Cloud-Based Security Tailored for Managed Security Service Providers
Today’s Presenters

John Malzahn
Senior Manager, Service Provider Solutions Marketing
Cisco Systems

Rishi Agarwal
SP Business Leader, Cisco Umbrella
Cisco Systems
Agenda

1. Challenges
2. Umbrella Overview
3. Solution for SP/MSSPs
4. Customer Success Stories
5. Vision and Direction
6. What do I do next?
Challenges
Challenges and needs as an SP

Challenges
- Inefficient service creation and ongoing operations
- Increasingly competitive environment
- Differing customer needs
- Flexibility to adjust services quickly and efficiently

Needs
- Improved management and visibility/interoperability
- Vendors who are easy to do business with
- Flexible licensing models
- Minimal upfront capital investments
Challenges as an MSSP

Visibility
Do you see all the traffic?

Enforcement
Are you able to enforce policy?

Management
Can you consistently adapt?
Benefits of Umbrella

- Growth opportunity
- Easy to deploy and manage
- Complements security portfolio
Umbrella Overview
DNS
Overview

Domain registrar
Maps and records names to #s in “phone books”

Authoritative DNS
Owns and publishes the “phone books”

Recursive DNS
Looks up and remembers the #s for each name

© 2018 Cisco and/or its affiliates. All rights reserved.
Data centers co-located at major IXPs

30 data centers worldwide
Where does Umbrella fit?

Benefits

- Block malware before it hits the enterprise
- Contains malware if already inside
- Internet access is faster
- Provision globally in minutes
Cisco Umbrella Traction

150B requests per day
90M daily active users
15K enterprise customers
160+ countries worldwide
Solution for SP/MSSPs
## Capture all segments with SP / MSSP Offers

### Secure Connectivity

<table>
<thead>
<tr>
<th>SP Easy Protect*</th>
<th>SP Mobile Protect*</th>
<th>Umbrella + MR (Beta)</th>
<th>MSSP*</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Circuit Level Security</td>
<td>• Mobile Security</td>
<td>• Secure WiFi for SMB</td>
<td>• Umbrella Enterprise</td>
</tr>
<tr>
<td>• Simple attach</td>
<td>• Simple attach</td>
<td>• Meraki AP Integration</td>
<td>• Automated trial portal (PPOV)</td>
</tr>
<tr>
<td>• SP portal integration</td>
<td>• SP portal integration</td>
<td>• “Single” Meraki Offer</td>
<td>• MSSP management portal</td>
</tr>
<tr>
<td>• Minimal admin burden</td>
<td>• Minimal admin burden</td>
<td>• Extends to Meraki WLAN agreements – not MSLA</td>
<td>• Yearly and monthly terms</td>
</tr>
<tr>
<td>• Yearly and monthly license terms</td>
<td>• Yearly and monthly license terms</td>
<td>• Per-AP license</td>
<td>• Pre and Post Paid</td>
</tr>
<tr>
<td>• Pre and Post Paid</td>
<td>• Pre and Post Paid</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Logs kept for 30 days</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Available on MSLA¹ and GPL

### Simple
- Small Business

### Advanced
- Large Enterprise

¹. Only Insights package for MSSP on MSLA
MSSP organization

Centralized settings | MSSP admins | Centralized reports | Log management

Customer 1
Subscription | Admin and settings | Reports

Customer 20K
Subscription | Admin and settings | Reports

© 2018 Cisco and/or its affiliates. All rights reserved.
## Customer Management

<table>
<thead>
<tr>
<th>License</th>
<th>Seats</th>
<th>Service Period</th>
<th>Centralized Log Status</th>
<th>Networks</th>
<th>Roaming Clients</th>
<th>VAS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bimbee (Insights)</strong></td>
<td>100</td>
<td>Apr 03, 2018 – Apr 02, 2021</td>
<td>Not configured</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Centific (Professional)</strong></td>
<td>50</td>
<td>Apr 03, 2018 – Apr 02, 2021</td>
<td>Not configured</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Prolia (Platform)</strong></td>
<td>500</td>
<td>Apr 03, 2018 – Apr 02, 2021</td>
<td>Not configured</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Total Seats: 650
### Total Customers: 3
Customer Success Stories
Users: 600,000

**Objective:** As Italy’s businesses grew increasingly vulnerable to the threat of ransomware, data breaches, and other malicious malware attacks, service provider TIM sought an innovative solution to effectively and efficiently protect the network and data of its business users.

**Solution:** Cisco Umbrella for Service Providers (SPs): Easy Protect

**Impact:**
- Rolled out TIM Safe Web to more than 600,000 customers, with less than 1 in 10,000 customers opting out of the service
- Provided TIM with a unique competitive differentiator
- Created an incremental revenue stream for TIM

“Cisco Umbrella helps us improve our customers’ lives and deliver the best customer experience by integrating service simplicity with ground-breaking protections against phishing and malware for businesses.”

Salvatore Nappi
Head IT Business Marketing
TIM
Company: Avanade
Headquarters: Seattle, WA
Employees: 10,000

Objective: Enable highly mobile consultants to work securely at client sites, on public networks, and in other vulnerable areas around the world that are outside of the corporate network.

Solution: Cisco Umbrella

Impact:
- Strengthened protection for employees and clients against malware, ransomware, and other threats
- Increased visibility into threats and decreased remediation time
- Achieved fast time-to-value

“Our business is driven by consultants working outside of the office, so protecting them and the clients they work with means protecting them everywhere they go. Umbrella allows us to do so in a way that’s both easy to deploy and effective.”

Joseph Paradi
Sr. Director – ITS Infrastructure
Avanade
Users: 24,000

Objective: By adding Cisco Umbrella to its existing security stack, Memorial Hermann Health System achieved a significant reduction in malware and extended off-network protections for its employees.

Solution:
Cisco Umbrella
Cisco Umbrella Investigate

Impact:
- Reduced security events below .05%
- Reduced investigation time by 80%
- Extended protections to off-network devices

“Cisco Umbrella protects against threats like ransomware that target PHI and PII and jeopardize our ability to care for patients.”

Zach Phillippe
Cyber Security Manager
Memorial Hermann Health System
Employees: 4,350

Objective: Enhance the customer experience by building automation into the security practice

Solution:
Cisco Umbrella
Cisco Umbrella Investigate

Impact:
• Decreased incident response time from days to minutes through automation, enabled by the Investigate API
• Reduction in network security incidents and infected endpoints
• Enriched security event data and threat intelligence with Investigate

“Cisco Umbrella gives us more confidence in our ability to proactively protect our customers and employees, and more efficiency in our incident response process.”

Vivek Raman
Head of Security
Yelp
Vision and Direction
The traditional model
Disruption: To the cloud

Internet / SaaS / IaaS

SD WAN  DIA/DCA

Branch office  HQ  Roaming/mobile

© 2018 Cisco and/or its affiliates. All rights reserved.
You need coverage everywhere

- **Boost**
  - Existing security
  - HQ

- **Transform**
  - Edge security
  - Branch (DIA/DCA)

- **Enable**
  - Off-network security
  - Roaming/mobile
App Discovery with Umbrella

- Visibility into apps that exist within an org’s env.
- Understand risks and identities, who is using what
- Workflow Management

What’s next:

- App Control (Block a select # of Apps / List to grow over time)
- Redirect from CSR to App Discovery in UMB
- Pkg & Pricing in progress (Add On SKU, Bundle option)
Meraki MR + Umbrella

- Simplest way to deploy Umbrella across a wireless network
- Conveniently enable Umbrella policies directly in the Meraki dashboard
- Create granular policies on a per-SSID basis or by using Meraki group policies
How it works

Step 1 (Umbrella dashboard)
Copy API key and Secret.

Step 2 (Meraki dashboard)
Input API key and secret.
How it works

Step 3 (Meraki dashboard)
Apply Umbrella policy.

Step 4
That’s it. Seriously, it’s that easy.
Cisco Security Connector
One app, two layers of security

Encryption and enforcement
Internet requests

Auditing and correlation
App traffic flows

Works anywhere
On- and off-network

One app, two extensions
Automatically provisioned via Meraki

Requests attributed by iOS identity

Flows attributed by iOS identity and app
Flexible deployment options

**Today**
- ISR 4K
- ISR 1K
- AnyConnect
- Meraki MR
- WLAN controller
- Security Connector for iOS

**Future**
- Meraki MX
- SD-WAN (Viptela)*
EU data warehouse

• The launch of a data warehouse within the EU, headquartered in Frankfurt

• Solution for customers who are concerned about Data Sovereignty or have concerns about having their data stored in the US
  • Customers will be able to choose which datacenter they would like to have their personal data located (US or EU)
What do I do next?
What do I do next?

1. Meet MSSP requirements
2. Get access to MSSP console
3. Get customers on trial using new PPOV

Umbrella
Start blocking in minutes
What PPoV can do for you

With this tool, you can easily:

- Provision 21-day customer trials
- Track multiple customer trials from an easy-to-use cloud-based console
- Extend trials for another 21 days
- Request access to customer’s trial
- Produce reports to show blocked attacks

Which leads to:

More closed deals!
For more information

Visit www.cisco.com/go/mssp
or contact your Cisco account representatives
Questions?