zscaler™

Four secrets to a successful Office 365 deployment

There's no denying that Office 365 is a big deal. It's a big part of the Microsoft Intelligent Cloud strategy. It's big in terms of its user base. And it has a big impact on your network. Fully deployed, Office 365 will quickly become your greatest consumer of bandwidth and slayer of firewalls.

Office 365 is unlike any other SaaS app and, even with careful planning, it's fair to say that deployment doesn't always go without a hitch. But there are some secrets that will put you on the road to success. They've been widely discussed—not least of all by Microsoft—so they're not exactly classified material. Even so, many organizations are still struggling with questions about the proper network setup for Office 365, so we're outlining four of the best ways to ensure a successful deployment. Here's the scoop.

SECRET #1

ABANDON THE IDEA THAT YOUR EXISTING NETWORK IS UP TO THE TASK

Most larger companies rely on a hub-and-spoke network to route traffic from branch offices through a central data center where applications are housed and security controls are applied. If you're also running apps on Azure, you may have set up ExpressRoute connections to those workloads. So, it's reasonable to think that you could use those same pipes for Office 365, right? Think again. You're about take a huge application and its data and move it to cloud. It's time to think differently about your data and your network.

What does Microsoft say?

Microsoft has written much on the topic of Office 365 connectivity. We've summed up the core principles here, but if you want a deeper dive, the Microsoft **support site** and this **blog** examine the details. In regard to networking and Office 365, Microsoft's core recommendation for the best performance is based on the use of "local egress," instead of backhauling traffic to a central gateway:

Regarding hub-and-spoke networks:

"When compared to backhauling data across the corporate WAN, the user is most likely going to get better performance by egressing Office 365 network traffic to the Internet close to their location where it can be connected to Microsoft's global network."

What does Zscaler™ recommend?

We recommend establishing a local network egress as close as possible to the user. Also known as "direct-to-internet," this approach minimizes latency on user traffic. Latency is the enemy of Office 365, and the quicker you can get your user traffic to a Microsoft data center, the better.

Get to know your latency

Know the latency users experience when getting to the internet—on your network, over VPN, and from your branch offices. The round-trip time (RTT) should be less than 250ms, with Exchange requiring less than 50ms and SharePoint Online less than 25ms. Anything above these numbers is a deal breaker.

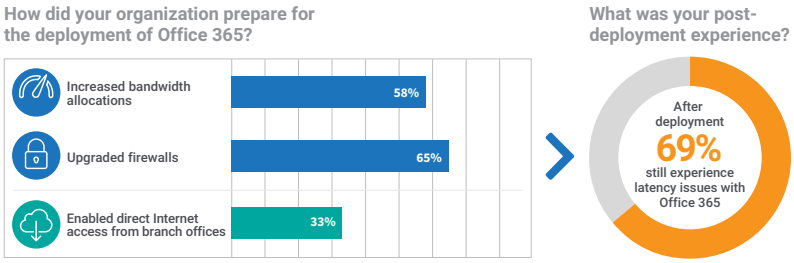
Embrace your new network

When it comes to Office 365, the internet is the de facto network. Companies with successful deployments are using local internet breakouts at branch offices, which gets Office 365 traffic to Microsoft as quickly as possible and avoids the latency added when traveling through older hub-and-spoke networks.

SECRET #2

DON'T COUNT ON YOUR EXISTING GATEWAY TO HANDLE OFFICE 365 TRAFFIC

You've probably invested a great deal in your gateway, so it's perfectly natural to turn your focus to the gateway when the Office 365 project hits your plate. It's possible you've been able to do just that with other SaaS projects: you scope out your gateway, plan for added bandwidth, and upgrade appliances as needed. The problem is that Office 365 is unlike any other SaaS application you've dealt with in the past. It will lay waste to even the best-planned gateway upgrades. In a recent survey,[1] 250 enterprises were asked about their post-deployment experience, and their responses reflect this reality.



While a third of the survey respondents enabled direct internet access from their branch offices, the majority focused on the traditional approaches of bandwidth management and appliance upgrades. It's no surprise, then, that a similar percentage of those respondents also reported latency problems post deployment.

What does Microsoft say?

In its blog on connectivity guidance for Office 365, Microsoft highlights a key problem of the centralized gateway approach with security appliances:

"Unfortunately, whilst all this equipment reduces the enterprise risk of Internet connectivity, it also increases the cost and resources required for Internet connectivity, and it reduces the performance for network connections."

What does Zscaler recommend?

Because Office 365 opens an unusually high number of long-lived sessions, you will want to avoid exhausting the resources of your existing gateway appliances.

Embrace local internet breakouts

Instead of overloading your existing gateway, or taking on the added cost of upgrading your appliances, you should look to the local internet breakout. By breaking out Office 365 at the branch level, you can extend the life of your existing gateway appliances and avoid Office 365 performance headaches.

Deliver security without breaking the bank

Many think that local internet breakouts will be more expensive, as they require the installation of appliances at every branch in order to deliver security. By embracing a security-as-a-service approach, you can deliver both the security required for your internet-bound traffic and the user performance needed for your Office 365 connections.

[1] TechValidate and Zscaler. "Challenges with Office 365 Deployment" Survey. Q1 2017.

SECRET #3

GET YOUR USERS AS CLOSE TO OFFICE 365 AS YOU CAN

To get the very best Office 365 performance—and the happiest Office 365 users—you need to connect to Microsoft as quickly as possible. Since we know that local internet breakouts help you accomplish that goal, you should now train your focus on the last leg of your Office 365 connection. This is where a lot of companies falter, because they don't handle DNS locally, too, which results in unnecessary latency. If you provide Microsoft with DNS information for your headquarters in San Jose, your Office 365 traffic will be routed through the Microsoft Office 365 data center in San Jose, even for your users in the St. Louis branch.

What does Microsoft say?

Microsoft has a robust global network in which to provide Office 365 services like Skype, SharePoint, and Exchange. Care should be put into planning the internet portion of the journey once it breaks out of your network.

"Many Office 365 applications use DNS requests to determine the user's geographic location. If a user's DNS lookups are not done at the same point as the network egress, the user may be directed to a distant Office 365 front-end server."

What does Zscaler recommend?

There are some key areas that can make your Office 365 deployment a success, and they have a lot to do with making sure you have the quickest connection possible to Microsoft.

Think through your DNS strategy

As your traffic breaks out to the internet from your branches, you will want it to resolve to a DNS that is closest to your users. By leveraging a DNS infrastructure that is always local to a Microsoft Office 365 connection, you can guarantee your traffic won't take unnecessary hops, and you'll reduce latency for consistent user performance no matter where users connect.

Peering with Microsoft is key

You should also focus on ways to peer with the Microsoft global network. By selecting an outbound network connection that peers with Microsoft in multiple data center exchanges, you can get your connection handed off to Microsoft with a minimal 1-2ms hop. Zscaler peers with Microsoft Office 365 in 20 different exchanges globally, which guarantees a fast connection from any location.

SECRET #4

DON'T ASSUME THAT IT'S GOING TO BE A SET-AND-FORGET SERVICE

With all the hardware and services you'll be offloading to Microsoft after your Office 365 migration, you might have the impression that Office 365 will give you some precious time back. But the reality is that managing and maintaining Office 365 can itself be a full-time job.

What does Microsoft say?

Microsoft maintains a **master XML list** of all connection points, known as "Office 365 endpoints." Microsoft makes changes to these endpoints on a regular basis, and will notify you of the change. It is your responsibility to adjust firewalls, proxies or other access control equipment when these changes occur.

"When new endpoints are announced, there is usually a 30+ day buffer before they are effective and network requests begin going to them. This buffer is to ensure customers and partners have an opportunity to update their systems."

What does Zscaler recommend?

Automate URL/IP updates

Staying on top of Office 365 updates on a regular basis, across your entire infrastructure, can be time consuming. In addition, missing an update can cause outage problems. Look for a vendor like Zscaler that can help streamline this process. Zscaler provides a one-click configuration option that automatically updates URL and IP changes for applications in the Office 365 suite without any additional administrator workload.

Remember that your users are everywhere

As users leave your network, be sure you have a good strategy for getting them to Office 365. Forcing them onto the VPN and through your network only to head back out to the cloud and Office 365 is far from efficient. Zscaler offers a great option, as it enables all users, on- or off-network, to connect directly to the internet through the Zscaler cloud platform. With over 100 data centers and peering with Microsoft, every user gets a fast connection to Office 365 as well as a complete security stack, delivered as a service, that protects traffic bound for the open internet.

Take the next steps

Now that you've got the inside scoop, we hope you're feeling more confident about the next steps in your Office 365 deployment. If you'd like a deeper dive, or you're running into problems with your current migration, read our **"Survival guide for Office 365 networks."** This document explores strategies for getting your network ready for Office 365, and the specific steps you should take to make your deployment a success.

About Zscaler

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler connects users to applications and cloud services, regardless of device, location, or network, while providing comprehensive security and a fast user experience. All without costly, complex gateway appliances.

zscaler™