Cisco Umbrella

What is Umbrella?

- **First line of defense against threats:** built into the foundation of the internet, blocks requests to malicious/unwanted destinations before a connection is even established—without adding any latency.
- **Visibility and protection everywhere:** users and apps have left the perimeter. Umbrella provides visibility needed to protect internet access across all devices on network, all office locations, and roaming users.
- **Enterprise-wide deployment in minutes:** simplest security product to deploy and can protect users across an organization in minutes. By performing everything in the cloud with 100% uptime, there is no hardware to install, and no software to manually update.

Why Do Customers Need It?

- **Reduces alerts and prevents threats before they happen:** despite deploying many security products at the perimeter and on endpoints, attackers still get in and security teams deal with too many infections.
- **Eliminates gaps in coverage:** security teams lack visibility into all internet activity across all locations, devices and users, blocking threats over all ports and protocols.
- **Enforces consistent policies:** most products are too complex for smaller security teams, don't perform well everywhere, and don't easily integrate with existing security investments.

How Do I Sell It?

As first line of defense against threats to security pros who have:

- Too many security alerts or malware infections
- With apps and data moving to the cloud, users with roaming laptops no longer turn the VPN, exposing organizations to threats

As a replacement to web security solutions for orgs who have:

- A decentralized network with many direct-to-internet branch offices who need off-network coverage
- A small or understaffed security team
- Guest Wi-Fi or a BYOD policy

Low Hanging Fruit

- Hit by ransomware (e.g. CryptoLocker, CryptoWall, Locky)
- Employ mobile users working on roaming laptops (Windows and Mac OSX)
- Use sanctioned cloud apps (e.g. Office365, Google Drive, Box)
- Own Blue Coat, Websense, McAfee, or other SWG appliances that: (1) is not effective against threats, or (2) can't scale to their traffic loads
- Own AMP Threat Grid, FireEye, or another product that we integrate with