Increasing Recurring Revenue with Cisco-Based Cloud Managed Security Offers

Cisco Knowledge Network
February 11, 2020

Ted Donat, *SP Product Management Lead
Sachin Gorde, *SP Technical Solutions Architect
Agenda

Welcome
Opportunity and growth drivers
Security leadership
Managed security solutions
Profit and grow with Cisco
How to get started
Opportunity and growth drivers
MSSP Market Segmentation

- **Communications Service Providers (CSPs)**
  - Tier 1
  - Tier 2 & 3

- **IT Service Providers (ITSPs)**
  - Global Managed Service Providers / Strategic Integrators
  - Regional Managed Service Providers / Strategic Integrators
  - Pure-Play MSSPs
  - Managed Detection & Response (MDR) Providers

- **Value Added Resellers (VARs)**
  - D-VARs
  - Resellers

- **Small and Medium Business**
  - MSPs
  - Distribution

$13.5B in estimated cloud opportunities as businesses shift to IaaS and SaaS models for speed and cost.

*SP

85% of Cisco’s business comes through partners like you.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Breaches increasing in frequency and scale

Reported breaches and records lost

Breaches
Records lost
Average records lost
(millions)


*2019 year to date
Source: Public sources
Threats encountered by the channel intensify

- Email spam: 83%
- Ransomware: 71%
- Phishing: 74%
- Malware: 72%
- Denial of service: 43%
- Insider threat: 29%
- Identity theft: 42%
- Info leakage: 38%
- Web attacks: 32%
- Botnets: 35%
- Crypto jacking: 28%
- Cyber espionage: 24%

Source: Candefero survey, 95 channel respondents, September 2019
Customers are under pressure, especially SMBs

- Complexity
- Speed
- Regulations
- Costs
- Ecosystems
- Skills
What’s on your mind?

Which vendors should I align with?

Which tools should I use?

How do I implement policies and controls?

How can I get more out of my security investments?
Security leadership
The dynamics of the SP market

$13.5 billion

in estimated cloud opportunities as businesses shift to IaaS and SaaS models for speed and cost.

Source: IHS Markit Report 2020

© 2020 Cisco and/or its affiliates. All rights reserved.
Cisco is investing in CLOUD security growth

*Source: Canalys estimates, Cybersecurity Analysis, March 2019
Cisco is a recognized leader in security
Stop global threats more effectively with integrated threat intelligence

Massive Volume
- 600 billion Email samples
- 1.5 million Daily malware samples
- 16 billion Daily web requests
- 3.4 billion AMP Queries

Unparalleled Expertise
- 300+ threat intel researchers; 24 – 7 – 365
- Over 100 Threat intelligence partners

Cloud – Public, Private
The cybersecurity vendor landscape is crowded

2,500+ vendors

Start ups +180 a year

Consolidation -150 a year

Source: Canalys estimates, Cybersecurity Analysis, September 2019
CSTA-Engineered integrations across the breadth of security
Multiple ways to partner

- Manage it myself
- Manage it together
- Manage it for me
Managed security solutions
Turning business needs into today’s technology

- Single Pane of Glass for operator & tenant
- Multi-tenant
- User Pricing & Automated Billing
- Hierarchical & Role Based Access Control
- Open Platform (API integration with OSS & BSS)
- Flexible Delivery Models
- One-Touch Provisioning & Orchestration
- Scalable Architecture Investment
Managed security services offers
Protection with reliable recurring revenue

Network
- Managed Next Generation Firewall (FTD)
- Managed UTM (Meraki MX)
- Secure Wifi (Meraki MR + Umbrella)
- Secure SD-WAN

Endpoint
- Managed Endpoint (AMP for Endpoints (A4E))
- Managed Email (Email Security Appliance)

Cloud
- Managed DNS Security (Umbrella MSSP, Easy Protect, Mobile Protect, Secure Internet Gateway)
- Managed Behavioral Analytics (Stealthwatch Cloud)
- Managed Email Security (SMP with ESAv)
Cisco security management platform – a white labeled platform for partners to manage and build a security business

**Interfaces**
- Tenant Hierarchy & Operator Portal with RBAC modules
- Integration Modules (Ordering, Billing)
- APIs

**Security Management Platform**
- Portal & Apps Service View Catalogue
- Customer Onboarding
- Orchestration & Provisioning
- Events, Monitor, & Reporting
- Log Export SIEM Feed
- Orchestration Support Services & Business Support Services

**Technology Modules**
- Email
- WSA

**Infrastructure**
- PaaS (AWS) or SP Managed Data Centers

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Cisco threat response
The unifying force powering Cisco’s integrated security architecture

Simple
Detect, investigate, and remediate across multiple integrated security technologies

Fast
Reduce time spent on security operations functions up to 85%*

Effective
Aggregate threat intelligence into immediate action

…and it’s FREE with existing Cisco Security licenses

*based on internal simulations
Threat response integrates across Cisco’s security platform

Included FREE with the following licenses

- Cisco AMP for Endpoints
- Cisco Umbrella
- Cisco Email Security
- Cisco Threat Grid
- Cisco Firepower

…and more integrations to come!
Poll Question 1
Umbrella has expanded to a full secure internet gateway

- Secure web gateway
- Cloud access security broker
- Cloud-delivered firewall
- Interactive threat intelligence
- DNS-layer security

Cisco Umbrella

Secure Internet Gateway

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Securing the Enterprise in the SDWAN and Cloud Era
Cloud migration opens floodgates to Wild Wild Web

Typical legacy Enterprise Architecture

Direct Internet Access Enterprise Architecture

Direct Internet Access for SaaS/IaaS opens new attack vector
<table>
<thead>
<tr>
<th>Customer Pain Point</th>
<th>Cisco Solution</th>
</tr>
</thead>
</table>
| SDWAN Distributes the attack surface | Small/SMB – MX and/or SIG  
Mid/Large – NGFW + IPS + UMB + AMP + TG + URL-F (Sec. SDWAN Stack) |
| • Distribute the security stack | AnyConnect for VPN  
UMB for DNS-Layer security  
AMP4E – Detect and protect  
DUO – Secure MFA access  
ISE – TrustSec and IAM |
| • Maintain same Security posture across Small/SMB – MX and/or SIG  
Mid/Large – NGFW + IPS + UMB + AMP + TG + URL-F (Sec. SDWAN Stack) | AnyConnect for VPN  
UMB for DNS-Layer security  
AMP4E – Detect and protect  
DUO – Secure MFA access  
ISE – TrustSec and IAM |
| Zero-Trust Network | UMB & CloudLock, WSA – Secure access, App Discovery & Control  
DUO for Authenticate, Authorize and enforce sec Posture  
FTD(v) with DDoS, AMP and Umbrella  
Tetration - Secure the workload / Applications |
| • Work-load moving to Cloud | UMB & CloudLock, WSA – Secure access, App Discovery & Control  
DUO for Authenticate, Authorize and enforce sec Posture  
FTD(v) with DDoS, AMP and Umbrella  
Tetration - Secure the workload / Applications |
| • SaaS | AnyConnect for VPN  
UMB for DNS-Layer security  
AMP4E – Detect and protect  
DUO – Secure MFA access  
ISE – TrustSec and IAM |
| • BYOD, Contractor, customer access | AnyConnect for VPN  
UMB for DNS-Layer security  
AMP4E – Detect and protect  
DUO – Secure MFA access  
ISE – TrustSec and IAM |
| Multi-Cloud | ON-Prem (ESA), Cloud-based (CES, SMP) with AMP, UMB  
Secure emails, remove malware, block unwanted access and exploits |
| • SaaS – authenticate and Authorize | Stealthwatch (Ent / Cloud) – Network-wide visibility 24/7 monitoring, ML based Alerting, 98% accuracy (reduce false +ve)  
CTR – Threat hunting and Remediation |
| • IaaS – security posture as on-prem | Stealthwatch (Ent / Cloud) – Network-wide visibility 24/7 monitoring, ML based Alerting, 98% accuracy (reduce false +ve)  
CTR – Threat hunting and Remediation |
| • Public + Private + On-prem DCs | Stealthwatch (Ent / Cloud) – Network-wide visibility 24/7 monitoring, ML based Alerting, 98% accuracy (reduce false +ve)  
CTR – Threat hunting and Remediation |
| Email | CDO for NGFW management (ASA, FTD, MX, ISR)  
vManage for secure SDWAN  
MSSP Portals for Umbrella, AMP4E, StealthWatch, SMP (email) |
| • Most exploited for Malware, Ransomware, Phishing | CDO for NGFW management (ASA, FTD, MX, ISR)  
vManage for secure SDWAN  
MSSP Portals for Umbrella, AMP4E, StealthWatch, SMP (email) |
| Regain the control | CDO for NGFW management (ASA, FTD, MX, ISR)  
vManage for secure SDWAN  
MSSP Portals for Umbrella, AMP4E, StealthWatch, SMP (email) |
| • 24/7 ML assisted monitoring and alerting | CDO for NGFW management (ASA, FTD, MX, ISR)  
vManage for secure SDWAN  
MSSP Portals for Umbrella, AMP4E, StealthWatch, SMP (email) |
| • Threat-hunting and Remediation | CDO for NGFW management (ASA, FTD, MX, ISR)  
vManage for secure SDWAN  
MSSP Portals for Umbrella, AMP4E, StealthWatch, SMP (email) |
| Management | CDO for NGFW management (ASA, FTD, MX, ISR)  
vManage for secure SDWAN  
MSSP Portals for Umbrella, AMP4E, StealthWatch, SMP (email) |
| • Easy to manage multiple different components | CDO for NGFW management (ASA, FTD, MX, ISR)  
vManage for secure SDWAN  
MSSP Portals for Umbrella, AMP4E, StealthWatch, SMP (email) |
| • Cross components analytics/investigation | CDO for NGFW management (ASA, FTD, MX, ISR)  
vManage for secure SDWAN  
MSSP Portals for Umbrella, AMP4E, StealthWatch, SMP (email) |
## Secure Enterprise - Sample Offer Matrix

<table>
<thead>
<tr>
<th></th>
<th><strong>Basic</strong> (Legacy-equivalent)</th>
<th><strong>Enhanced</strong> (mitigate evolved threats)</th>
<th><strong>Ultimate</strong> (Comprehensive futuristic protection)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SDWAN</strong></td>
<td>DNA Advantage</td>
<td>DNA Advantage + UMB (SIG) Insight (Essential) WSA (for OnPrem)</td>
<td>DNA Premier (incl. UMB, TG, StealthWatch) + UMB (SIG) WSA (for OnPrem)</td>
</tr>
<tr>
<td><strong>End-Point (mobile user)</strong></td>
<td>AMP4E, UMB Insights, Anyconnect*, DUO (MFA)</td>
<td>AnyConnect* + Umbrella Advantage, AMP4E Connector, DUO (Access)</td>
<td>AnyConnect* + Umbrella connector, AMP4E Connector, DUO (Beyond)</td>
</tr>
<tr>
<td><strong>Multi-Cloud</strong></td>
<td>FTD(v)</td>
<td>FTD(v) + AMP + UMB + Stealthwatch Cloud</td>
<td>NGFW + AMP + UMB + TG + DDoS StealthWatch Cloud + Tetration + ISE</td>
</tr>
<tr>
<td><strong>Visibility and Control in Cloud (SaaS/Apps)</strong></td>
<td>SMP Email Security (ESAv)</td>
<td>SMP Email Security ESAv</td>
<td>SMP Email Security (ESAv), CES CASB</td>
</tr>
</tbody>
</table>

* ASAv for AnyConnect Terminations
## Security Needs Vary per Use-case/Profile/Cost

<table>
<thead>
<tr>
<th></th>
<th>Basic (Legacy-equivalent)</th>
<th>Enhanced (mitigate modern threats)</th>
<th>Ultimate (Comprehensive Protection)</th>
</tr>
</thead>
</table>
| Same security level as prior to SDWAN and cloud transition | • Firewall  
• Application Control  
• URL Filter  
• IPS  
• Network AV  
• MFA  
• Remote Access | • Firewall  
• Application Control  
• URL Filter  
• IPS  
• Network AV  
• MFA  
• Remote Access | • Firewall  
• Application Control  
• URL Filter  
• IPS  
• Network AV  
• MFA  
• Remote Access |
| Modern Threat Protection | • Phishing/Ransomware  
• DLP  
• BYOD – Device security posture  
• 24/7 visibility and alerting | • Phishing/Ransomware  
• DLP  
• BYOD – Device security posture  
• 24/7 visibility and alerting | • Sandbox  
• CASB  
• Workload security  
• ETA/CTA**  
• Security Posture enforcement (MDM) |
<p>| Complete security solution to address zero-trust, modern threats, multi-cloud transitions |                         |                                    |                                    |</p>
<table>
<thead>
<tr>
<th>Offer</th>
<th>Solution Components</th>
<th>Customer profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Duo MFA</td>
<td>SMBs, Doctors/Dentist office, mom-pop shops</td>
</tr>
<tr>
<td></td>
<td>Umbrella Essentials AMP4E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AMP4E</td>
<td></td>
</tr>
<tr>
<td>Enhanced</td>
<td>DUO Access</td>
<td>Small and Mid enterprise branches</td>
</tr>
<tr>
<td></td>
<td>Umbrella Advanced AMP4E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AMP4E</td>
<td></td>
</tr>
<tr>
<td>Ultimate</td>
<td>Duo Beyond</td>
<td>Finance, Healthcare, Gov, Defense, Large Enterprise</td>
</tr>
<tr>
<td></td>
<td>Umbrella SIG AMP4E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AnyConnect</td>
<td></td>
</tr>
</tbody>
</table>
Managed SD-WAN Leads to Managed Firewall
Managed services license agreement (MSLA)

- Initial three-year term
- Accommodates reuse and upgrades
- Greater licensing flexibility
- Utility pricing with monthly postpaid billing
- Shared risk with lower barrier to entry

A Utility-Based Buying Program - Shared Risk, Shared Success
Poll Question
Cisco Managed Detection and Response (MDR) can detect and respond to potential security threats with response actions that can protect your most critical assets and shield your organization from the high costs of a security breach.
Cisco Managed Detection and Response (MDR)

- Expert team of researchers, investigators, and responders
- MDR Threat Intelligence and Automation Platform
- Defined investigations and response playbooks
- Integrated security architecture and automation
- Customer portal
- Talos® incident response

Stealthwatch® Cloud
AMP for Endpoints
Threat Grid
Umbrella™
Profit and grow with Cisco
Our *SP partner strategy

Partnering with SPs to deliver business outcomes

- **Grow Revenue**: Make money through compelling B2B services
- **Reduce Costs**: Save money by reducing complexity and automating operations
- **Mitigate Risk**: De-risk the business with trust, security, support, and financial breadth
Value of driving integrated services together

**Innovation Rates**
Drive rapid offer releases and feature velocity

**Drive Acquisition**
Differentiate from connectivity competitors with business outcome-focused conversation

**Accelerate Sales**
Joint GTM with proven digital marketing and dedicated sales resources

**Increase Margins**
Low-friction sale, deployment, management, and support
New incremental revenue to current customer base

**Increase Stickiness and Reduce Churn**
Simplify IT while providing valuable business insights and customer engagement capabilities, along with the latest security solutions
Three or greater services reduce churn by 75%
Cisco Cloud & Managed Services Program (CMSP)

Partner Levels

- Express
- Advanced
- Master

Partner Benefits

- Grow with incentives, promotions, and market development funds
- Reach new customers with marketing tools and resources
- Offer solutions that accelerate your customers’ digital transformation
Enabling your success

Your Practice

- Managed Services eBook
- Security Service Creation Playbook – Coming Soon
- SD-WAN Service Creation Playbook

Your Go to Market

- TruMethods vCIO ebook
- MSP University
- Secure SD-WAN Partner White Paper
- Firejumper Training

Ecosystem and Integrations
Get started

ebooks.cisco.com/story/managed
Poll Question
Questions?
Thank you!