Securing Remote Workers at Scale
How Communications Service Providers Create Services around Cisco Umbrella for Consumers and SMBs

May 5, 2020
A new economic model based on remote working

- **10%-50%** Wireline Internet traffic growth
- **25-40%** VPN traffic increase (USA)
- **Up to 150%** Internet peering traffic growth
- **10%-50%** Mobile Internet traffic growth
- **up to 400%** Video conferencing traffic increase
- **40%** Increase in DDoS traffic
Communications Service Providers standing up to the challenge

Source: Speedtest
Make best use of Cisco to support an economy working from home
Cybersecurity during a pandemic

- 667% increase in phishing
- 100k new domains with covid-19 appear in the first 3 weeks
- 40% more/30% longer DDoS attacks

Source: Cisco Umbrella Investigate
Put the right level of security in place
Win With Cisco Umbrella

Easy Protect/Mobile Protect

Secure Access Lines

Easy Deployment, Low Cost

Proven ARPU Booster
Umbrella DNS-layer security

Benefits
See all internet traffic across users
Block attacks earlier
Contain malware if already inside
Cisco Umbrella: security that just works!

- First layer of defense against threats on the internet, such as malware, ransomware, phishing and more.
- 100% Cloud-based – very easy to deploy
- Best DNS layer security in the industry*
- Best-in-class threat intelligence – integrated with TALOS

200B | 100M | 18.5K | 190+
---|---|---|---
requests per day | daily active users | Enterprise customers | Countries worldwide

Discover

3M+ new domain names daily

Identify

60K+ malicious destinations daily

Enforce

7M+ malicious destinations while delivering fast internet access

© 2019 Cisco and/or its affiliates. All rights reserved.

* Cisco Umbrella DNS-layer security detection exceeds competition: 280% higher than Palo Alto | 96% higher than Akamai | 47% higher than InfoBlox
Umbrella Easy Protect / Mobile Protect
For small business and consumer

Service Provider

Small business broadband (attach to business line; up to 25 users)

Mobile

Consumer broadband (attach to consumer line; up to 6 users)

Umbrella

Extend value-added security to consumer customers

- Same industry-leading security
- Same simple attach
- New opportunity to grow ARPU with new addressable market (>1B broadband lines globally)
# Umbrella Easy Protect / Mobile Protect delivers “clean pipe” with simple attach

<table>
<thead>
<tr>
<th>Umbrella Easy Protect</th>
<th>Umbrella Mobile Protect</th>
</tr>
</thead>
<tbody>
<tr>
<td>[small business and consumer]</td>
<td></td>
</tr>
<tr>
<td><strong>SP service</strong></td>
<td>Internet services</td>
</tr>
<tr>
<td><strong>Target customer</strong></td>
<td></td>
</tr>
<tr>
<td>• Small business (up to 25 users)</td>
<td>Mobile services</td>
</tr>
<tr>
<td>• Consumer (up to 6 users)</td>
<td>Any customer with a SIM-based device</td>
</tr>
<tr>
<td><strong>Umbrella functionality</strong></td>
<td></td>
</tr>
<tr>
<td>• Blocks malware, phishing, ransomware &amp; more</td>
<td></td>
</tr>
<tr>
<td>• Simple add on for “clean pipe” offer</td>
<td></td>
</tr>
<tr>
<td>• One policy for all customers</td>
<td></td>
</tr>
<tr>
<td>• Full SP network coverage</td>
<td></td>
</tr>
</tbody>
</table>

Value proposition: bundle with remote worker connectivity. Easy to deploy and simple to manage security value add. “Clean pipe.”
SMBs & Cybersecurity: little resources, need for simple offers that “just work”

**Low End of SMBs**

Approximately 80% of SMBs are low-end, characterized by:

- Local “Mom & Pop” (1-9 employees)
- Little/no IT resource or knowledge
- Unprotected (little/no security expertise)
- Do-It-Yourself: owner purchases IT through web/call center
- Budget conscious

**Needs for SP offering that serves this market**

- Low-priced offering
  - Security price that is 10% or less of overall service price
- Security bundled into connectivity
  - Around 80% SMBs prefer this
- Security that “just works”
  - Simple set-up, ease of use
  - Monthly aggregate reporting
Cyber-security protection especially for small SMBs is inadequate – high risk of costly incidents

Share of Businesses Not Feeling Protected Against a Cyber-Security Attack (%)\(^1\)

- 24% of businesses with 0-9 employees
- 18% with 10-249 employees
- 10% with 50-249 employees
- 11% with 250-1000 employees

One quarter of micro businesses with inadequate protection

Cost of Security-Related Incidents in the last 12 Months (US-\$/Employee)\(^2\)

- $400 for 0-9 employees
- $300 for 10-249 employees
- $200 for 50-249 employees
- $100 for 250-1000 employees

Question 1: How well is your business protected against any type of internal data theft/loss, or external cybersecurity threats and attack?

Question 2: How much would you estimate that the incident(s) cost your company (including direct losses as well as costs incurred to recover from the breach(es) and restore the lost information, legal costs to your business, and costs of repairing your business’ reputation)?

Source: Analysys Mason, Small and medium-sized businesses: technology buying behavior and channel preferences, n=2.983, September 2019
SMBs trust their existing suppliers/connectivity providers when it comes to security.

**Primary Driver for Adoption of Security (%)**

- Recommendation by... 42%
- Internal Compliance 34%
- Government Regulations 34%
- Risk Assessment 33%
- Awareness of Attacks on... 32%
- Direct Experience of... 22%
- Other 2%

**Intention of businesses to buy services other than connectivity from their fixed service provider (%)**

- Remotely Managed IT Services 34%
- Software/Applications 36%
- Cyber-Security 37%
- Cloud Storage/Hosting 38%
- Unified Communications 40%

---

**Question 1:** What are your Primary Drivers for Adoption of Security?

Source: STL Partners, SMB Customer Interviews, How Telcos Can Win With SMBs: Strategies for Success, August 2019

**Question 2:** Would you consider purchasing the following services from your principal fixed provider?

Source: Analysys Mason, Small and medium-sized businesses: technology buying behavior and channel preferences, n=2.983, September 2019
Service Provider value highlights

Business or consumer end customers

- New ways to generate revenue beyond connectivity
  - Add ARPU per month

- Fast deployment shortening SP time to revenue
  - Easy deployment of new services at low cost

- A new way to build loyalty with customer base
  - Low churn, increase penetration

- Brand differentiation from competition
  - Network-level security that just works
Umbrella Easy Protect/Mobile Protect
Security that’s simple to deploy and easy to maintain

It just works.

Scale
Ability to provide coverage to very large networks

SP Retains Control
‘Fire and forget’ security
Caching deployment model

Make Money Fast
Increase ARPU, protect base, low co.

Fast to Launch
Simple Attach, Point to Umbrella Cloud

Cost Effective
Simple Term and MSLA contracts
Heavy data privacy language

Low Customer Complaints
Easy to explain to customers
No support calls

Best Security in the Industry
Cisco Umbrella + TALOS

Data Privacy Friendly
Caching deployment model

© 2019 Cisco and/or its affiliates. All rights reserved.
Attractive business case for Service Providers

Example Scenario

- Additional ARPU: $36/line/year ($3/line/mo)
- Opt-out model for 500k lines
- SP gross revenue: $18M/year

SP gross revenue

- SP overhead = $1/line/year
- SP profit $12.5M/year (positive loyalty effects)

SP profit
Umbrella Benefits for End Users

• **Benefit from Cisco Threat Intelligence**: protection from Advanced Persistent Threats, including
  ✓ Protection against phishing attacks that aim at subtracting personal/sensitive information (mobile banking credentials, passwords etc.)
  ✓ Protection against most advanced ransomware
  ✓ Protection against zero day malware (not protected through “signature based” solutions)

• **Preserve Customer Experience**: Non-invasive (no agent in the end device, PC/smartphone)
  ✓ No battery drain, zero impact on the devices
  ✓ No need to update any local software
  ✓ No install/configuration needed by the end users

• **Give Visibility**: Evidence how Umbrella is protecting the end customer
  ✓ Block Pages
  ✓ Aggregate reporting, relayed e.g. in newsletters
Go-To-Market Models

Opt-out
- Automatically bundle for entire target customer base
- Low churn

Hybrid Models

Opt-in
- Active selling, try & buy
- Target new customers and renewals/upsells
- Penetration typically 15–25%

GTM Guiding Principles
- Embed network-level security into broadband connectivity for small business or consumer customers
- Respect regulatory and customer protection framework
Opt-out Go-To-Market Strategy
Simple Approach To Target The Entire Customer Base

1 letter notifying customers
one month free trial
Three Euro monthly charge
Opt-out anytime

© 2019 Cisco and/or its affiliates. All rights reserved.
Cisco Umbrella Outperforms Competition

Number of test cases 3,668. Detection rate of links pointing directly to PE malware (e.g. EXE files), links pointing to other forms of malicious files (e.g. HTML, JavaScript) as well as phishing URLs.

Source: AV Test February 2020
Providers worldwide build on Cisco Umbrella
Leverage the Cisco brand

Case Studies

© 2019 Cisco and/or its affiliates. All rights reserved.
More threats blocked daily than anyone else

TALOS
Cisco Security Research

20B

Fortinet 972M
Symantec 250M
Palo Alto 4M
Check Point 700K
Zscaler 800K
Trend Micro 1M
Proofpoint 1M

972M
250M
4M
700K
800K
1M
1M
What sets Umbrella apart

- Fastest and most reliable cloud infrastructure
- Easiest connect-to-cloud deployment
- Broadest coverage of malicious destinations and files
- Most predictive intelligence to stop threats earlier
- Most open platform for integration

- Low Cost for Support
- Fast way to revenue
- Low risk to your brand

© 2019 Cisco and/or its affiliates. All rights reserved.
Win With Cisco Umbrella

*Easy Protect/Mobile Protect*

- Secure Access Lines
- Easy Deployment, Low Cost
- Proven ARPU Booster
Summary, Key Takeaways

1. There is a large opportunity Easy Protect

2. Let's start a **business conversation** about growing APRU with simple security attach

3. Contact your **Cisco account manager** or email us at **umbrella.sp@cisco.com**