Umbrella Improves O365 Deployment Success and On-going Performance

Current Situation

The combination of two key trends is driving a high rate of conversion to Microsoft O365. The move to the cloud for key applications has picked up momentum and progressed from an early adopter status to a mainstream concept, plus Microsoft has become increasingly aggressive with programs that promote the transition to O365 for all Office renewals. While O365 is a strong offering and has many productivity and cost advantages, there are some significant network and security issues that are causing problems as organizations migrate.

In many cases, trials or small initial deployments work well but when the entire organization is turned on, issues arise. The activity generated by a SaaS office suite is different than other applications. There tends to be a high volume of traffic from multiple locations, with many open threads and extended session times. Large organizations have users connecting from all over the globe. This scenario doesn't typically perform well in organizations that are backhauling traffic to a data center and Secure Web Gateway (SWG) or using a cloud proxy to intercept and decrypt all of the traffic. These performance issues can stall O365 adoption, frustrate users, and result in a higher number of shadow IT solutions.

Microsoft's response to these issues is to recommend not using a proxy for the core O365 traffic and in some cases purchasing their "ExpressRoute" offering to improve performance. They say "Don't proxy O365 traffic" and recommend allowing O365 traffic to be sent directly to their cloud service, whitelisting it from a SWG/proxy (both on-prem, and cloud-based) as can be seen in this recent MS KB article. To date customers have had trouble adopting this advice with the frequent IP changes from Microsoft and even when they do, performance issues still linger in many cases. Microsoft is trying to help by implementing a new API-based model whereby the list of domains is split into categories, designating three types of traffic:

- Optimize: These are the core MS destinations (roughly 75% of the traffic) that should not be inspected, decrypted, or authenticated by a proxy. MS hosts these IPs and URLs and claims that security is included. MS is reducing this to ~8 URLs to further simplify.
- Allow: Non-critical destinations, where MS recommends applying the organization's default security policy, but still advises not to decrypt. Some network latency is not expected to cause major performance issues.
- Default: These are other destinations that may not necessarily be hosted by MS, and proxy inspection policies can be applied as these are just like standard web browsing.

Key challenges

- It is a well-known fact that SWGs and proxies do not play nicely with Microsoft O365. Long-lived connections get broken by a proxy in the middle, and the multiple connections that the O365 apps generate add heavy load to a proxy (and to any other appliances or other infrastructure at a customer's edge).
- While recommending to whitelist traffic from a proxy to their cloud-based O365 service, Microsoft also frequently updates the list of their cloud URLs and IPs used by the service.
- These frequent updates and new domains also make it challenging for vendors to accurately categorize them under their content categorization engines, often leading to O365 domains being classified under a number of different content categories, causing inconsistent enforcement of policies.
- Poor performance impedes adoption and causes backlash from unhappy end users.
- Slow response times lead to increased shadow IT activities for core functionality like collaboration and file storage/ sharing which expands the threat surface.
- Organizations see an increase in email related security incidents when using Microsoft email security and need better protection.
- There is a need for data loss prevention for email, and data in SharePoint and OneDrive.

Umbrella solution and advantages

- Because of the way that Umbrella works (enforced at the DNS layer) and thanks to Umbrella's selective proxy, requests to O365 in most cases will not be redirected via any cloud DC and will be sent to MS direct from the customer's egress. (In other words, Umbrella doesn't break the traffic from the start, unlike the many other vendors who do, and therefore then need to implement additional mechanisms to prevent this.)
- Umbrella is also peered closely with MS O365, and in fact we're directly peering in over 90% of the locations in our global network. We utilize our knowledge of Microsoft data centers/web servers to deliver better DNS resolution performance.
- Umbrella utilizes EDNS Client Subnet (ECS) to retain the context of requests including the location. Leveraging this data to select the best route for O365 traffic provides better performance than just relying on the centralized customer location or their cloud proxy data center point of egress.
- While MS doesn't support EDNS in their entire O365 infrastructure[1], Cisco has worked with MS to ensure that all DNS queries for O365 destinations will always be resolved to the best MS DC for the user's breakout egress, regardless of location of the Umbrella DC that resolved the request (taking full advantage of our Anycast infrastructure for reliability and simplicity, but without any compromise on performance).
- Umbrella's intelligence is applied at the time of DNS resolution, in most cases without the need for further inspection of traffic. This of course applies for all requests to O365, including non-web, encrypted, and other proprietary traffic, but being at the DNS layer doesn't interfere with or break any O365 traffic. If a requested destination is highlighted by Umbrella's models as risky or malicious (for example, the requested host may have been compromised), security is still applied in one of two ways:
  1. If Umbrella sees the requested destination as malicious, the request will be blocked at the time of DNS query
  2. If Umbrella sees the requested web destinations as risky, the request will be redirected to Umbrella's selective proxy for further inspection.

Improved performance

We have seen Umbrella provide improved performance in several O365 deployments when compared to using Microsoft's ExpressRoute service or a variety of full proxy solutions. While usage patterns, office locations and deployments vary by customer we have seen better performance across a set of metrics when using Umbrella.

Sample performance improvement:

Umbrella (w/roaming client) compared to Microsoft ExpressRoute.

Item	Improvement
Reduced DNS resolution time	An average of 50 to 90% reduction in DNS TCP round trip times globally An average of 60 to 98% reduction in DNS ICMP round trip times globally
Improved routing performance	An average of 60 to 80% improvement in O365/IPV4 ICMP round trip times
Reduction in routing hops	25 to 40% reduction in the number of network hops for O365/IPV4 network hops
More efficient CDN results	50 to 75% improvement in http round trip times 70 to 85% reduction in download times 300 to 500% increase in CDN bandwidth Improved multimedia performance over wireless and wired networks

[1] Cisco is working with Microsoft, and encouraging for the adoption of EDNS Client Subnet within the Office 365 global network. This is "in the works" and has been adopted by some subsets of MS services, but at time of writing is not in use globally. O365 is not a single unified product, so we've been pushing for adoption primarily on outlook.office365.com, but that hasn't happened yet."

As mentioned above customer environments, locations and traffic patterns vary so the best way to test for improved performance is to set up an Umbrella trial and compare results.

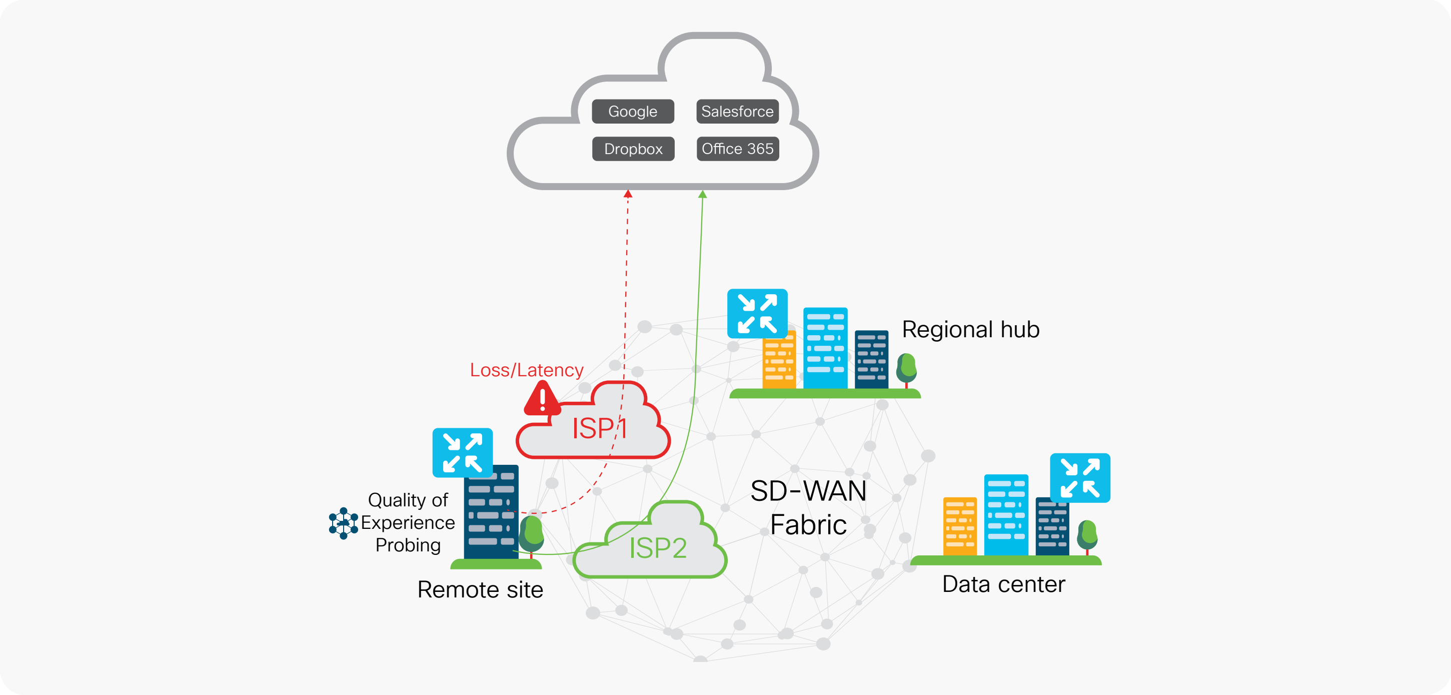
Additional Cisco Security Solutions for O365

Cisco SD-WAN (Viptela)

A fundamental tenet of the Cisco SD-WAN fabric is connecting users to applications in the cloud in a seamless, secure, and reliable fashion with the best performance. Cisco delivers this comprehensive capability for SaaS applications with the Cloud onRamp for SaaS solution, in alignment with Microsoft's connectivity principles for Office 365 (aka.ms/pnc). With Cloud onRamp for SaaS, the SD-WAN fabric continuously measures the performance of a designated SaaS application through all permissible paths. For each path, the fabric computes a quality-of-experience score ranging from 0 to 10. This score gives network administrators visibility into application performance that has never before been available. Most importantly, the fabric automatically makes real-time decisions to choose the best-performing path between the end users and the cloud SaaS application. Enterprises have the flexibility to deploy this capability in multiple ways, according to their business needs and security requirements.

- Cisco SD-WAN enables customers to apply business-centric, application-aware, and differentiated routing policies providing end users direct connectivity to performance-intensive trusted applications, such as Office 365, while routing generic Internet traffic via SWGs, CASBs, or the customer's data center.
- Enterprises can leverage Cisco's Cloud onRamp for SaaS capabilities to intelligently route Office 365 traffic, providing a fast, secure, and reliable end-user experience.
- All paths to Office 365 from each circuit at the branch, regional hub, and data center will be monitored continuously for performance, and the application traffic will be dynamically routed to the best-performing path without requiring human intervention.
- Cloud onRamp for SaaS provides network administrators superior real-time and historical visibility into application performance through a quality-of-experience metric.

This performance aware approach for evaluating and selecting the ideal path for O365 traffic can have a significant positive impact on the user experience from all locations.



Cisco Cloud Email Security (CES)

Cisco Cloud Email Security protects O365 users from sophisticated, targeted phishing attacks and uses global intelligence to identify and block other emerging email threats. Cisco also helps customers protect email attachments with confidential data, as well as the emails themselves that contain sensitive content. Today's attacks are becoming more complex and that includes those that target Office 365 users. A file attachment that may look benign when it comes in can transform into malware hours, days, or weeks after entering an environment. Our retrospective security alerts administrators when a file turns malicious, making it a critical factor in determining security options for Office 365. In addition, Mailbox Auto-Remediation can automatically remove these malicious attachments, saving teams hours of work and helping them contain threats before they cause more damage. There is a simple "Threat Analyzer" process which scans a set of mailboxes to show prospects the threats that are getting through their current email security solution.

Fortified by shared intelligence, our Email Security solution goes way beyond single-point-in-time scanning to provide:

- The most robust and predictive global intelligence from Cisco Talos that sees attacks before they impact your systems.
- Protection from risky files no matter when they become malicious and mitigation of damage if an infection occurs.
- Deep, real-time URL scans, analysis and blocks that catches malicious changes at click time.
- Prevention of sensitive information from inadvertently getting out so you can stay compliant with industry and government regulations.
- Comprehensive and real-time reporting to reduce investigation and response times.

Cloudlock

Cisco Cloudlock provides user, data and app security for O365. User and entity behavior analytics are used to detect compromised accounts and malicious insiders. Prebuilt and custom data loss prevention (DLP) policies are available to detect sensitive data in SharePoint or OneDrive and there are a set of response actions including the ability to alert users and administrators, remove collaboration rights or revoke sharing permissions. This data visibility and control enables Cloudlock to protect files from improper storage and exposure in O365. Cloudlock also gives customers the ability to see all of the third-party apps that are connected to O365 via OAuth. It includes crowd-sourced trust scoring and provides the ability to revoke the OAuth connection to risky apps.

Summary

The adoption of office productivity tools such as Office 365 has become mainstream because of the many efficiency benefits they provide. Many organizations have found that to realize these great benefits in a secure way across their environment they need to streamline their connection methods and enhance security. Cisco provides a set of cloud security solutions to facilitate adoption and enable a unique combination of performance and security to both protect and delight users.

Need more information?

Contact your Cisco or partner sales representative for more information on Umbrella or start a free demo at: https://signup.umbrella.com/