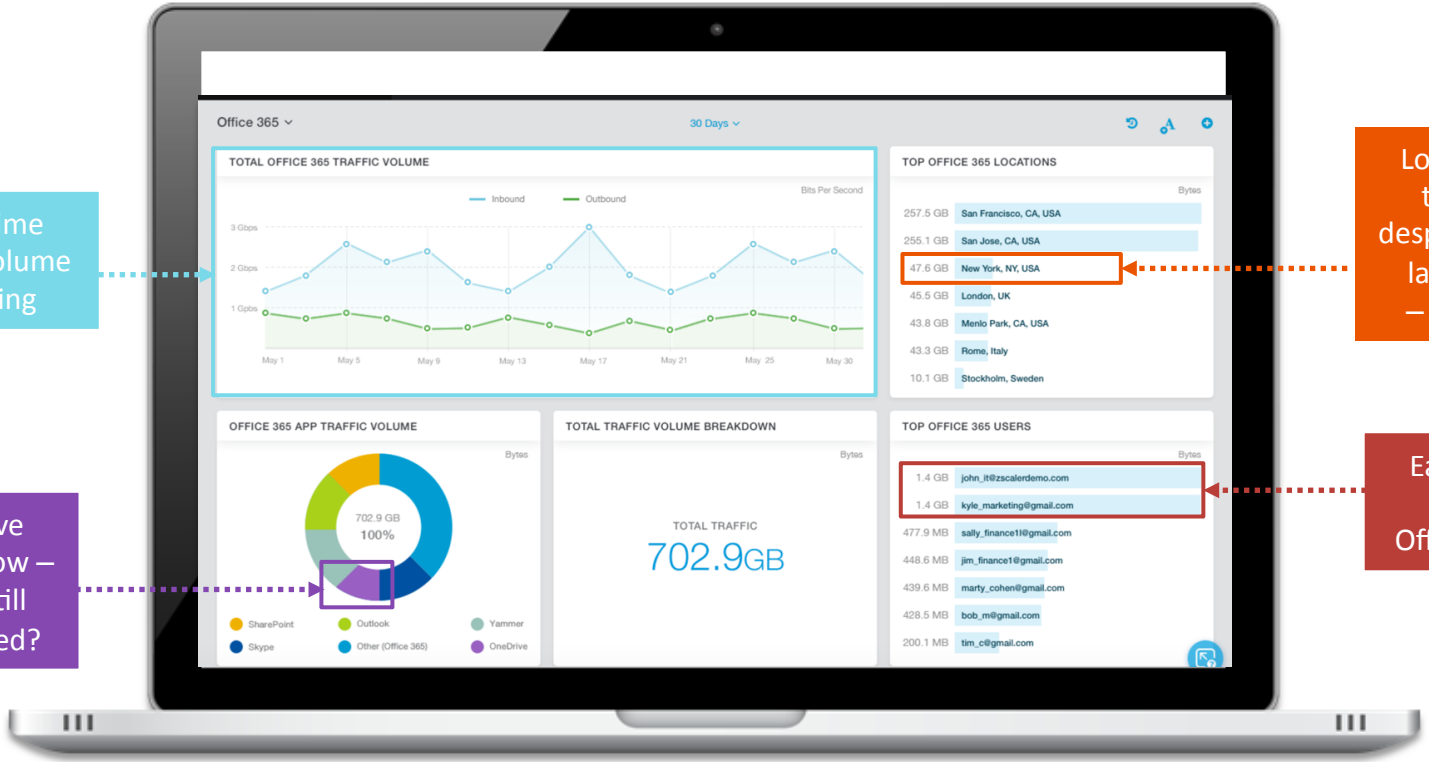
Leverage **cloud-based security platform** to enable a direct-to-internet architecture and improve O365 performance while enhancing security posture

Visibility Into the Deployment Was Crucial

Actionable Data Used for Capacity Planning and to Validate Deployment Assumptions With Project Stakeholders

Real-time traffic volume trending

OneDrive traffic is low – is Box still being used?



Low Office 365 traffic in NY despite one of the largest offices – user issues?

Easily identify the top Office 365 users

Enabling the Business to Fully Leverage All O365 Applications

Optimize Connectivity to Prioritize O365 Applications and Deliver a Consistent End-User Experience

#RSAC

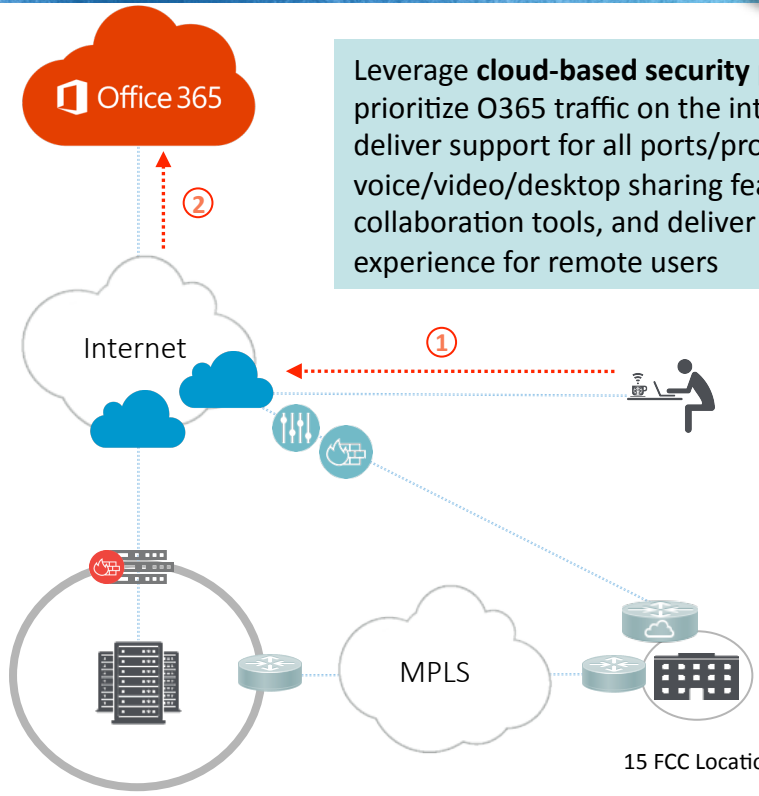
What You Need to Prepare For

Setup a reinvestment model
As you recognize savings, give some back to the business and invest the rest in technology to improve the end-user experience

Drive Business Engagement
Deliver frequent O365 training. Pitch O365 benefits to leaders (collaboration capabilities, less travel, & enhanced productivity)

Support All Ports & Protocols
Understand how to handle traffic outside of standard proxy ports

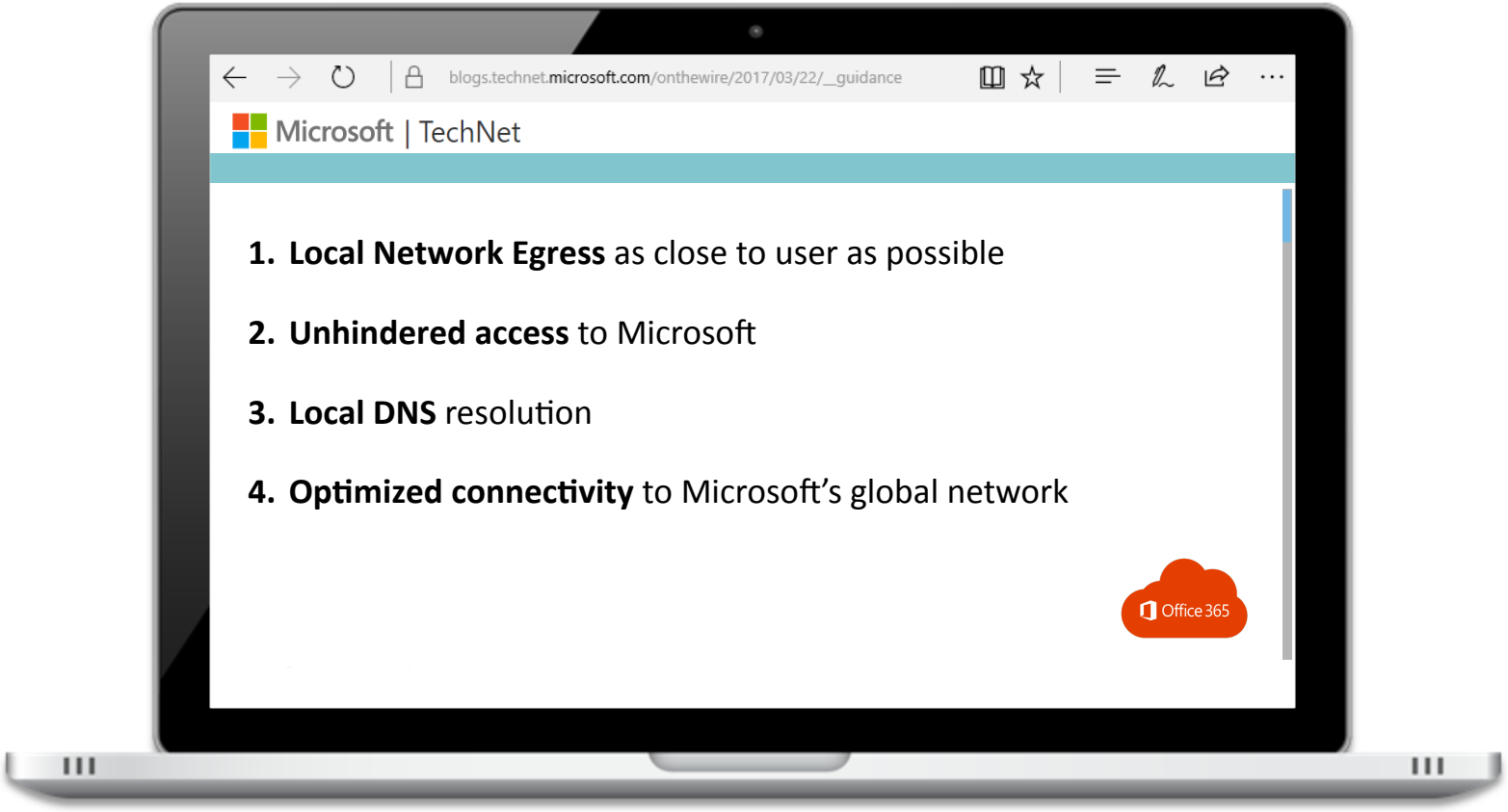
Changing remote access architecture to improve end-user experience.



Leverage **cloud-based security platform** to prioritize O365 traffic on the internet connections, deliver support for all ports/protocol to enable voice/video/desktop sharing features within collaboration tools, and deliver a consistent experience for remote users

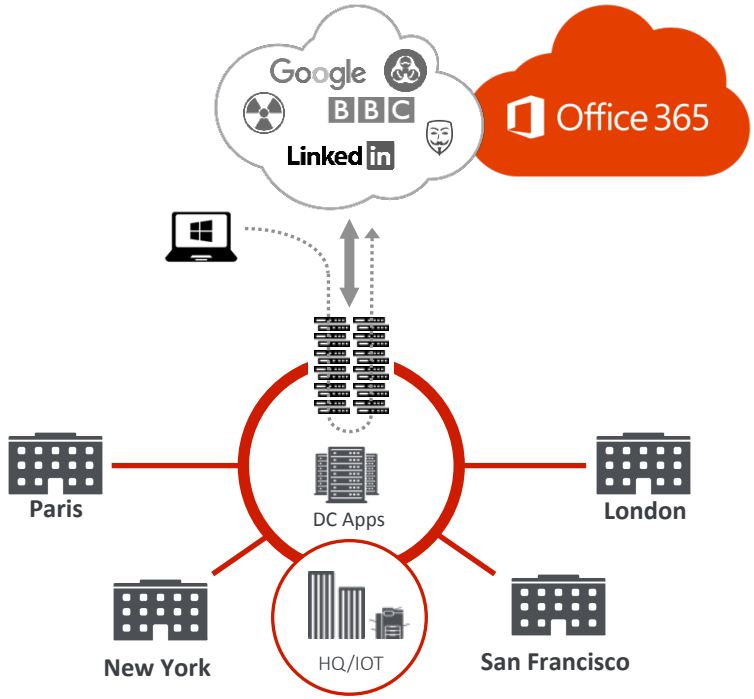
The Best Approach

Follow Microsoft's Guidance - TechNet Blog: https://blogs.technet.microsoft.com/onthewire/2017/03/22/__guidance/



Legacy Hub and Spoke is the WRONG approach

Local Network Egress: Cloud apps need low latency connections



Hub-and-Spoke Network

Microsoft recommends against using a Hub and Spoke network with Office 365

Cloud apps like Skype and Sharepoint are designed for low latency direct access

Hub and Spoke and VPN requirements add unnecessary latency

The user experience for Office 365 is compromised

Backhauling and Security Appliance Sprawl adds extra cost to deployment

Local Network Egress
Unhindered Access

Simplify Office 365 Administration

Unhindered Access: Get Out of Managing an Evolving IP/Domain Whitelist

#RSAC

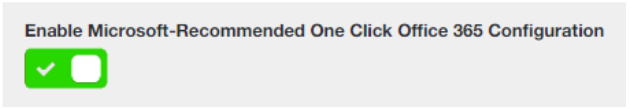
Microsoft

Updates Office 365 connection details multiple times a week

Traditional approach requires **constant firewall updates** to maintain connectivity

.XML update list

One Click Configuration



Easily maintains updates without day to day Office 365 administration

Fingerprints all Office 365 applications

No more keeping up with URL and IP changes in the Office 365 applications.

Automatically configures white list

Exempts Office 365 traffic from authentication and SSL decryption, as recommended by Microsoft.

Minimize Office 365 latency with Local DNS

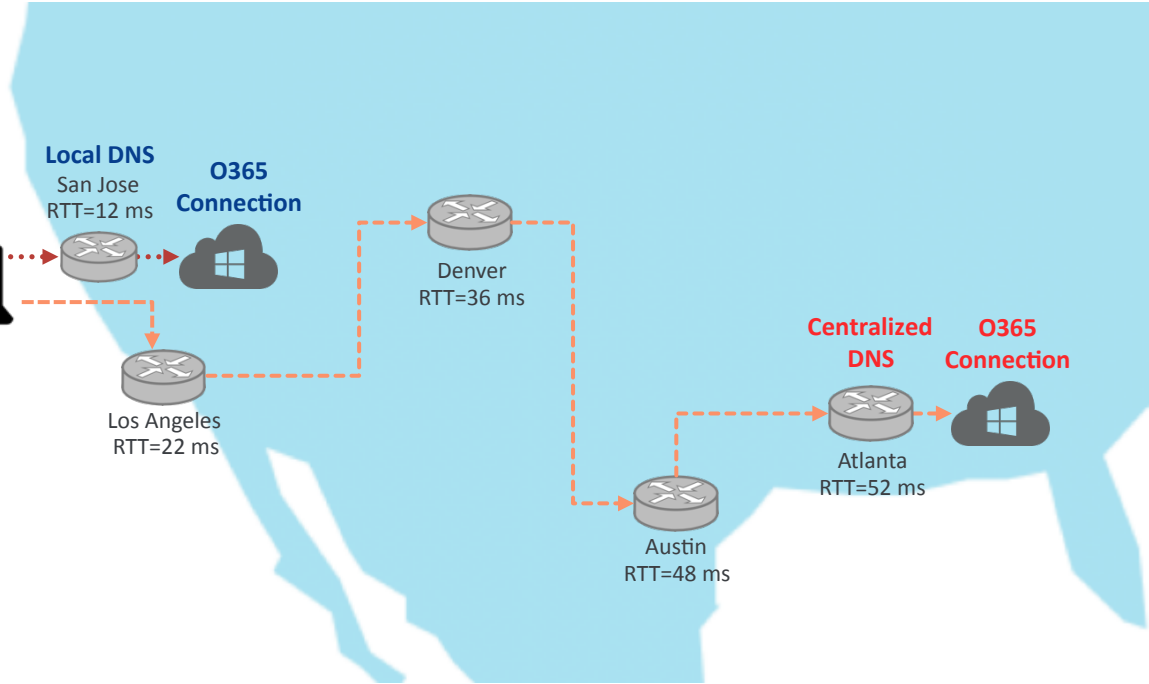
Guarantee a fast, local connection regardless of location

Local DNS Architecture

San Francisco User > San Francisco DNS > San Jose O365

Shortest path, fewer hops = faster user experience

Latency: 12ms



Common Centralized DNS Architecture

San Jose user > LA > Denver > Austin > Atlanta O365

Lots of hops increases: slower user experience

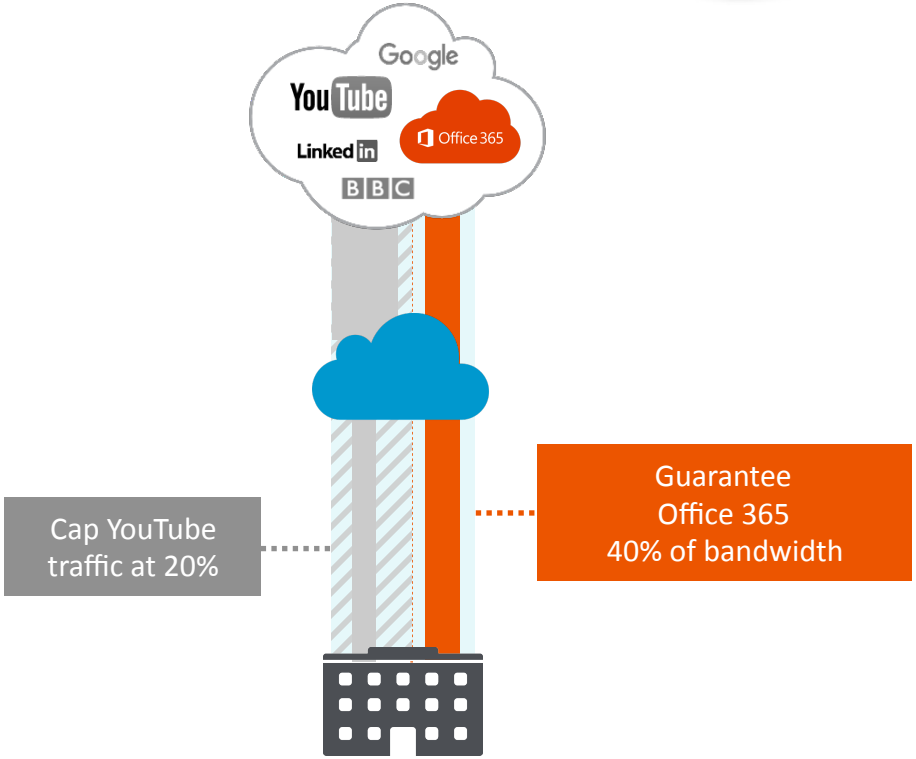
Latency: 158ms *(22ms+36ms+48ms+52ms)*

Optimize Connectivity with Bandwidth Control

Prioritize Office 365 Over Other Apps on Local Internet Connections

Enforce policies in the cloud,
before the last mile bottleneck

Window shaping and bandwidth throttling
will deliver a smooth user experience



Direct-To-Internet Architecture Leveraging a Cloud-Based Security Platform for Access to Office 365: Five Reasons Why

1. Follows Microsoft recommended deployment model
2. Best possible user experience (closer to the internet, fast response times)
3. Rapid deployment (no hardware deployments or upgrades)
4. Investment protection and cost avoidance (no hardware or backhaul)
5. Visibility into all Internet traffic within seconds (single console)

Start Your Cloud Journey Right

Build a **Future Proof and scalable** network and security Infrastructure that delivers a **consistent user experience across all apps**, regardless of location

Start your Cloud Journey Right

O365 is probably your first step to the cloud. Do it right so your company will want more, and have an app strategy that focuses on end-user experience

Challenge the Status Quo

Transforming your architecture to leverage both cloud-based and internal apps will force IT organizations to collaborate in new ways