Cisco Umbrella

Delivering predictive cloud security for Service Providers

Ken Davidson
Director SaaS
5/16/2017
The Service Provider Opportunity

• The SP is uniquely positioned to deliver security as a managed service - consumer and business customers

• The SP can rapidly deliver security offers as part of an integrated offer - leveraging the network is key

• The SP has the skillsets / processes / infrastructure to sell the services – telesales to focused high-touch sales teams

• The SP can deliver security offers cost effectively – investment alignment

• The SP can reinforce their brand identity through managed security offers

Cisco Umbrella
Addressing the Opportunity

Customers
- IOT
- Consumer
- Small Business
- Branch
- Enterprise

Technologies
- Cellular
- Wi-Fi
- Internet (Fiber/XDSL/cable)
- Cloud Services

Support Multiple Access Technologies

Cisco Umbrella
Addressing the Opportunity

Customers
- IOT
- Consumer
- Small Business
- Branch
- Enterprise

Technologies
- Cellular
- Wi-Fi
- Internet (Fiber/XDSL/cable)
- Cloud Services

Scale
- XXX,000,000
- XX,000,000
- X00,000
- X0,000
- X,000

Scale end devices & Customers

Cisco Umbrella
Addressing the Opportunity

<table>
<thead>
<tr>
<th>Customers</th>
<th>Technologies</th>
<th>Scale</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOT</td>
<td>Cellular</td>
<td>XXX,000,000</td>
<td>$</td>
</tr>
<tr>
<td>Consumer</td>
<td>Wi-Fi</td>
<td>XX,000,000</td>
<td>$$</td>
</tr>
<tr>
<td>Small Business</td>
<td>Internet (Fiber/</td>
<td>X00,000</td>
<td>$$$</td>
</tr>
<tr>
<td></td>
<td>XDSL/cable)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Branch</td>
<td>Cloud Services</td>
<td>X0,000</td>
<td>$$$$</td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td>X,000</td>
<td>$$$$$$</td>
</tr>
</tbody>
</table>

Tight coupling of functionality to price
### Addressing the Opportunity

<table>
<thead>
<tr>
<th>Customers</th>
<th>Technologies</th>
<th>Scale</th>
<th>Price</th>
<th>SP Eng. Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOT</td>
<td>Cellular</td>
<td>XXX,000,000</td>
<td>$</td>
<td>Low</td>
</tr>
<tr>
<td>Consumer</td>
<td>Wi-Fi</td>
<td>XX,000,000</td>
<td>$$</td>
<td>Low</td>
</tr>
<tr>
<td>Small Business</td>
<td>Internet (Fiber/</td>
<td>X00,000</td>
<td>$$$</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>XDSL/cable)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Branch</td>
<td>Cloud Services</td>
<td>X0,000</td>
<td>$$$$</td>
<td>Medium</td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td>X,000</td>
<td>$$$$$$</td>
<td>High</td>
</tr>
</tbody>
</table>

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
### Addressing the Opportunity

<table>
<thead>
<tr>
<th>Customers</th>
<th>Technologies</th>
<th>Scale</th>
<th>Price</th>
<th>SP Eng. Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOT</td>
<td>Cellular</td>
<td>XXX,000,000</td>
<td>$</td>
<td>Low</td>
</tr>
<tr>
<td>Consumer</td>
<td>Wi-Fi</td>
<td>XX,000,000</td>
<td>$$</td>
<td>Low</td>
</tr>
<tr>
<td>Small Business</td>
<td>Internet (Fiber/XDSL/cable)</td>
<td>X00,000</td>
<td>$$$</td>
<td>Low</td>
</tr>
<tr>
<td>Branch</td>
<td>Cloud Services</td>
<td>X0,000</td>
<td>$$$$</td>
<td>Medium</td>
</tr>
<tr>
<td>Enterprise</td>
<td></td>
<td>X,000</td>
<td>$$$$$$</td>
<td>High</td>
</tr>
</tbody>
</table>

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
SP Managed Services

Protecting Your Customers

- Critical infrastructure
  - Amazon, Rackspace, Windows Azure, etc.
- Business apps
  - Salesforce, Office 365, DocuSign, etc.
- Branch office
- Roaming laptops
- Workplace desktops
- IoT devices
Cisco Umbrella & Managed Security

- High Security Efficacy - Prevents access to malware sites, Contains infections by blocking control (C2) traffic, threat intelligence updated worldwide in minutes.
- Cost effective for each offer
- Device / Application / Port Agnostic
- High Availability – 100% since 2006
- Network friendly – no overhead and reduces malicious traffic on network
- Improved user experience – faster page load
- Network enabled – SP controlled access to Security based on subscribed services
- Fast TTM – minimal integration, leverages existing standards based approach to enable all functionality, easy to manage
- Highly scalable – 1 to x0,000,000’s devices
Our view of the internet

100B requests per day
85M daily active users
12K enterprise customers
160+ countries worldwide

Our efficacy

Discover 3M+ daily new domain names
Identify 60K+ daily malicious destinations
Enforce 7M+ malicious destinations while resolving DNS
Intelligence
Statistical models

Co-occurrence model
Identifies other domains looked up in rapid succession of a given domain

Natural language processing model
Detect domain names that spoof terms and brands

Spike rank model
Detect domains with sudden spikes in traffic

Predictive IP space monitoring
Analyzes how servers are hosted to detect future malicious domains

Dozens more models

2M+ live events per second
11B+ historical events

Cisco Umbrella
Cisco Umbrella GTM

- Integrates into existing sales motions – telesales, kiosks, higher end security sales etc.
- Simple to explain, deploy and manage
- Personalized ‘SP’ user experience
- Minimal infrastructure investment – focus investment on marketing & branding
- Establish brand for network enabled security – safer Internet, managed security
- Introduce as first layer of security - creating upsell opportunities around SMB & Enterprises
It’s ok to point
Sample Cisco Umbrella Integrations

- ISR 4k family
- Cisco Wireless WLC family
- Cisco MPC
- Jasper

Cisco Umbrella Control Center
Branch Security at the DNS Layer: Cisco 4000 Series ISRs and Umbrella

- **Advanced Threat Detection**
  - DNS: First layer of defense
  - Worldwide visibility
  - Advanced research and threat intelligence

- **Apply Policies**
  - Select from predefined policies
  - Automated deployment
  - Optimized for any port, IP address, or application

- **Automate Your Security**
  - Order
  - Cloud provision
  - Protect

- **Digitization Driving Business**
  - Easy to deploy
  - Streamline business operations
  - Dramatically reduce TCO
  - Improve customer experience

Protecting the Branch
Network Security is Integral to Digitization

Cisco Umbrella helps secure the enterprise

Block current and emerging threats
Protect any device on network against:
  • Malware
  • Phishing
  • Command and Control (C2) callbacks for data exfiltration

Web content policy based on:
  • SSID
  • User Role
  • Location

Domain filtering
  Custom whitelist and blacklist

Cloud-delivered
Protection in minutes
Policies for guests and corporate users
Powerful reporting and analytics

Simple to deploy and manage
DEMOs

- Circuit Attach
- MPC attach
- ISP / MSSP
SMB : Circuit Attach Offer
<table>
<thead>
<tr>
<th>Category</th>
<th>Allowed</th>
<th>Blocked</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>1,201</td>
<td>5,169</td>
<td>6,370</td>
<td>3.23%</td>
</tr>
<tr>
<td>Prevent</td>
<td>1,193</td>
<td>4,466</td>
<td>5,659</td>
<td>2.87%</td>
</tr>
<tr>
<td>Malware</td>
<td>39</td>
<td>4,466</td>
<td>4,505</td>
<td>2.28%</td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>56</td>
<td>0</td>
<td>56</td>
<td>0.03%</td>
</tr>
<tr>
<td>Newly Seen Domains</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Potentially Harmful</td>
<td>788</td>
<td>0</td>
<td>788</td>
<td>0.40%</td>
</tr>
<tr>
<td>DNS Tunneling VPN</td>
<td>310</td>
<td>0</td>
<td>310</td>
<td>0.16%</td>
</tr>
<tr>
<td>Contain</td>
<td>8</td>
<td>703</td>
<td>711</td>
<td>0.36%</td>
</tr>
<tr>
<td>Botnet</td>
<td>6</td>
<td>550</td>
<td>556</td>
<td>0.28%</td>
</tr>
<tr>
<td>Phishing</td>
<td>2</td>
<td>153</td>
<td>155</td>
<td>0.08%</td>
</tr>
<tr>
<td>Categories</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Destination Lists</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>PURIFIED</td>
<td>190,811</td>
<td>-</td>
<td>190,811</td>
<td>96.77%</td>
</tr>
<tr>
<td>Total</td>
<td>192,012</td>
<td>5,169</td>
<td>197,181</td>
<td>100.00%</td>
</tr>
</tbody>
</table>
Consumer / Business : Mobile Network Security Offer
Evolve or start now with full MSSP capabilities

MSSP organization
- Centralized settings
- MSP admins
- Centralized reports

IOC
- Umbrella Investigate
  - Intelligence to stop threats earlier
- Your current security stack
  - Integrations to amplify existing security
- MSSP threat analysis and intelligence
  - Maintain your intellectual property secret

Cisco Umbrella
MSSP OFFER

MSSP organization

Centralized settings  |  MSP admins  |  Centralized reports

Customer 1

Subscription  |  Admin and settings  |  Reports

Customer n

Subscription  |  Admin and settings  |  Reports
Visibility and protection for all activity, anywhere

Umbrella

- HQ
- IoT
- Mobile
- Branch
- Roaming

All office locations
Any device on your network
Roaming laptops
Every port and protocol

ALL PORTS AND PROTOCOLS
Leverage our APIs to enforce your intelligence

Protect your customers while keeping your intellectual property secret

MSSP threat analysis and intelligence

- Intel uncovered by your teams remains your secret sauce

Umbrella enforcement and visibility

- **Automatically push** newly discovered malicious domains via API
- **Logs or blocks** all internet activity destined to these domains
- **Isolated** only used for your customers — no inspection or leakage
Investigate: the most powerful way to uncover threats

Key points

- Intelligence about domains, IPs, and malware across the internet
- Live graph of DNS requests and other contextual data
- Correlated against statistical models
- Discover and predict malicious domains and IPs
- Enrich security data with global intelligence

domains, IPs, ASNs, file hashes

Console

SIEM, TIP
Easiest security product you’ll ever deploy

1. Signup
2. Point your DNS
3. Done

Umbrella
Start blocking in minutes
Data centers co-located at major IXPs

25 data centers worldwide
Integrations to amplify existing security
Block malicious domains from partner or custom systems

YOUR CURRENT SECURITY STACK

- Appliance-based detection
  - FireEye + Others
- Threat intelligence platform
  - ANOMALI + Others
- Threat analysis feed
  - AMP Threat Grid + Others
- Custom integrations
  - Python Script Bro IPS + Others

Cisco Umbrella
Co-occurrence model
Domains guilty by inference

Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe.

Possible malicious domain
Known malicious domain
Possible malicious domain

Cisco Umbrella

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
IP geo-location analysis

Host Infrastructure
Location of the server
IP addresses mapped to domain

Hosted across 28+ countries

DNS Requesters
Location of the network and off-network device
IP addresses requesting the domain

Only US-based customers requesting a .RU TLD
PhishTank

Internet's largest clearinghouse of data about phishing scams
Our cloud platform

- 25 data centers located at major IXPs
- 500+ partnerships with top ISPs and CDNs
- 100% uptime since 2006 with DDoS protection and global failover
Spike rank model
Patterns of guilt

Massive amount of DNS request volume data is gathered and analyzed

DNS request volume matches known exploit kit pattern and predicts future attack

y.com is blocked before it can launch full attack
MPC Attach Security Service

- Customer can subscribe to service as in ‘opt in’ or be delivered as an ‘opt out’ service
- Service can be Enterprise and / or Consumer focused
- On service activation, external DNS traffic now screened – phishing, malicious sites, C&C
- Violations – can be flagged on customer device (if appropriate)
- Capability to generate Monthly Network Stats to be sent to each Customer to demonstrate value of security provided by Operator
- No client on end device with improved battery utilization and faster responses for browsing
- Malware traffic dramatically lowered on network and DNS infrastructure savings
Addressing Mobile Networks: New Challenges

- Operate at scale (x0,000,000s devices)
- Easy to deploy and require minimal intervention / infrastructure upgrades by Mobile Operator
- Minimal impact to end user experience – latency / usability / battery life / service availability
- Independent of device type
- Network friendly – minimize overhead / reduce resource usage on the network and control infrastructure
- High security efficacy and cannot be bypassed and be available worldwide
- Cost Effective
- Strengthen the Mobile Operator’s brand