SMB Security Service Offerings
Growing SMB Revenue with Bundled Security Offers

Alex Foster, John Malzahn & Darryl Clarke (Encapto)
SP Channel Service Creation
May 29, 2018
Agenda

• Market Overview & Examples

• Offer Overview

• Meraki, Umbrella & Cloud Security Platforms

• Encapto Platform for SP Customization & Differentiation
Large Opportunity in SMB Driven by Number of Sites and Employees, Heavy Concentration in Sub 250 Space

<table>
<thead>
<tr>
<th>Employees</th>
<th>WW</th>
<th>USA</th>
<th>CAN</th>
<th>MEX</th>
<th>UK</th>
<th>GER</th>
<th>FRA</th>
<th>JPN</th>
<th>AUS</th>
<th>IND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large SMB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>250–999 Employees</td>
<td>321</td>
<td>30</td>
<td>8</td>
<td>6</td>
<td>5</td>
<td>9</td>
<td>4</td>
<td>10</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Mid-Market SMB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20–249 Employees</td>
<td>6,239</td>
<td>828</td>
<td>124</td>
<td>76</td>
<td>123</td>
<td>140</td>
<td>136</td>
<td>310</td>
<td>39</td>
<td>449</td>
</tr>
<tr>
<td>Small SMB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5–19 Employees</td>
<td>25,756</td>
<td>2,203</td>
<td>288</td>
<td>170</td>
<td>348</td>
<td>735</td>
<td>412</td>
<td>636</td>
<td>156</td>
<td>1,408</td>
</tr>
<tr>
<td>Total SMB</td>
<td>32,316</td>
<td>3,061</td>
<td>420</td>
<td>252</td>
<td>476</td>
<td>884</td>
<td>552</td>
<td>956</td>
<td>197</td>
<td>1,867</td>
</tr>
</tbody>
</table>

33% of networking TAM and 26% of security TAM are in 20–250 segment

31% of all U.S. employees are employed in 20–250 segment and 48% in the E.U. SMEs (10–250)

Source: AMI SMB report, EU data
SMBs Have Same Security Challenges as Large Enterprises . . . But Fewer Resources

Small Business Cyberattacks

61%
Experienced cyber attack in past 12 months

Inability to Keep Up with Latest Technology

67%
insufficient security personnel

Proliferation of Malware and Threats

52%
experienced ransomware in past 12 months

Complexity of Security Solutions

54%
experienced a data breach

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Overwhelming SMB Preference to Purchase Network-related services from SP

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Network Service Provider</th>
<th>Direct from Vendor</th>
<th>Value Added Reseller</th>
<th>Local Consultant</th>
<th>Don’t Want Managed</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed WiFi</td>
<td>67%</td>
<td>9%</td>
<td>8%</td>
<td>6%</td>
<td>7%</td>
<td>4%</td>
</tr>
<tr>
<td>Managed LTE/4G Backup</td>
<td>53%</td>
<td>13%</td>
<td>16%</td>
<td>6%</td>
<td>8%</td>
<td>5%</td>
</tr>
<tr>
<td>Managed Network Security</td>
<td>49%</td>
<td>18%</td>
<td>11%</td>
<td>9%</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>Managed Web and Email Security</td>
<td>46%</td>
<td>18%</td>
<td>14%</td>
<td>9%</td>
<td>7%</td>
<td>6%</td>
</tr>
</tbody>
</table>

N = 1000 20–250 employee SMBs in U.S.
Cloud Enabled Solutions are Shifting SMBs Requirements

**SMBs Dependency to Access Business Productivity Solutions in the Cloud**

- Very Dependent: 46%
- Dependent: 45%
- Not Dependent: 7%
- Other: 7%

**SMBs Tendency to Switch Providers when Managed Services are not available**

- Very Likely: 34%
- Likely: 40%
- May Consider: 19%
- Other: 7%

82% of respondents expects technology solutions to be bundled with other managed service offerings from a single Managed Service Provider.

*Source: Cisco Proprietary US Survey Study, June 2017, n=1000*
SP SMB Security Services
Cloud Managed Security Solutions for SMB

24x7x365 operations

1.6 million global sensors

100 TB of data received per day

150 million+ deployed endpoints

35% worldwide email traffic

Cisco Talos Threat Intelligence

SP SOC

SP Dashboard

User: customer@serviceprovider.com
Pass: ****************

Log In

Meraki Umbrella
Cisco Cloud Email Security
Cisco AMP

Network

Endpoint

Cloud

Services
Joint Service Delivery

Cisco Responsibilities
- Operate Cisco cloud services
- Health of the cloud services
- Resolution of problems in the cloud services
- SLA related to Cisco cloud services
- Provide access to portal and APIs
- Usage data to SP

Cisco Cloud-managed Security

SP Dashboard

SP Responsibilities
- Sales, GTM, pricing, billing
- Service definition, SLA
- Customer portal, OSS/BSS
- SOC Operation
- Policy and enforcement
- Monitoring and management
- Level 1 customer support
Expand Your SMB Security Service Offerings and Revenue

Simple IT for SMBs
Powered by Cisco Meraki, Umbrella, CES, AMP

- Connectivity/Broadband
- Secure Business Broadband
- Secure Business Wi-Fi
- UTM with SD-WAN
- Advanced Threat, Ransomware Protection
Cloud based Security Offers Positioning

Cisco Solutions

- Umbrella Easy Protect
- Umbrella WLAN
- Umbrella MSSP
  CES, AMP4E, StealthWatch Cloud
- Umbrella MSSP
  Meraki UTM with AMP
- CSP Clean Internet
- Secure WiFi
- CSP Clean Internet
- Secure WiFi/UTM
- MSSP
  Managed Endpoints Security
  Managed Advanced Network Security

SP/MSSP offers

MSP/VAR Managed Office IT/Security Packages

Target Customers

- SOHO
- SMB
- Enterprise Like SMB
- Mid/Enterprise

CSP = Communication Service Provider, MSSP = Managed Security Service Provider. MSP = Managed Service Provider
Simplifying IT with cloud management

- A complete cloud managed IT solution
- Wireless, switching, security, SD-WAN, communications, EMM, and security cameras
- Integrated hardware, software, and cloud services
- Leader in cloud managed IT
- Among Cisco’s fastest growing portfolios
- Over 200,000 unique customers
- Over 3 million Meraki network devices online
A complete connectivity and threat management solution

Security
Next generation firewall
AES encrypted VPN
Intrusion prevention (IPS)
Malware protection
Geo-IP firewalling

Networking
3G / 4G failover
Branch routing
WAN balancing and failover
High Availability
Intelligent path control

Application Control
Bandwidth shaping
URL content filtering
Quality of Service control
Why service providers choose the Cisco Meraki MX

Powerful security that’s easy to implement
- Robust suite of Cisco Security technologies
- Intuitive GUI-based configuration
- Seamless updates from the cloud

Exceptional scalability
- Zero-touch provisioning with cloud brokered VPN
- Easy centralized management with built-in remote troubleshooting tools
- Multi-location configuration templates

Industry-leading visibility
- Fingerprints users, applications, devices, and threats
- Monitor one location or an entire deployment
- Unified monitoring and reporting with other Cisco Meraki technologies
# Ironclad security

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Generation Firewall</td>
<td>Application aware firewalling</td>
</tr>
<tr>
<td>Intrusion Prevention (IPS)</td>
<td>Based on Cisco Snort</td>
</tr>
<tr>
<td>URL Content Filtering</td>
<td>With over 80 categories and over 4 billion categorized URLs</td>
</tr>
<tr>
<td>Geo-based security</td>
<td>Allow or block traffic by country</td>
</tr>
<tr>
<td>Malware Protection</td>
<td>Cisco AMP and Threat Grid</td>
</tr>
<tr>
<td>Automatic updates</td>
<td>Software and security updates delivered from the cloud</td>
</tr>
<tr>
<td>PCI compliance</td>
<td>PCI 3.2 certified cloud management backend</td>
</tr>
</tbody>
</table>
Umbrella Offers for SMB

### Umbrella Easy Protect
*(First Layer defense for clean Internet)*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Per customer</td>
</tr>
<tr>
<td>Number of users</td>
<td>Up to 25 users</td>
</tr>
<tr>
<td>DNS Security</td>
<td>Malware, C2, phishing, potential harm domain</td>
</tr>
<tr>
<td>Policy</td>
<td>One global policy</td>
</tr>
<tr>
<td>Destination Lists</td>
<td>White / Black</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Per site/IP</td>
</tr>
<tr>
<td>Category Filtering</td>
<td>No</td>
</tr>
<tr>
<td>S3 Bucket for logs</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Support</td>
<td>7 x 24</td>
</tr>
</tbody>
</table>

### Umbrella WLAN
*(Protect WiFi Internet access AP)*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Per customer</td>
</tr>
<tr>
<td>DNS Security</td>
<td>Malware, C2, phishing, potential harm domain</td>
</tr>
<tr>
<td>Policy</td>
<td>Per network / global policies</td>
</tr>
<tr>
<td>Destination Lists</td>
<td>White / Black</td>
</tr>
<tr>
<td>Category Filtering</td>
<td>Yes</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Per SSID</td>
</tr>
<tr>
<td>S3 Bucket for logs</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Support</td>
<td>7 x 24</td>
</tr>
</tbody>
</table>

1. Web based attack is #1 for SMB (Based on Source: web-based-attack-smb)
Meraki MX - UTM for Secure Office

Integration with simplicity

- **Basic**
  - Managed firewall
  - Site-to-site VPN
  - Remote access VPN

- **Enhanced**
  - UTM (application firewall, VPN, IPS, Antivirus, content filtering)

- **Premium**
  - UTM and AMP
  - SD-WAN
Secure Office 365 with CES

Gartner estimates that 13% of companies are using cloud mailbox services today, but will increase to 60% by 2022.
## Secure Email for SMB

<table>
<thead>
<tr>
<th>Feature</th>
<th>Standard</th>
<th>Advanced</th>
<th>Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound email security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Outbound email security</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>On-Prem and Cloud Email (O365, Gmail)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anti-spam, anti-phishing, anti-virus</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>URL filtering</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AMP</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DLP</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SP predefined global policies</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Per customer reporting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
AMP4E MSSP Service Tiers

- **Premium**
  - PC + MAC + Android + iOS*
  - Customized Outbreak control
  - Self management
  - Threat analysis
  - Weekly summary + deployment summary + vulnerability report

- **Advanced**
  - PC + MAC + Android
  - Customized Outbreak control
  - Self management
  - Weekly summary + deployment summary report

- **Standard**
  - PC + MAC + Android
  - Pre-defined Outbreak control
  - Weekly summary report

*For customers without security admin staff

For customers with security admin staff

For customers without security admin staff
Ransomware Protection Suite

- COMPROMISED SITES AND MALVERTISING
- PHISHING SPAM

Web link
Web redirect

- Angler
- Nuclear
- NuTrino

Email attachment

Malicious Infrastructure
File drop

Encryption Key Infrastructure

RANSOMWARE PAYLOAD

- Blocked by Cisco Cloud Email Security with AMP
- Blocked by Cisco Umbrella Roaming (DNS Security)
- Blocked by Cisco AMP for Endpoints (Host Anti-Malware)
Encapto MSM
Managed Service Creation for SPs
MANAGED SERVICES TODAY

Managed Services comprise multiple specialist products, from multiple vendors that are often delivered to customers as is, and are somewhat unpalatable to the SMB:

- Multiple management interfaces, one for each service:
  - Too complex and requires a call to SP helpdesk for simple tasks
  - Inability to extend management access as too dangerous
- Lack of self management by the SMB
- Untailored to diverse customer profiles and often overly complex for the SMB skillset
- Undifferentiated in packaging as opposed to a single indispensable product
SERVICE CREATION

Network orchestration tools, integration with third party services, advanced user permissions, and custom interfaces make building complete managed service products for target markets simple.

- API encapsulation allows cherry picking of key functions from almost any vendor solution
- Templating of services for replay at scale
- Apply user permissions for specific resource access
- Vertical specific interface “just right” for the customer type
- Plug and go - default settings deliver a ready to run service as defined by SP
RAPID, FLEXIBLE ORCHESTRATION

Shorter time to market gives SPs a key competitive advantage. The Encapto Orchestrator automates customer, hardware & services provisioning at massive scale to slash time, costs, and errors.

- Customer order captured via SPs website to commence provisioning process
- Encapto receives customer order with service template type
- Encapto provisions new customer services via API calls to external vendors cloud or systems
- Customer receives hardware and services, follows a Quick Start Guide to connect hardware
- Default service setup - Out-of-the-box for SMBs less inclined to configure
To cater for particular market segments, Encapto powered hybrid products typically involve five components, namely:

a) selections of features from a portfolio of specialist products and services,

b) user interfaces that are tailored for niche requirements of diverse customer profiles,

c) existing SP systems such as BSS and OSS,

d) staff user interfaces that are tailored for helpdesk and reporting requirements, and

e) standardised single sign-on authentication portals for SP staff and customers.