# Consolidate Your Security in the Cloud with Cisco Umbrella

By Meg Diaz

November 5, 2019

What makes a great partnership? Open communication and a passion for constant advancement are two important elements. Our customers have helped us continuously innovate, and together, we're transforming how security is delivered. Over the past 12+ months, we embarked on a journey to take Cisco Umbrella to a new level.

DNS has always been at our core — starting as a recursive DNS service (OpenDNS) in 2006, then moving into the enterprise security space in 2012 with the release of Umbrella. Enforcing security at the DNS layer was something brand new at the time. People started to see how valuable it was to have a single view of all internet activity across every location, and it was an incredibly effective way to block threats at the earliest possible point (and who doesn't love fewer alerts to investigate!?). Add in the fact that it's delivered from the cloud and can be deployed enterprise-wide in minutes…you can start to see the appeal it has.

As we saw more applications and infrastructure move to the cloud, more people working off-network (and "forgetting" to turn on that pesky VPN), and the move to more direct internet access at remote offices, we heard more from our customers about what they needed from a security service. It wasn't just about DNS-layer security — they often needed more. We're excited to share that we're now delivering more. *Much* more.

Now, Umbrella offers secure web gateway, cloud-delivered firewall, and cloud access security broker (CASB) functionality — in addition to the DNS-layer security and threat intelligence from Investigate — all in a single, integrated cloud console. All of this is available in a new Umbrella package: Secure Internet Gateway Essentials.

By unifying multiple security services in the cloud, we are now able to offer our customers greater flexibility, sharper visibility, and consistent enforcement, everywhere your users work. The goal is simple – if we can simplify your security operations and reduce complexity, then you can reduce risk and accelerate secure cloud adoption.

## Here are a few examples of innovations that we’re introducing as part of this:

### Bye security silos, hello consolidation

It can be an overwhelming endeavor to help your organization transition to the cloud and secure direct internet access. It takes skill and a considerable amount of resources. How many office locations are you tasked with securing? We’ve heard loud and clear that it’s not sustainable for you to build a separate security stack in each location. By moving those core security services to a single cloud solution, you’ll be able to deploy the right level of security consistently across your organization. And you have the flexibility to deploy it as needed — you’re not forced to proxy everything or deploy in a specific way. For example, you could start with DNS for fast protection everywhere and leverage additional security services (secure web gateway, firewall, CASB, etc.) wherever you need them.

*“I like the simplicity of Cisco Umbrella from a management perspective, but I also enjoy the complexity of the advanced layers of protection that Cisco Umbrella provides. This one product has truly transformed our ability to protect our entire workforce, regardless of location.”* **– Ryan Deppe, Network Operation Supervisor, Cianbro Corporation**

### Well-known technology, brand new approach

IPSec tunnels have been around forever. But, we set out to do something different based on what we’ve heard from you. Cisco developed a new technology for IPSec tunnels that minimizes downtime and eliminates the need to build secondary tunnels with a patent-pending approach using Anycast technology for automated failover. A single IPsec tunnel can be deployed to send traffic to Umbrella from any network device, including SD-WAN. This integrated approach combined with Anycast routing can efficiently protect branch users, connected devices, and application usage from all internet breakouts with 100% business uptime.

### Real-time detection of DNS tunneling

Even though we’ve been a leader in DNS-layer security for years, we won’t rest on our laurels. We’re watching attacker tactics and quickly adjusting ours

— DNS tunneling is one example. DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic (i.e. HTTP) over port 53. There are legitimate reasons why you would use DNS tunneling, but attackers have been using it for data exfiltration and command and control callbacks. To better identify and stop this, we've added advanced detection capabilities, real-time heuristics, signature, and encoded data detection to Umbrella.

## Deeper web control, retrospective alerts on malicious files

Our new secure web gateway (full proxy) provides complete web traffic visibility, control, and protection — with capabilities such as content filtering at the URL-level, blocking applications or app functions, HTTPS decryption (either for select sites or all), file inspection with Cisco Advanced Malware Protection and antivirus, sandboxing unknown files with Cisco Threat Grid, and retrospective alerts on files that subsequently display malicious behavior. Think about it — file behavior can change over time or could put mechanisms in place to evade initial detection. If a file is initially determined to be safe by Threat Grid and downloaded from the web, but later is deemed to be malicious, you can now see that in Umbrella.

All of these Umbrella enhancements are designed to help your organization accelerate cloud adoption with confidence — you need assurance that your users will be secure wherever they connect to the internet and that's exactly what we're focused on delivering for you. If you want to learn more, join our virtual launch event on November 12th and check out Jeff Reed's blog to hear about other Cisco Security innovations.