



Cisco Community Live event

Portfolio de Segurança Cisco

Fabio Carneiro

CONSULTING SECURITY ENGINEER

18 de Junho, 2020

Novidades & Próximos eventos



Community Live Evento: Qualidade dos Serviços em Ambientes de Rede: da teoria à prática

Este evento ocorrerá na quarta-feira, 29 de Julho de 2020 às 2:00 pm (Brasília) / 6:00 pm (Lisboa) / 6:00 pm (Luanda)



JULHO 29, 2020

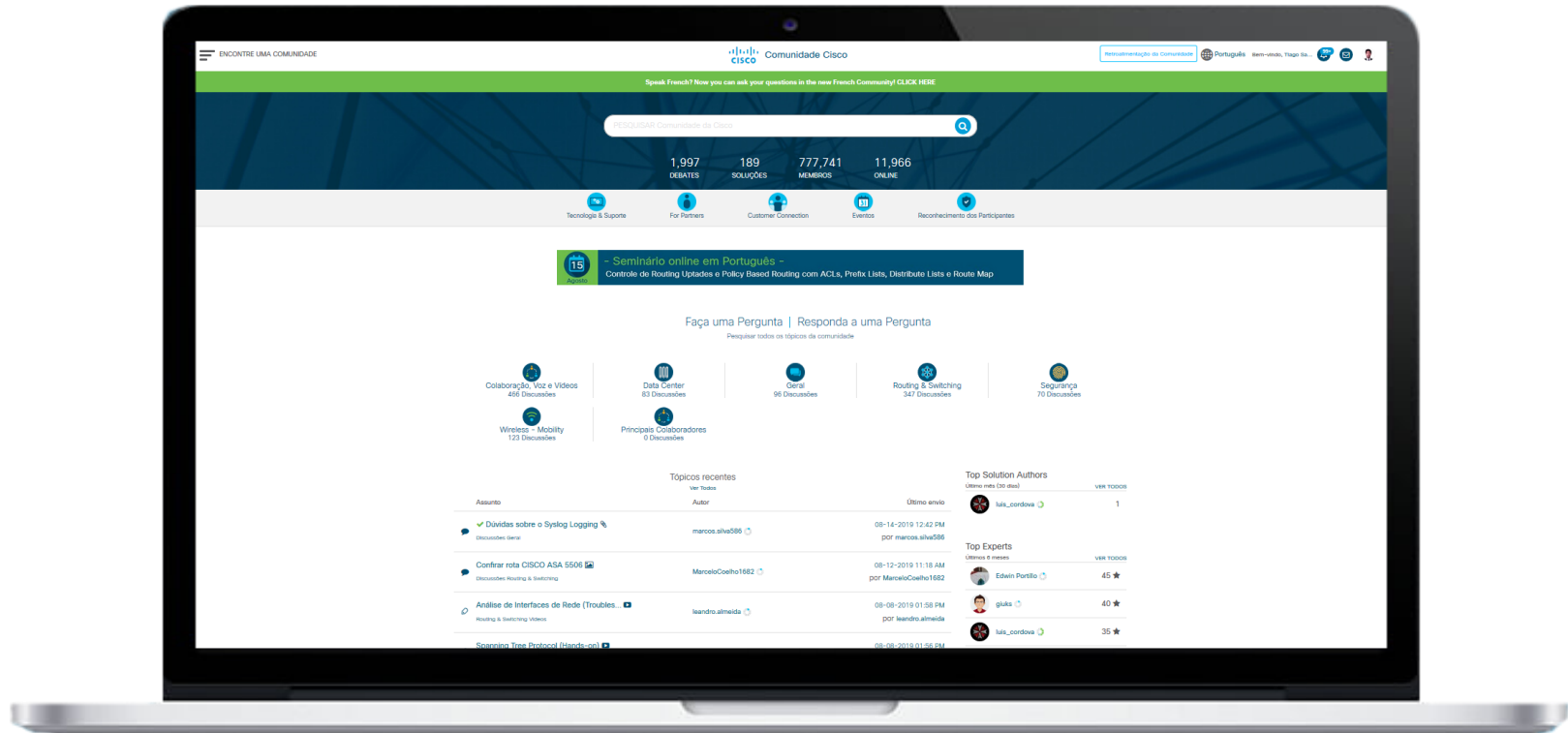
Community Live Evento
Apresentado por Olivia Braga

«Qualidade dos serviços em ambientes de rede: da teoria à prática»

The banner features a woman with glasses working in a server room. It includes a green checkmark icon, a date badge, the event title, the presenter's name, and a quote icon.

Faça sua [inscrição](#) para o evento Community Live Evento Qualidade dos Serviços em Ambientes de Rede: da teoria à prática.

Link: <https://bit.ly/qos0729>



<http://community.cisco.com>

Avalie os conteúdos publicados na Comunidade



Agradeça as pessoas que compartilham generosamente seus conhecimentos dentro da Comunidade dando um Kudo, ou seja, (clikando sobre a estrelinha).

Respostas

Blogs

Documentos

Eventos

Vídeos



Conheça o ranking dos membros com mais Kudos recebidos aqui:

<http://bit.ly/Cisco-Kudos>

Mostre que a sua dúvida foi resolvida!

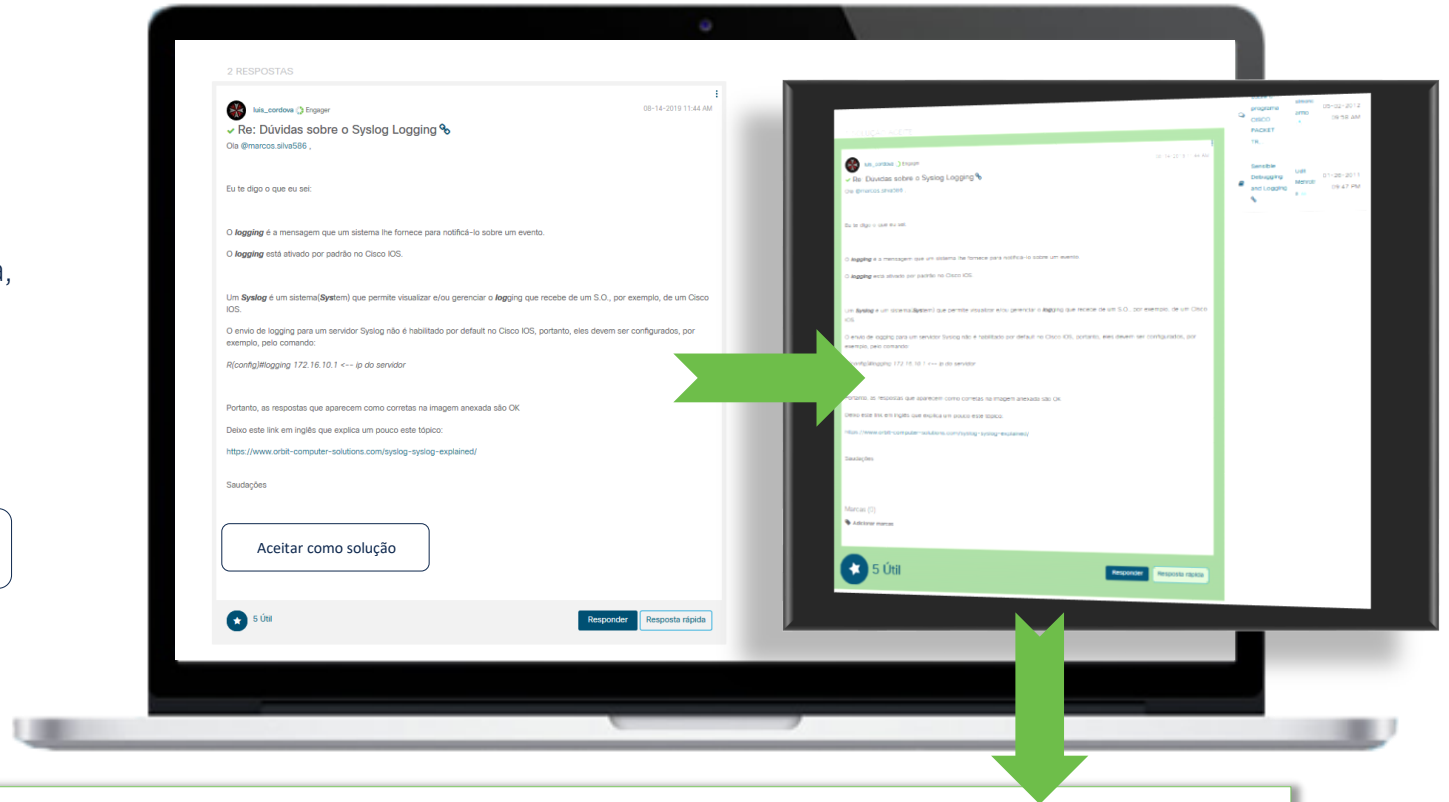
Embaixo de cada resposta se encontra o botão “Aceitar como solução”.

Se a resposta recebida resolve o seu problema, por favor faça como que todos saibam!

Simplesmente clique nesse botão:

Aceitar como solução

Aceitar como solução



Solucionado!

Especialista Convidado



Fabio Carneiro
Consulting Security Engineer



Question Manager



Nilton Maia
Consulting Security Engineer



Obrigado por
estar com a gente
hoje!



Link: https://bit.ly/Slides_1806

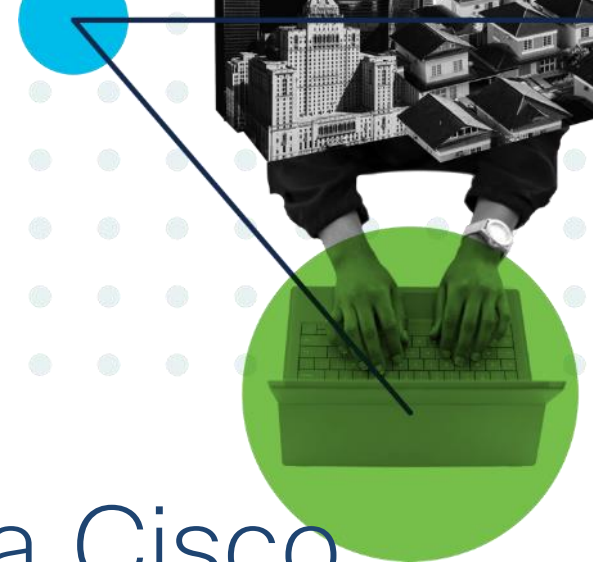
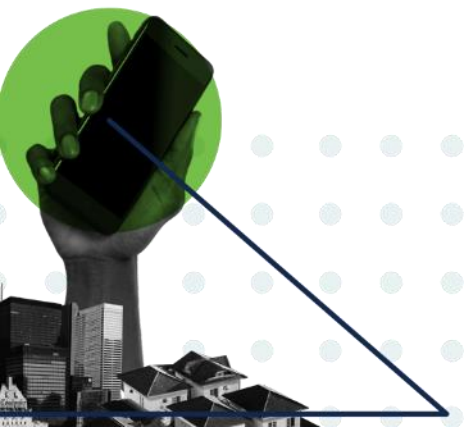
Publique as suas perguntas desde agora!

Use o painel de:
Perguntas & Respostas (Q&A) para
enviá-las.

Essas serão respondidas ao vivo
no final da apresentação pelo
especialista convidado.



Portfolio de Segurança Cisco



Agenda

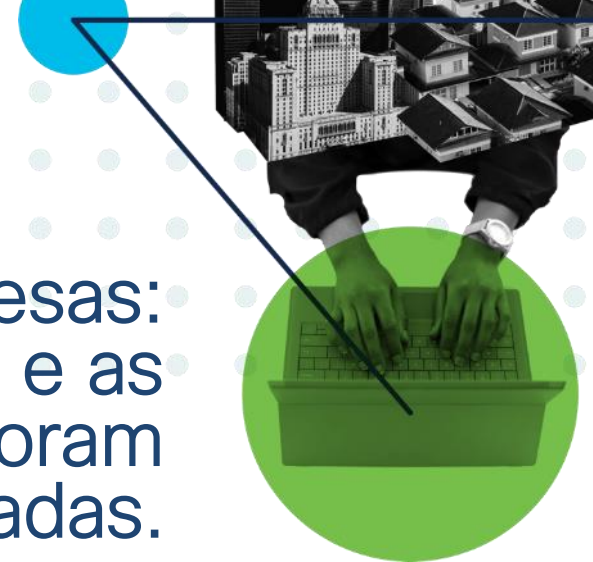
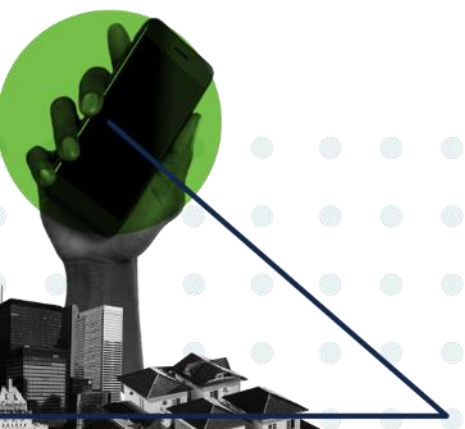
- História
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki

Agenda

- **História**
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki

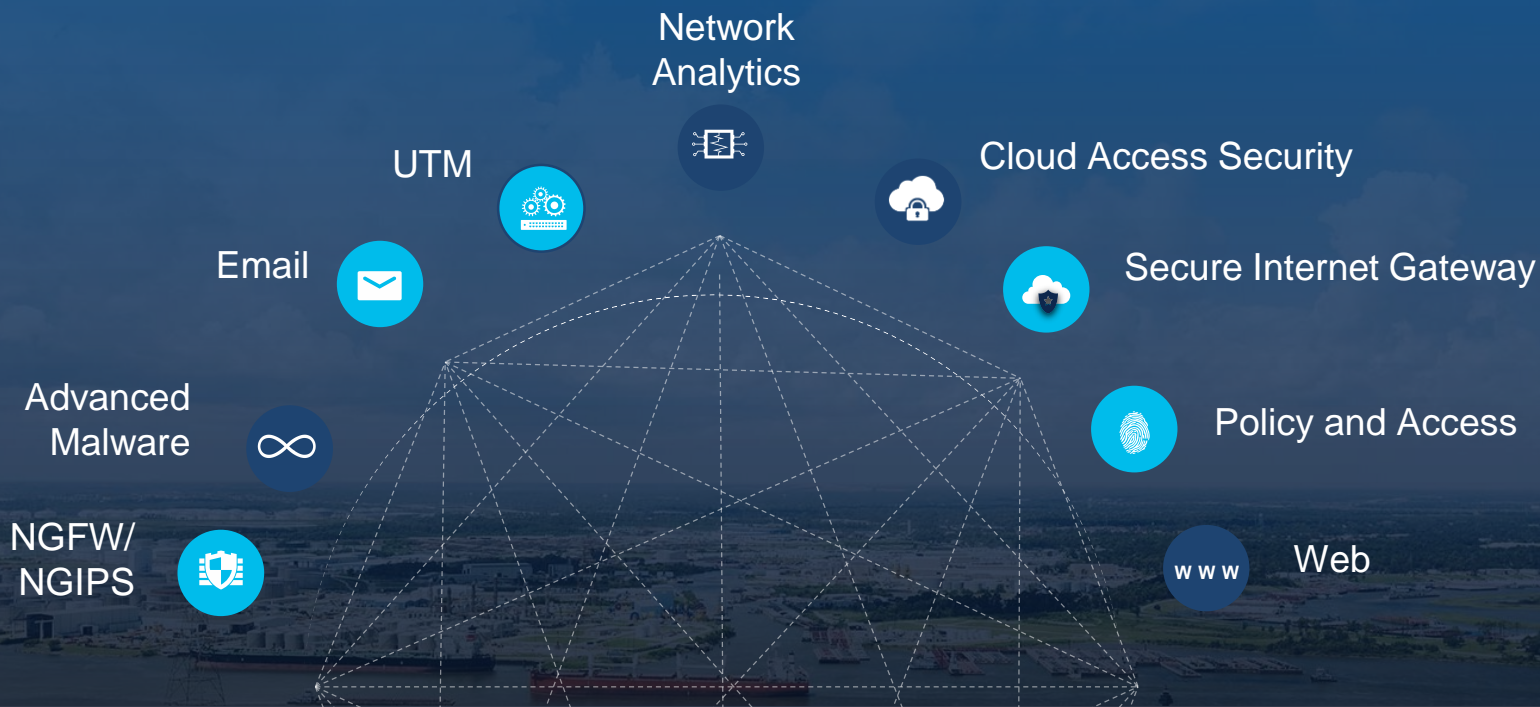
Existem dois tipos de empresas:
aquelas que foram hackeadas e as
que ainda não sabem que foram
hackeadas.

John Chambers
2015



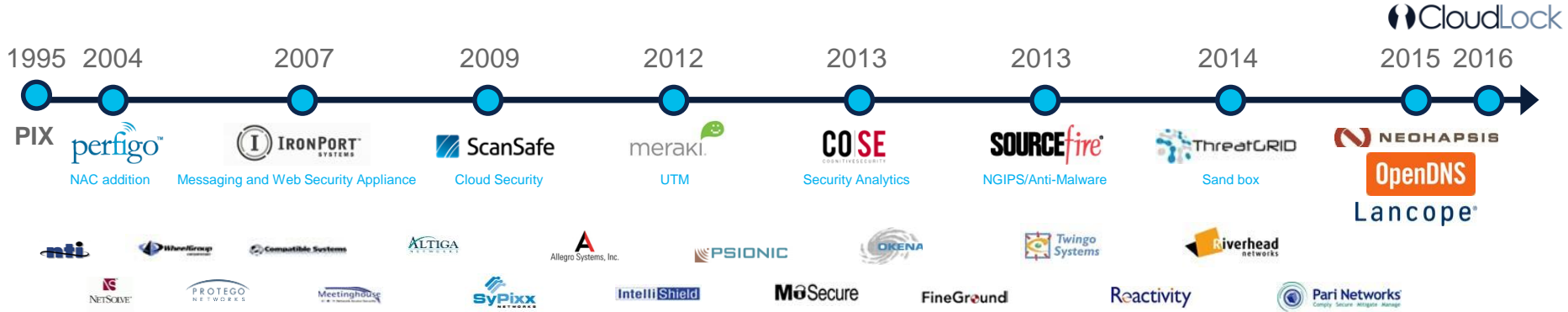
Premiere Portfolio in the Industry

Best of Breed and Integrated Architecture



Historia de aquisições

Em adição à Pesquisa e Desenvolvimento internos



Foram investidos mais de \$3.7B nos últimos anos

Security is Cisco's #1 priority. We are going big and making strategic investments to become our customers' and partners' most trusted security advisor.

*John Chambers, Executive Chairman, Cisco
April 2015*

Pergunta 1

- Você sabia que a Cisco possui um portfolio diversificado de soluções de Segurança?

A. SIM

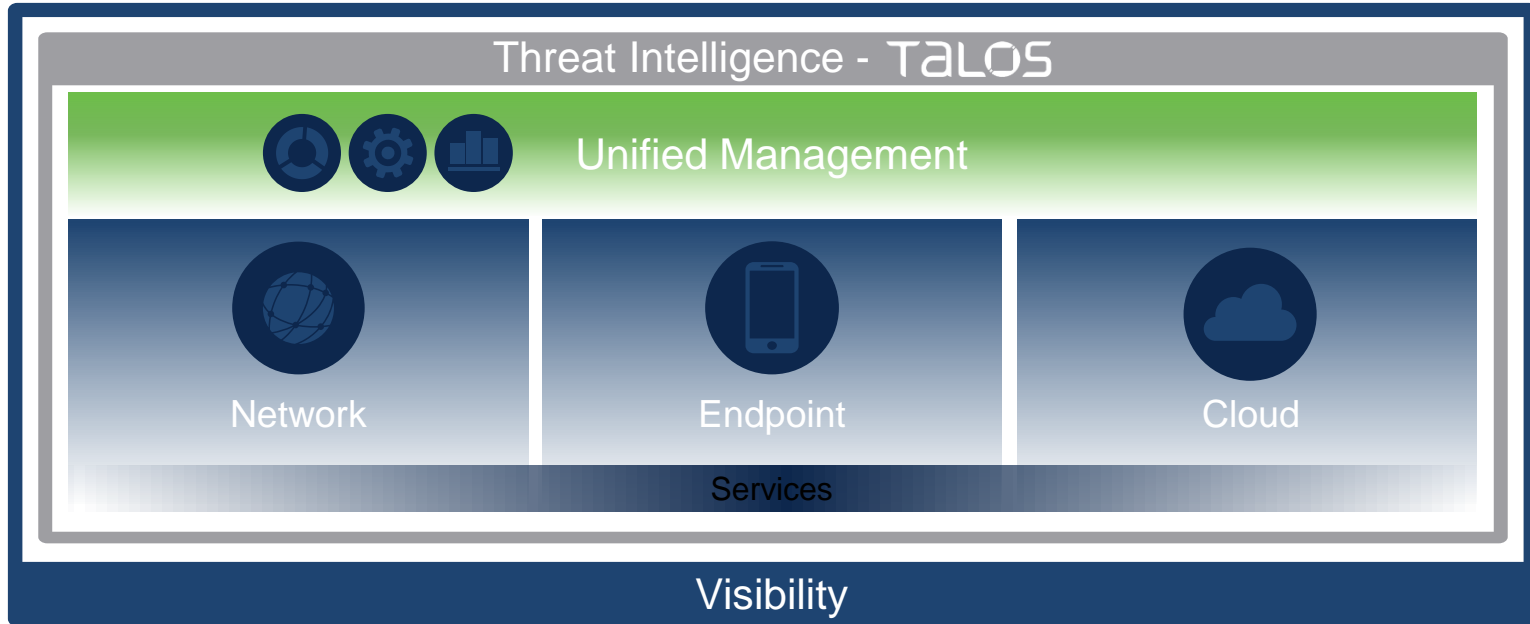
B. Já conhecia 1 ou 2 soluções

C. NÃO

Agenda

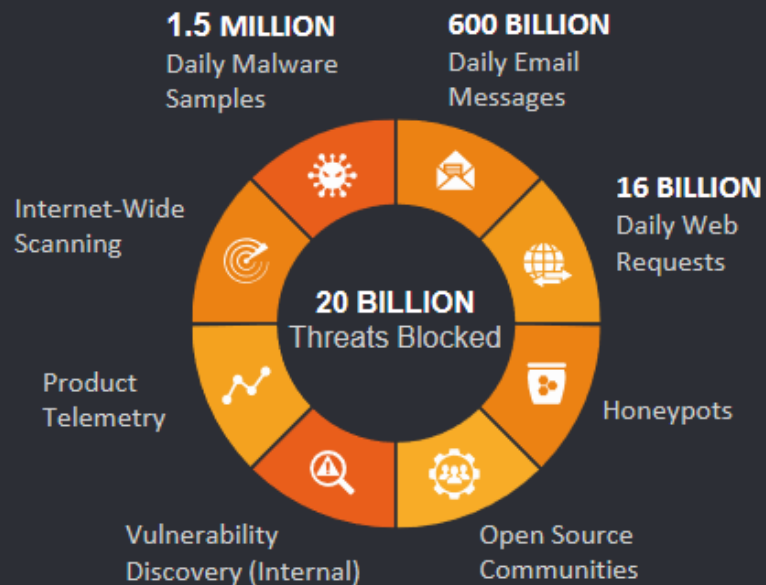
- História
- **Talos**
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki

Nuvem de Inteligência Cisco - Talos

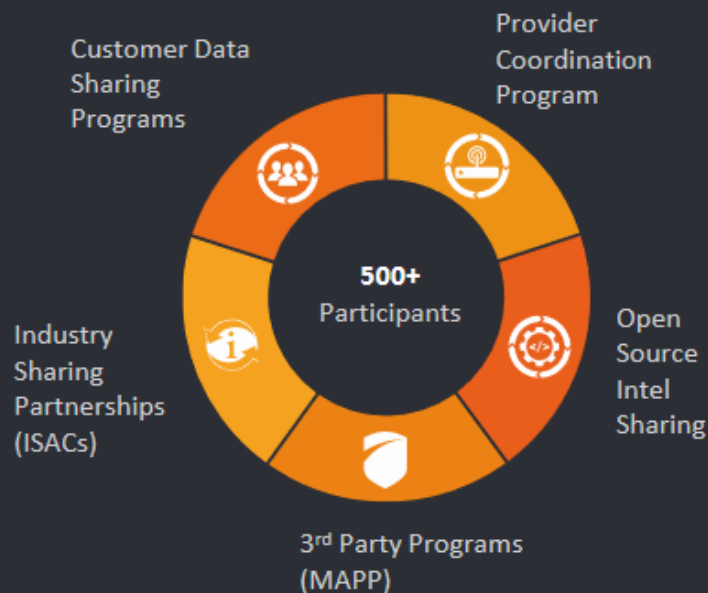


Talos Intel Background

THREAT INTEL



INTEL SHARING



250+
Full Time Threat
Intel
Researchers



MILLIONS
Of Telemetry
Agents



4
Global Data
Centers



100+
Threat Intelligence
Partners



1100+
Threat Traps

Agenda

- História
- Talos
- **Firepower**
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki

Modelos de Firewalls



FPR 9300 Series

- SM-40
- SM-48
- SM-56



- SM-24
- SM-36
- SM-44



FPR 4112/15/25/45



FPR 4110/20/40/50



FPR 2110/20/30/40



ASA 5525/45/55



FPR 1120/40/50



ASA 5508/16



FPR 1010

650 Mbps AVC
650 Mbps AVC+IPS

1.5-3 Gbps AVC
1.5-3 Gbps AVC+IPS

2-8.5 Gbps AVC
2-8.5 Gbps AVC+IPS

Stand-alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS 6

Six node cluster:
Up to 254 Gbps AVC
Up to 226 Gbps AVC+IPS

One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS

Six node (2 chassis) cluster:
Up to 336 Gbps AVC
Up to 307 Gbps AVC+IPS

SOHO/
SMB

Branch
Office

Mid-Size
Enterprise

Large
Enterprise

Data
Center

Service
Provider



Virtualização

Private Cloud

4 Core

- 1.2 Gbps AVC
- 1.1 Gbps AVC+IPS

8 Core

- 2.4 Gbps AVC
- 2.2 Gbps AVC+IPS

12 Core

- 3.6 Gbps AVC
- 3.3 Gbps AVC+IPS



Public Cloud

- 1.2 Gbps AVC
- 1.1 Gbps AVC+IPSc

AWS Instance types

- c3.xlarge
- c4.xlarge
- c5.large, c5.xlarge

Azure Instance types

- Standard D3
- D3v2
- D4v2
- D5v2



Funcionalidades x Código

Choose ASA for

- Traditional/Stateful L3-L4 Firewall
- Remote Access VPN Headend:
 - Clientless VPN
 - EZVPN/L2TP/3rd party clients
 - DAP/Hostscan
 - SAML Authentication
 - VPN Load balancing
 - Local authentication/TACACS/Kerberos

Choose FTD for

- Next-Gen Firewall and IPS (NGFW, NGIPS)
- Advanced Malware Protection (AMP)
- Talos intelligence feed and Snort rules
- True multi-tenancy with Multi-Instance
- Advanced visibility and threat analytics
 - Correlation Rules
 - Snort based intrusion rules
 - Firepower Recommendations
- Incident response and threat investigation
- TLS Decryption

Opções de Gerenciamento

On-box

Centralizada

Cloud

Firepower Device Manager



**Consolidated
management**

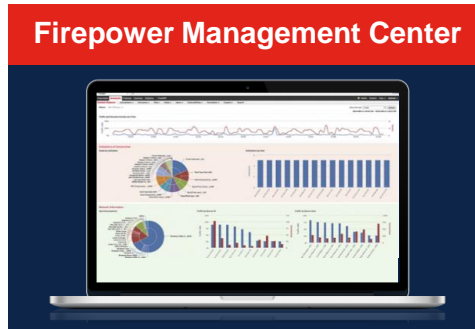


**Enhanced
control**



**Easy
set-up**

Firepower Management Center



**Unified
insight**



**Scalable
management**



**Intelligent
automation**

Cisco Defense Orchestrator



**Simple
interface**



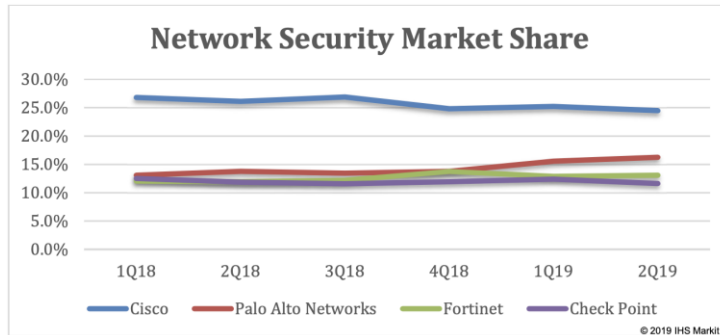
**Efficient
management**



**Streamlined
user experience**

Informações de mercado

Product		Exploit Block Rate ¹	NSS-Tested Throughput		
Cisco FirePOWER 8350 v5.3		99.2%	18,771 Mbps		
Evasions	Stability & Reliability	Application Control	Identity Aware	Firewall Policy Enforcement	
PASS	PASS	PASS	PASS	PASS	



Agenda

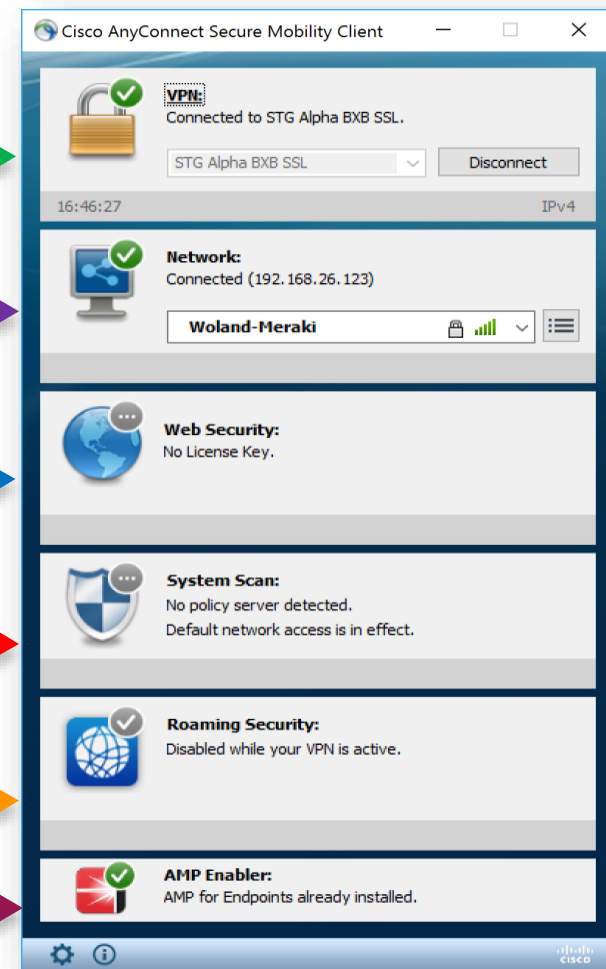
- História
- Talos
- Firepower
- **AnyConnect**
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki

Funcionalidades do AnyConnect



Módulos AnyConnect

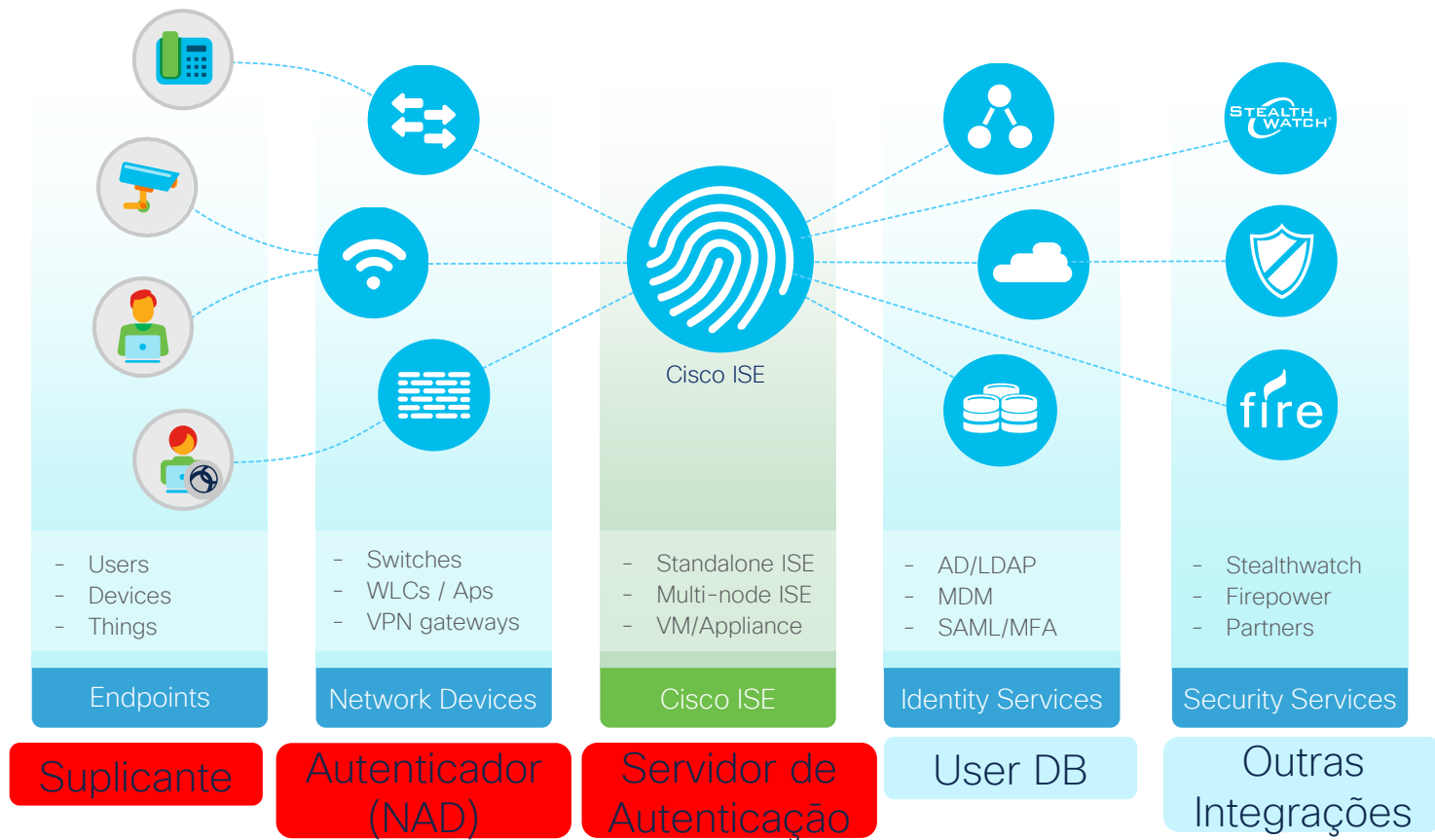
- VPN Module (Core)
- Network Access Manager (NAM)
- Web Security (CWS)
- Posture
- Umbrella Module
- HostScan (aka: ASA posture) (No UI)
- Network Visibility Module (NVM) (No UI)
- AMP Enabler Module
- Diagnostics and Reporting Tool (DART)



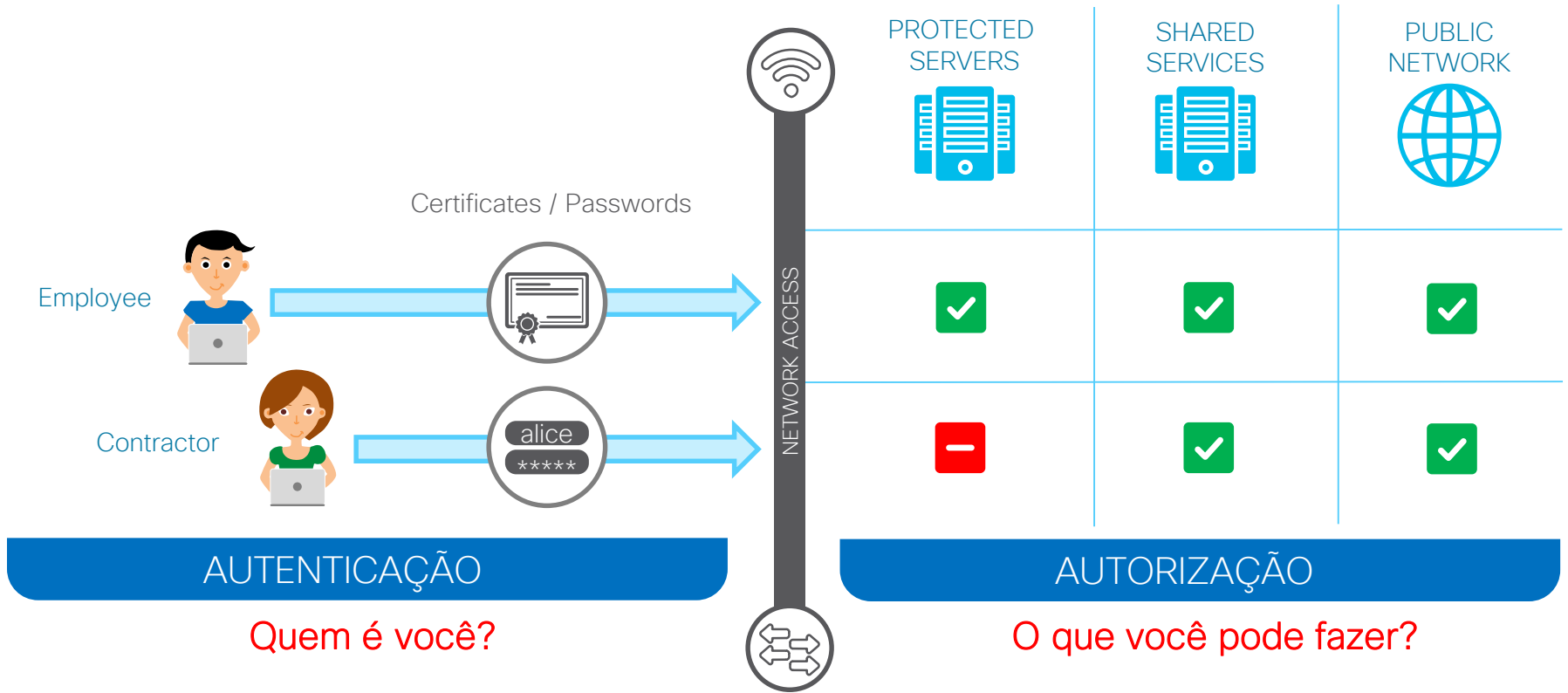
Agenda

- História
- Talos
- Firepower
- AnyConnect
- **ISE**
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki


Topologia típica de um caso de uso com ISE













AAA



Funcionalidades



	Device Administration	TACACS+ Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices
	Guest Access	Grant access to your network on the Internet for Guest users through the use of a Guest Portal. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest
	Asset Visibility	Device Profiling. Using the probes built into ISE and the network infrastructure to determine the type of device being used and granted network access based upon the information learned. Determining access for IoT devices. Differentiate between Corporate and Guest devices
	Identity-based Services	Allow access to network resources based upon the identity of the person. Use 802.1x , Easy Connect , or Passive ID
	BYOD	Allow employees to use their own devices to access network resources by registering their device and downloading certificates for authentication through a simple onboarding process
	SD Segmentation	TrustSec allows for segmentation of the network through the use of Scalable Group Tags (SGT) and Scalable Group ACLs (SGACL) instead of VLAN/ACL segmentation
	Context Exchange	pxGrid is an ecosystem that allows for direct integration into ISE from any application or vendor that builds it into their system for Network Visibility and Enforcement . Identity and context information is shared bidirectionally
	Compliance & Posture	Through the use of AnyConnect , an MDM , or an EMM , check the endpoints to ensure policies are met prior to allowing network access, such as antivirus definitions or patch levels
	Threat-Centric NAC	Using a Threat Analysis tool, such as Cisco Cognitive Threat Analytics, to grade an endpoints threat score and allow network access based upon the results
	SDA/DNA-C	ISE integrates with DNA Center to automate the network fabric and enforces the policies created in DNA-C throughout the entire network infrastructure

Cisco Security Technical Alliance



<https://www.cisco.com/go/csta>

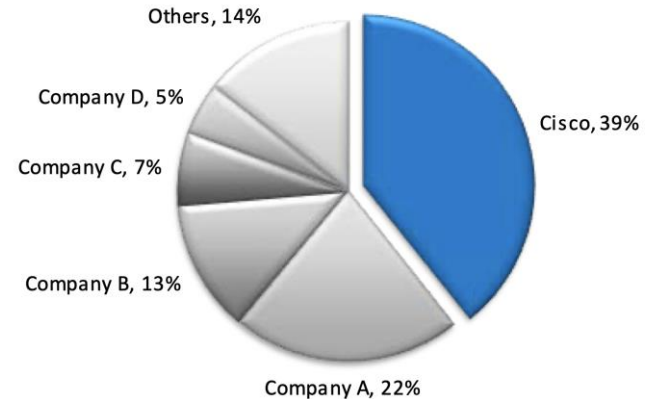


--	--

Informações de mercado

Gartner: *“Interoperability with other security solutions should also be considered an essential factor in choosing a NAC solution,”*

**Percent of Revenue
Total NAC Market: Global, 2015**



*<https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/market-leadership-award.pdf>

Pergunta 2

- De 1 a 5, em qual posição você vê a Cisco em relação ao mercado de Segurança?

A. 5

B. 4

C. 3

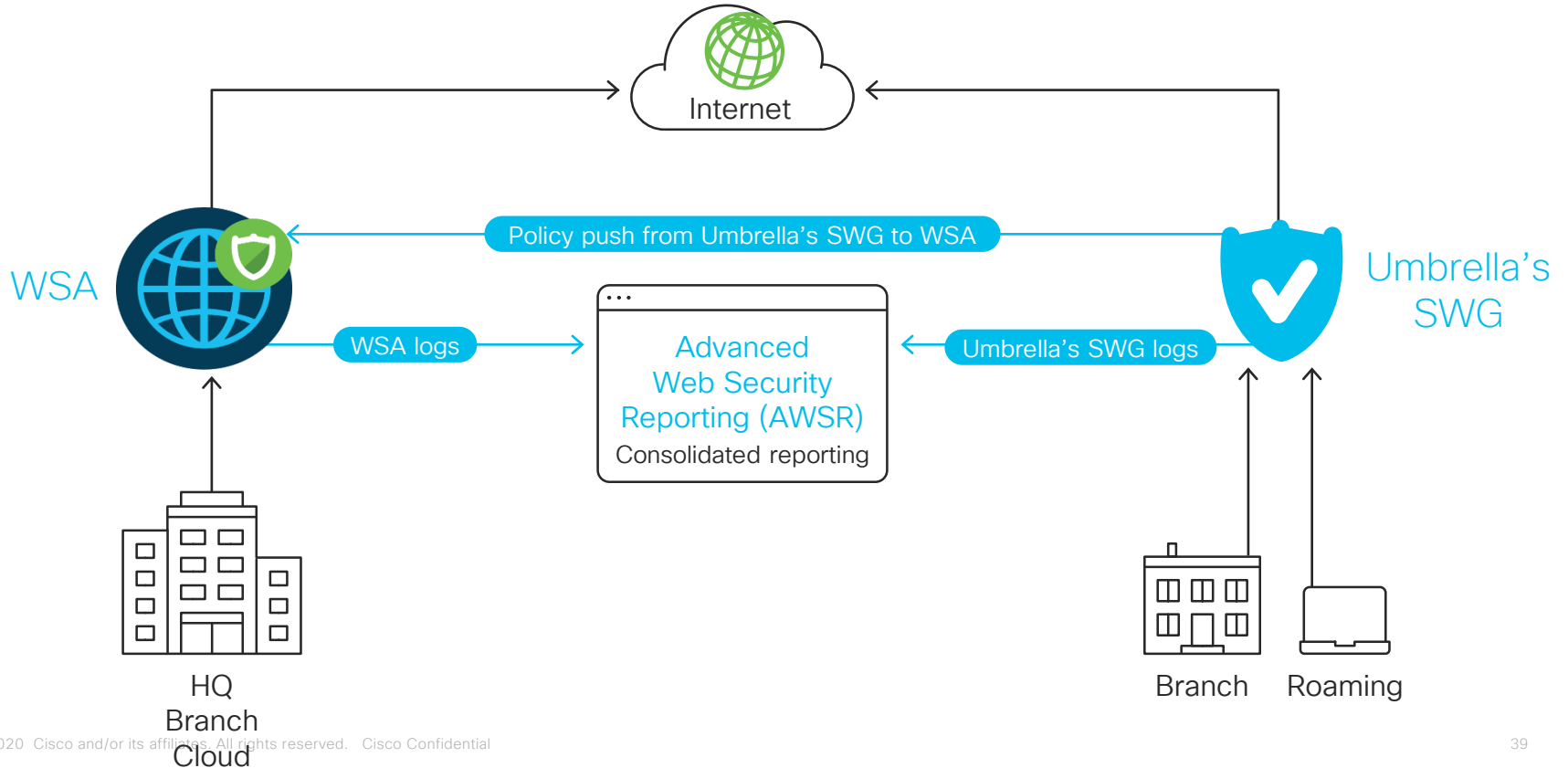
D. 2

E. 1

Agenda

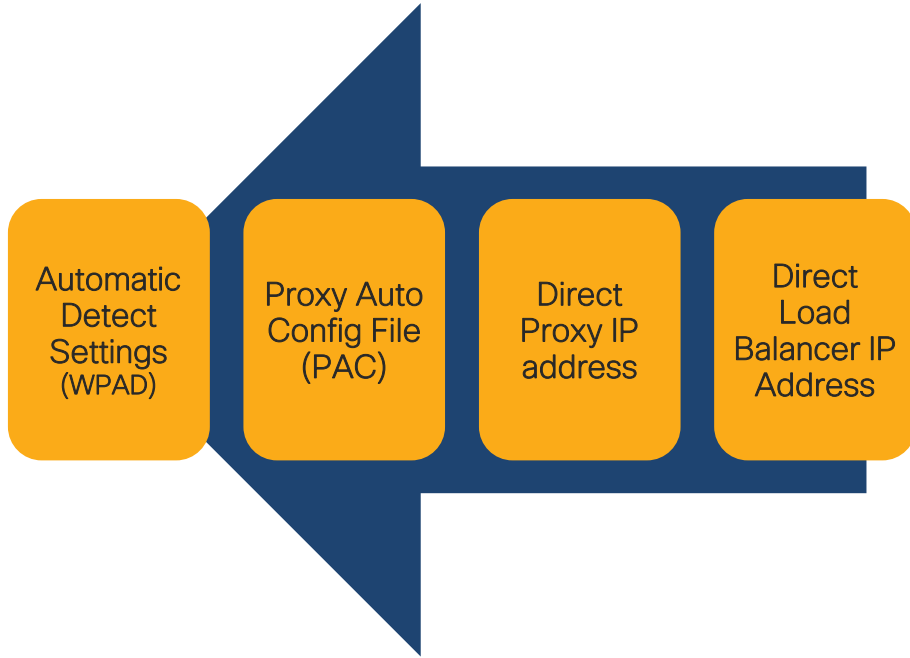
- História
- Talos
- Firepower
- AnyConnect
- ISE
- **WSA**
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki

Cenário híbrido com Umbrella

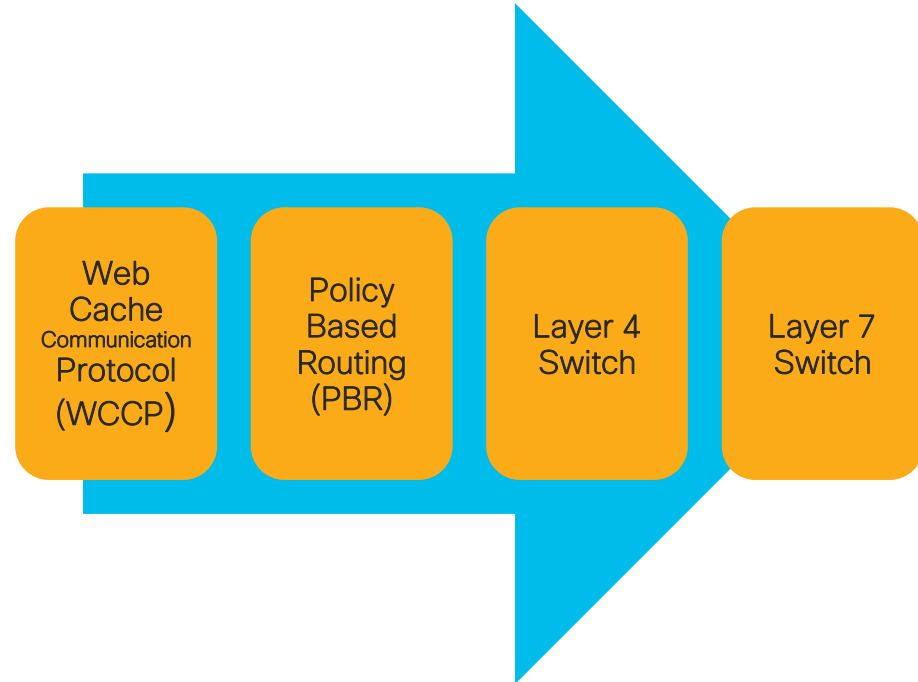


Modos de Deployment

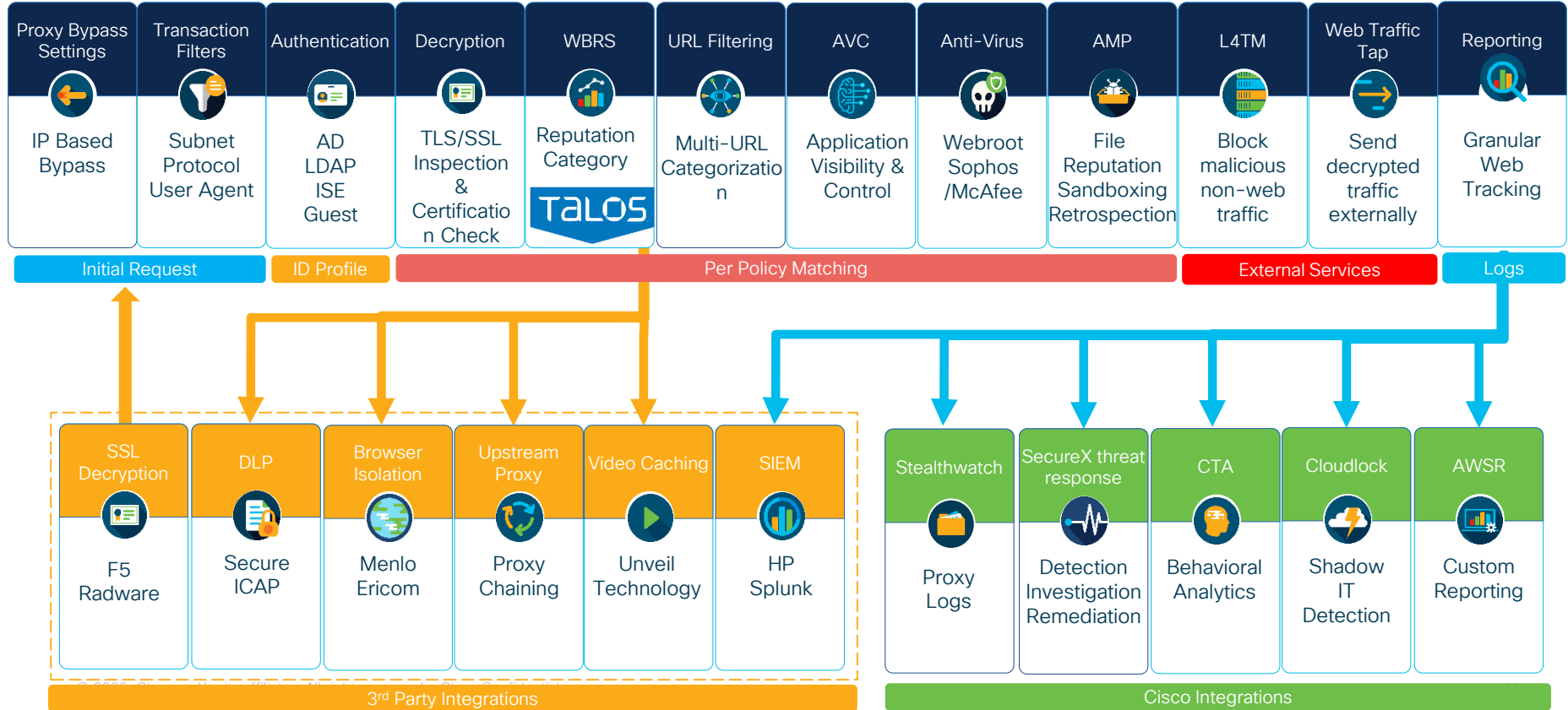
Explicito



Transparente

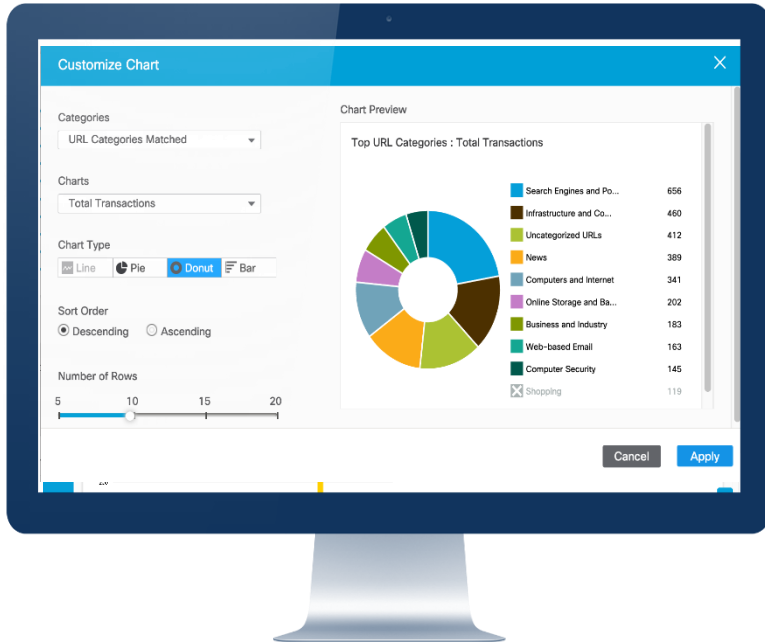


WSA Pipeline



Gerenciamento

Newer Reports on SMA



Features of SMA

Centralized Management



Centralized Upgrade



Centralized logging & Reporting



Multi-Configuration Master



Centralized Reporting for ESA

Agenda

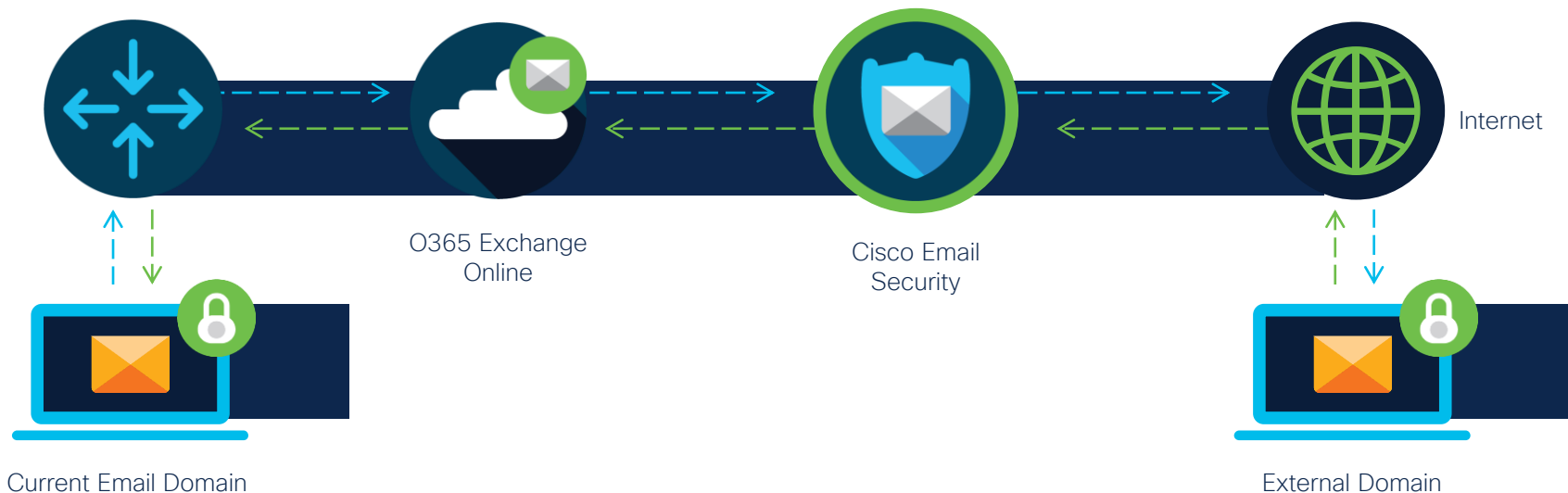
- História
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- **ESA**
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki



Email is still the #1 threat vector

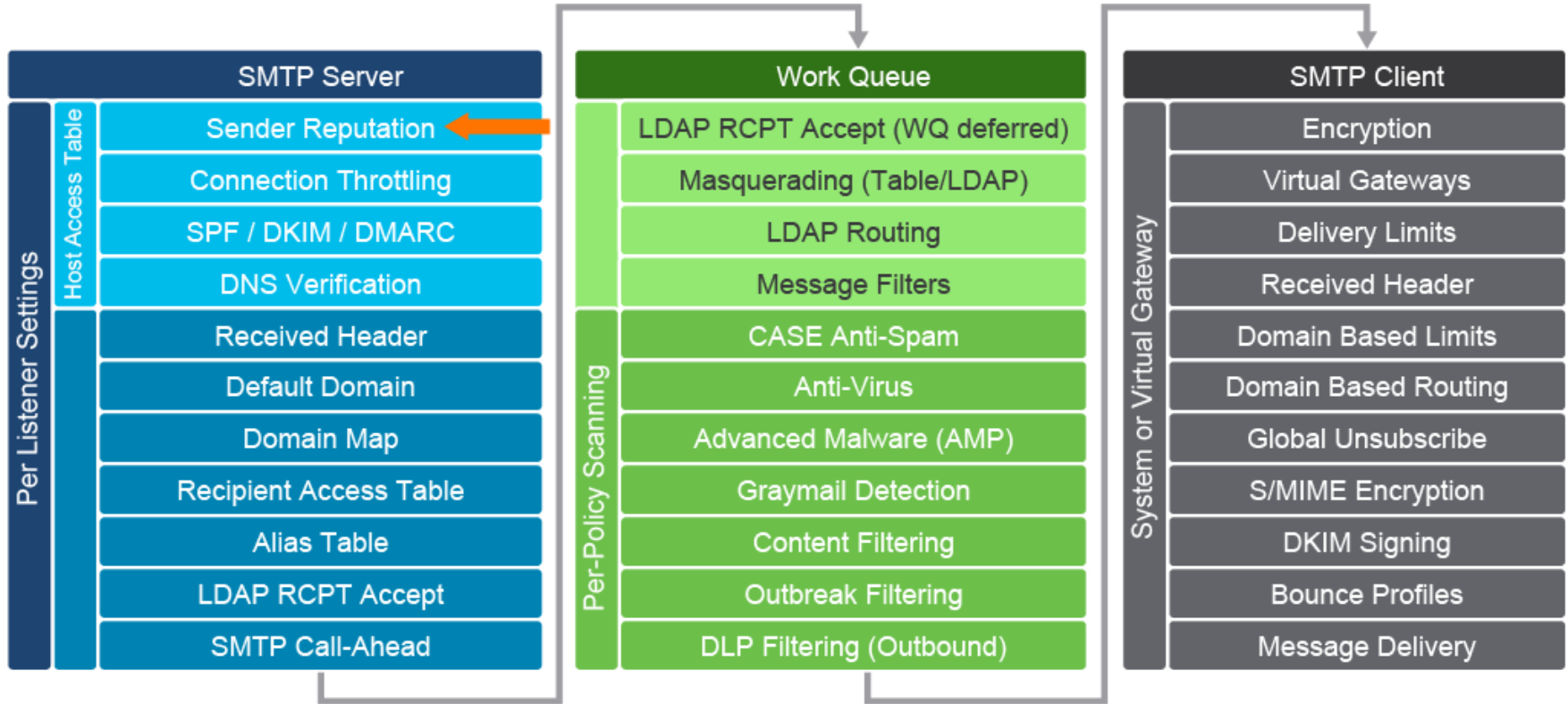


Topologia típica de um AntiSpam



----- Outbound Traffic
----- Inbound Traffic

ESA Pipeline





Software



Vulnerability Information



Reputation Center



Library

TALOS



Support Communities



About



Careers



Blog

Email Traffic Overview

As of: Thu Jun 01 2017 09:05:33 GMT-0500 (CDT)

100 TB
Of Data Received Daily



1.5 MILLION
Daily Malware Samples



600 BILLION
Daily Email Messages



16 BILLION
Daily Web Requests



24 · 7 · 365 Operations



250+
Full Time Threat Intel
Researchers



MILLIONS
Of Telemetry Agents



4
Global Data Centers



Over 100
Threat Intelligence Partners



**Global
scanning**



**30 years building
the world's networks**

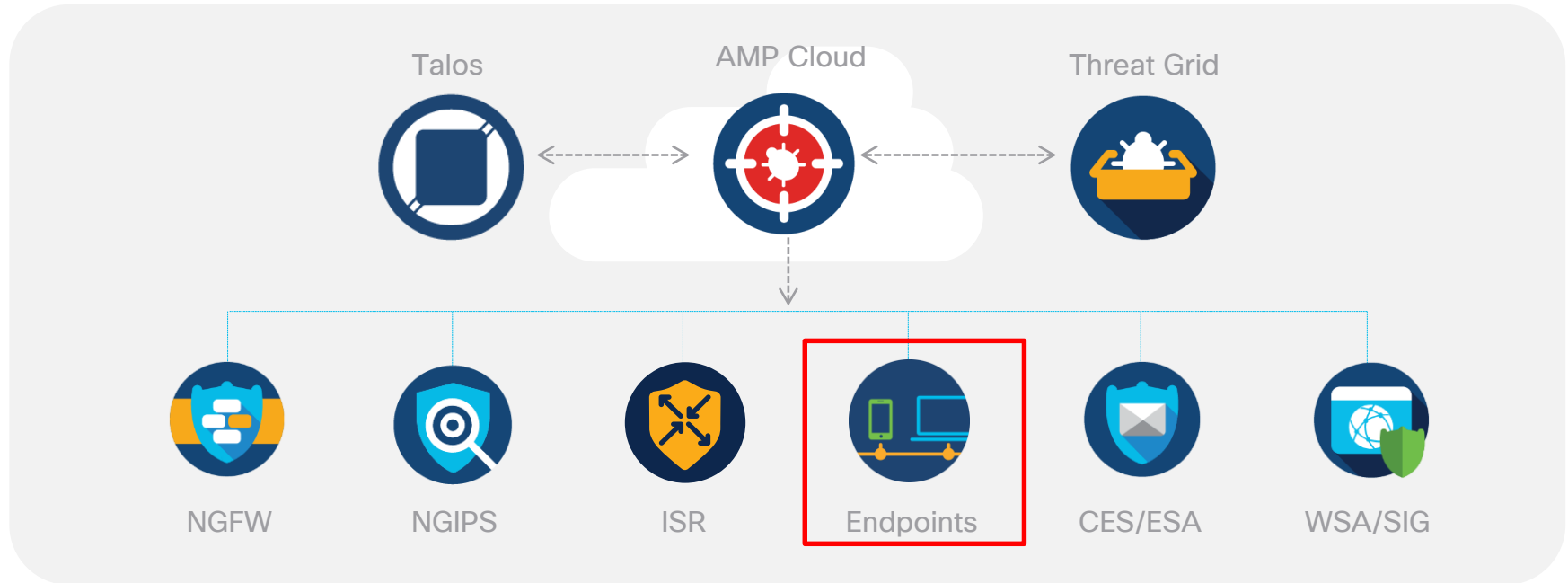
Informações de mercado



Agenda

- História
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- **AMP**
- StealthWatch
- Umbrella
- CloudLock
- Duo
- Meraki

Detecte uma vez, bloqueie em todos os lugares



Cisco AMP é completo



EPP

- Machine learning
- Behavioral analysis engine
- File-less malware prevention
- Cloud based file reputation engine
- Antivirus engine
- Network traffic protection



EDR

- Continuous activity monitoring
- Advanced endpoint search
- Sandboxing
- Cloud Indicators of Compromise
- Proactive threat hunting
- Custom block/allow lists for files and network traffic
- Vulnerable and low prevalence software identification
- Unmanaged endpoint discovery
- Endpoint isolation

Better protection

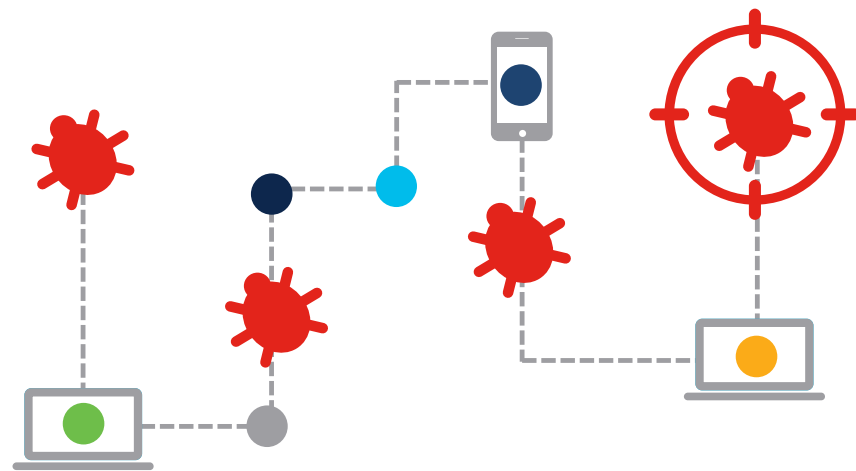
Cloud form factor

Easier to integrate

Análise Retrospectiva

- Identifica o ponto de origem da ameaça
- Vê o que ela está fazendo
- Vê onde ela esteve
- Rastreia como ela progride na rede
- Remedia cirurgicamente

Monitora + Detecta



● Recording

Informações de mercado

5,500+ Endpoint Customers

AV-Comparatives
2019 Business Security
Test Series

14.7M+ Endpoints

 Apple Partnership

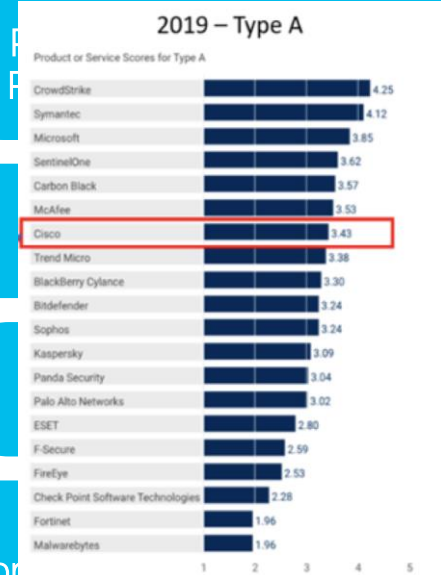
AMP Everywhere
90,000+ customers

NSS Labs
“Recommended”

Global Customer
Success

Cisco Partner
Ecosystem

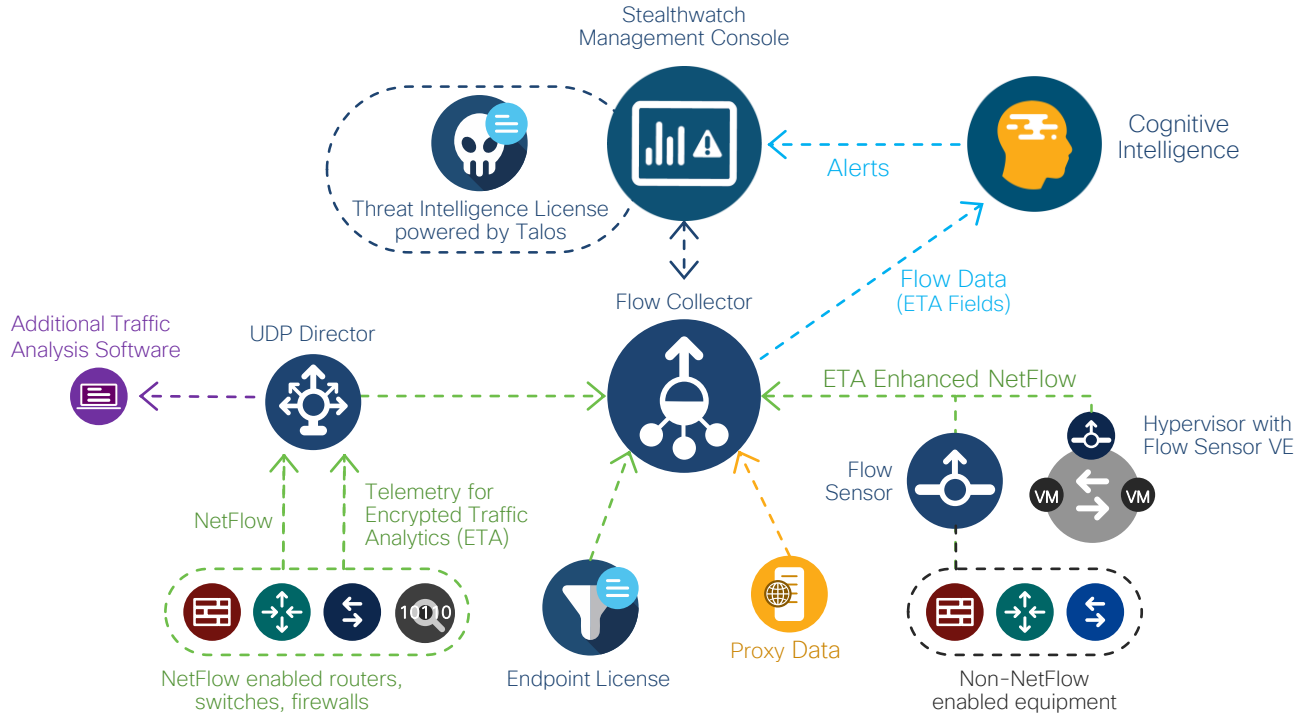
Broad OS,
Platform Support



Agenda

- História
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- **StealthWatch**
- Umbrella
- CloudLock
- Duo
- Meraki

Arquitectura StealthWatch



Visibilidade



CONHECE
Todos os hosts



VÊ
Cada conversação



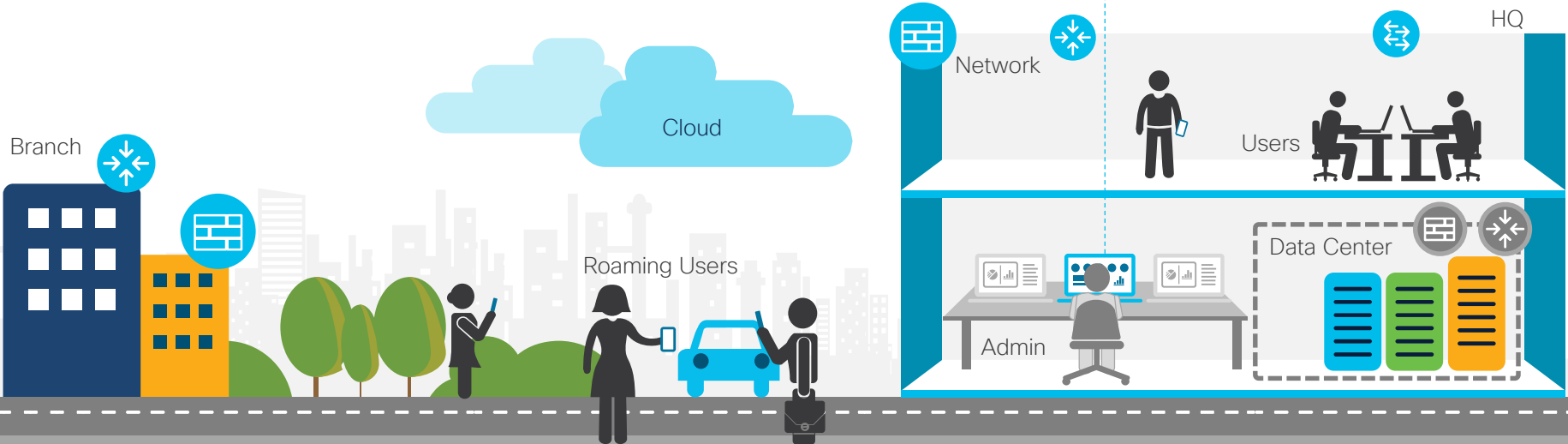
ENTENDE
O que é NORMAL



Alerta sobre
MUDANÇAS



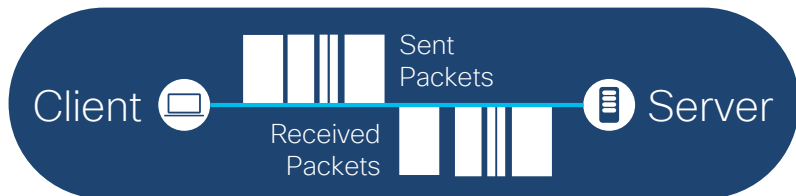
Responde à
AMEAÇAS



Identificação de tráfego Criptografado

Higher Efficacy with new Data

Model

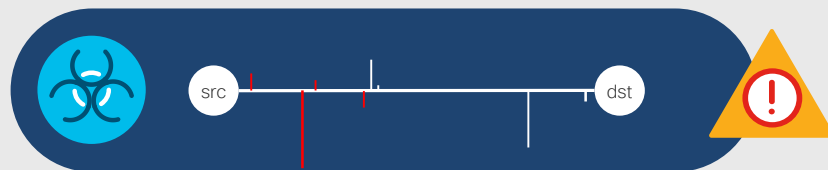


Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic

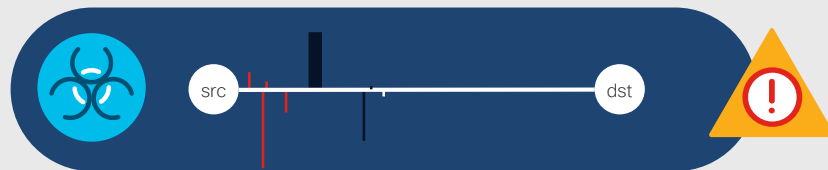
Google Search Page Download












Initiate Command and Control



Exfiltration and Keylogging

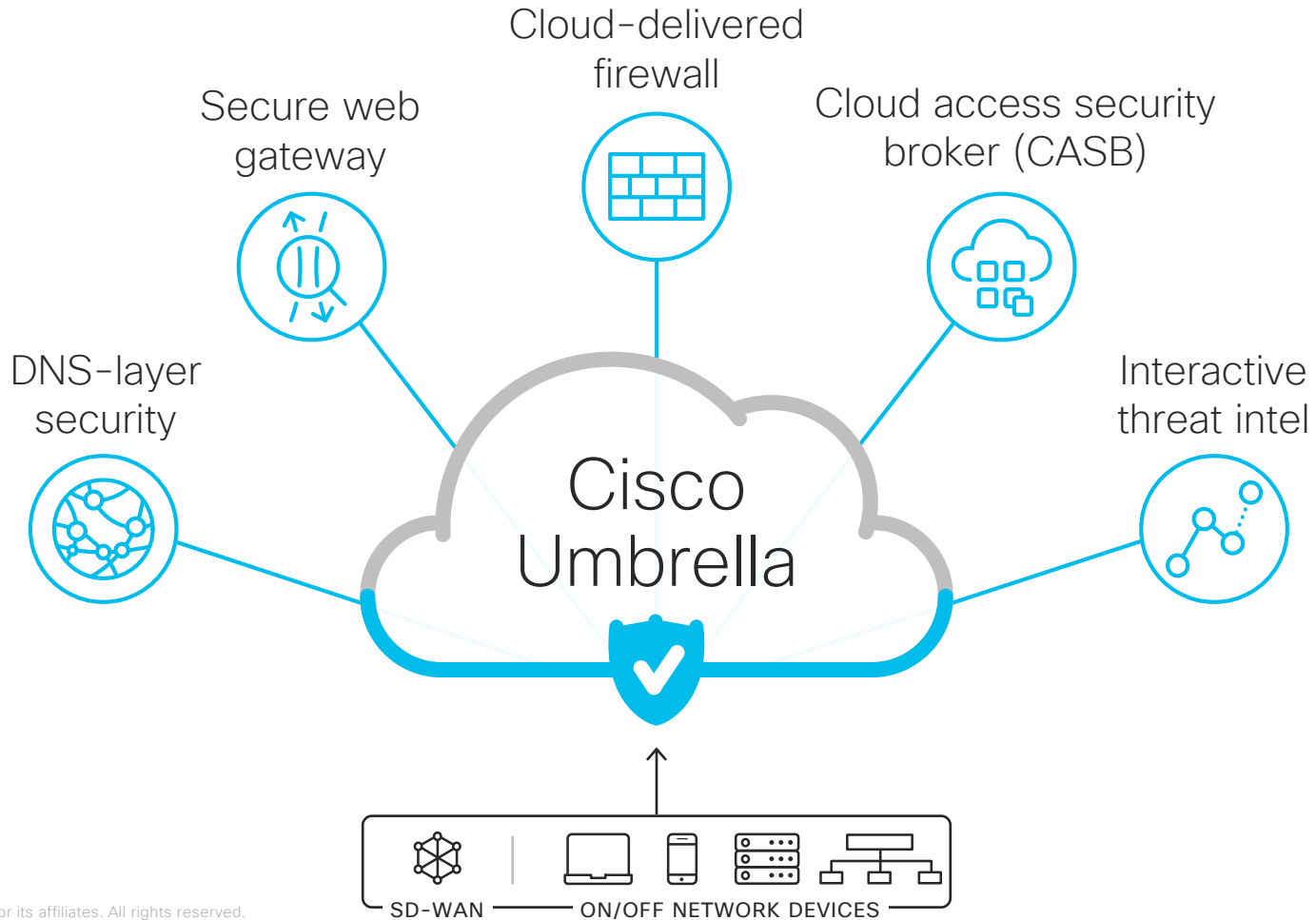


Integração com Cisco e outros Fabricantes

Device		Integration Type	Value
 Check Point	Checkpoint NGFW	v5/v9/IPFIX	NetFlow Gen for Visibility and NAT Stitching
 Barracuda	Barracuda NGFW	IPFIX	NetFlow Gen for Visibility
 Gigamon	Gigamon	v5/v9/IPFIX	NetFlow Generation from SPAN traffic
 ixia	IXIA NVS	IPFIX	NetFlow Gen for Visibility
 Palo Alto	Palo Alto	IPFIX	Enriched NetFlow Gen for Visibility
 TRIPWIRE	TRIPWIRE	Web Lookup	Correlation and Investigation Workflow
 ziften	Ziften	Web Lookup	Correlation and Investigation Workflow
 Savvius	Savvius	Syslog	Correlating events + Trigger packet capture
 ArcSight	Arcsight	Syslog	Correlating events from Stealthwatch

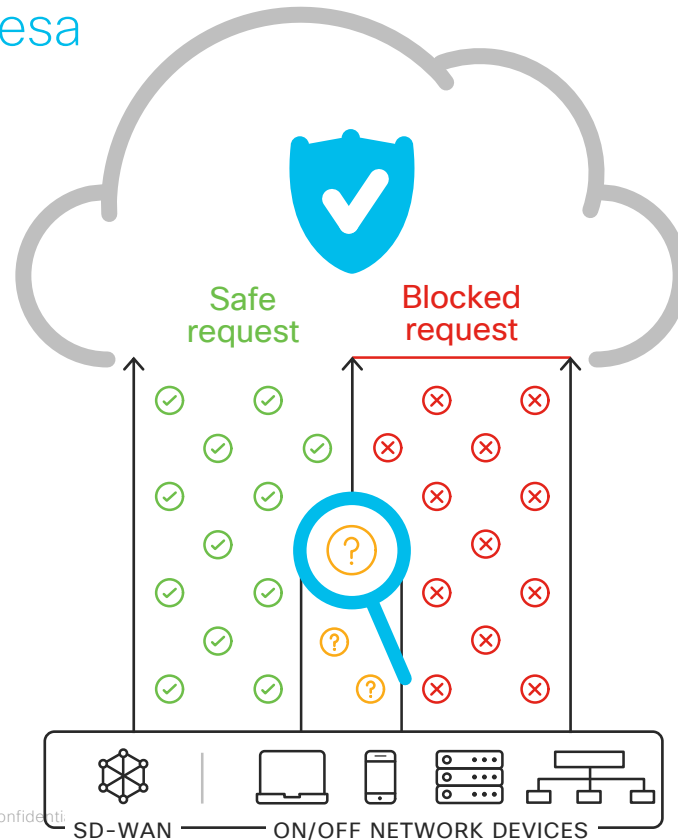
Agenda

- História
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- **Umbrella**
- CloudLock
- Duo
- Meraki



Segurança de Camada DNS

Primeira linha de defesa



Instalação do Umbrella



208.67.222.222

Your policy

Enforce all security settings for
67.215.87.11

Internet gateway



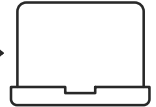
Network egress IP
67.215.87.11
DNS server
10.1.1.1

Internal DNS Server

Server IP
10.1.1.1

External DNS resolution
208.67.222.222

Laptop IP
10.1.1.3

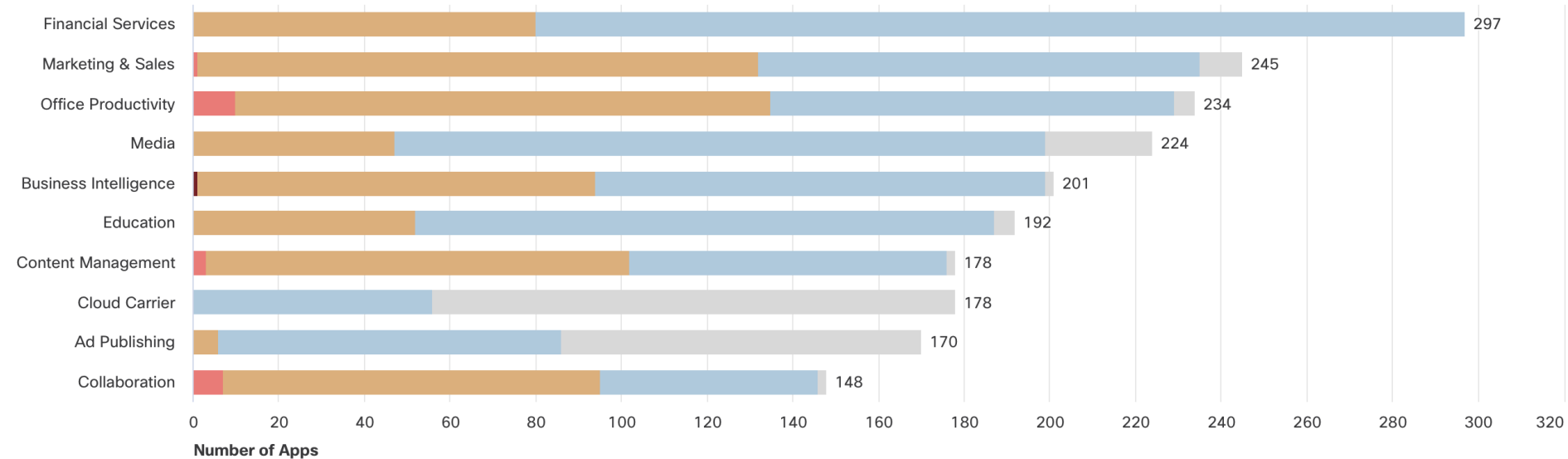


YOUR NETWORK

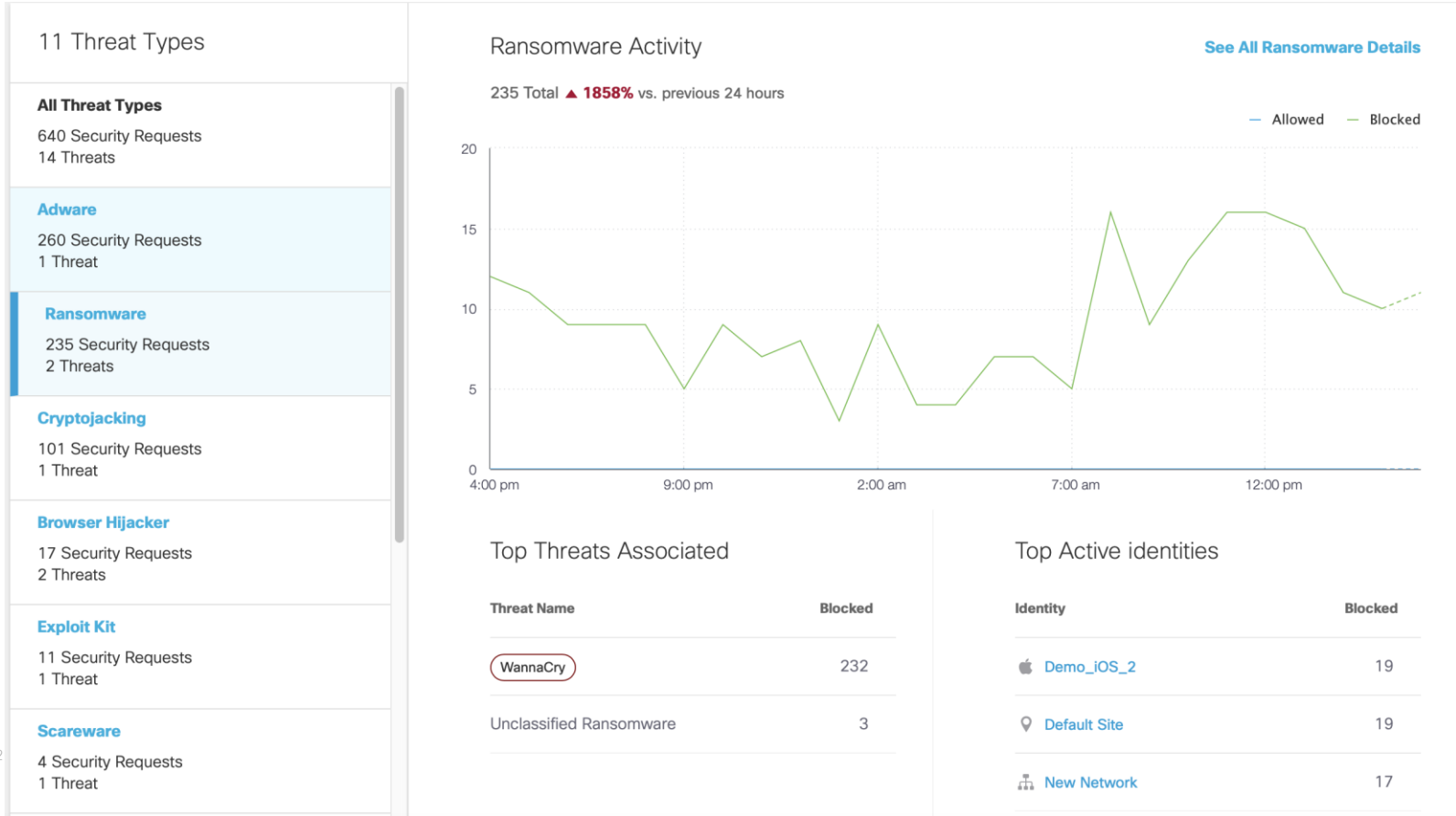
Exemplo de Relatório: App Discovery

Apps by Category and Risk


Top 10 categories (out of 38)



Exemplo de Relatório: Threats



Informações de mercado



Our customers have spoken!

We are thrilled to be named a January 2019 Customers' Choice for Secure Web Gateway on Gartner Peer Insights.

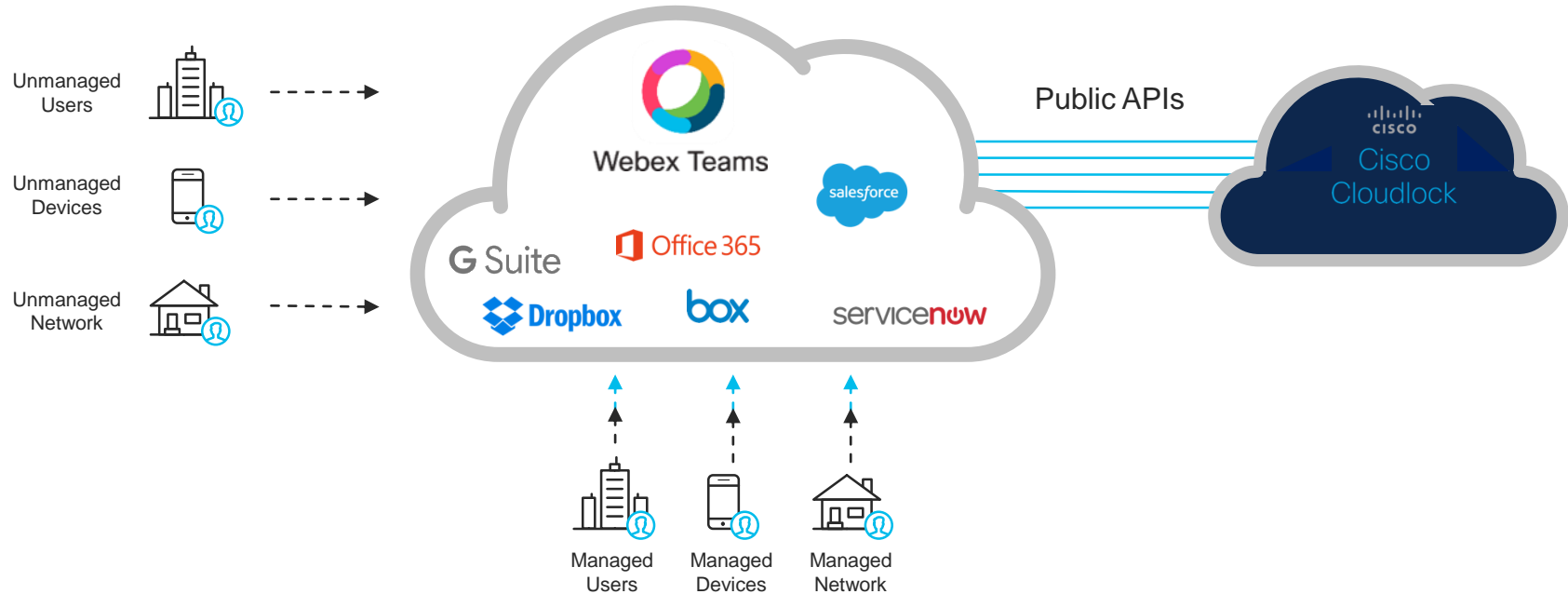
Secure Web Gateway: Análise inclui Umbrella e WSA



Agenda

- História
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- **CloudLock**
- Duo
- Meraki

Cisco Cloudlock



Controle e Visibilidade

Discover and Control



Compromised accounts



Insider threats



Data exposures and leakages



Privacy and compliance violations



OAuth discovery and control



Shadow IT



User and Entity Behavior Analytics



Cloud Data Loss Prevention (DLP)



Apps Firewall
App to App Comms

Exemplo de visibilidade e segurança



Mais de 80 politiques de DLP



PII

- SSN/ID numbers
- Driver license numbers
- Passport numbers



Education

- Inappropriate content
- Student loan information
- FERPA compliance



General

- Email address
- IP address
- Passwords/login information



PHI

- HIPAA
- Health identification numbers
- Medical prescriptions



PCI

- Credit card numbers
- Bank account numbers
- SWIFT codes

Plus the ability to easily create custom policies

Agenda

- História
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- **Duo**
- Meraki

Senhas

81%

dos incidentes são devido a senhas roubadas ou fracas

- Credenciais comprometidas representam um grande risco.
- Tokens não são amigáveis / fáceis de usar.

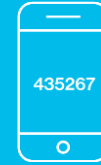


Grande range de opções de MFA

- Possível integrar com centenas de aplicações
- Habilite múltiplas opções para facilitar a vida do usuário



Push



Soft Token



SMS



Phone Call



U2F



Wearables



Biometrics



Hardware Tokens



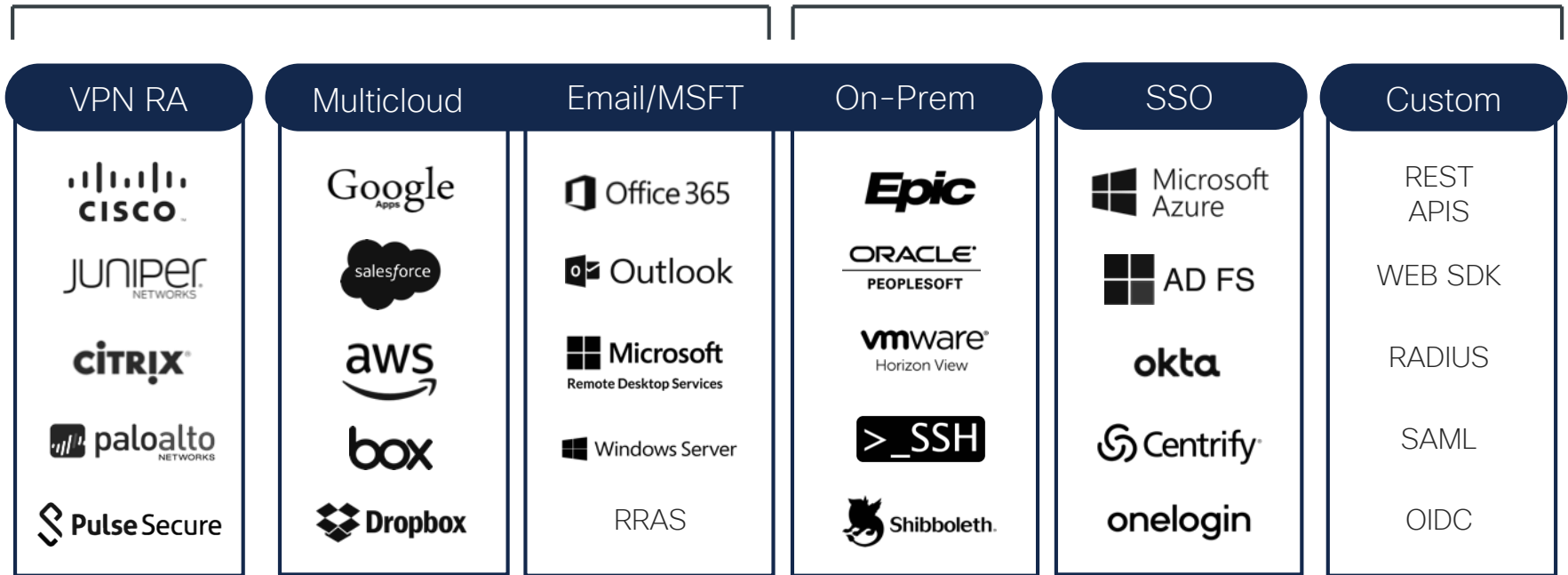
Duo Security is
now part of Cisco.



Aplicações suportadas

Start Here

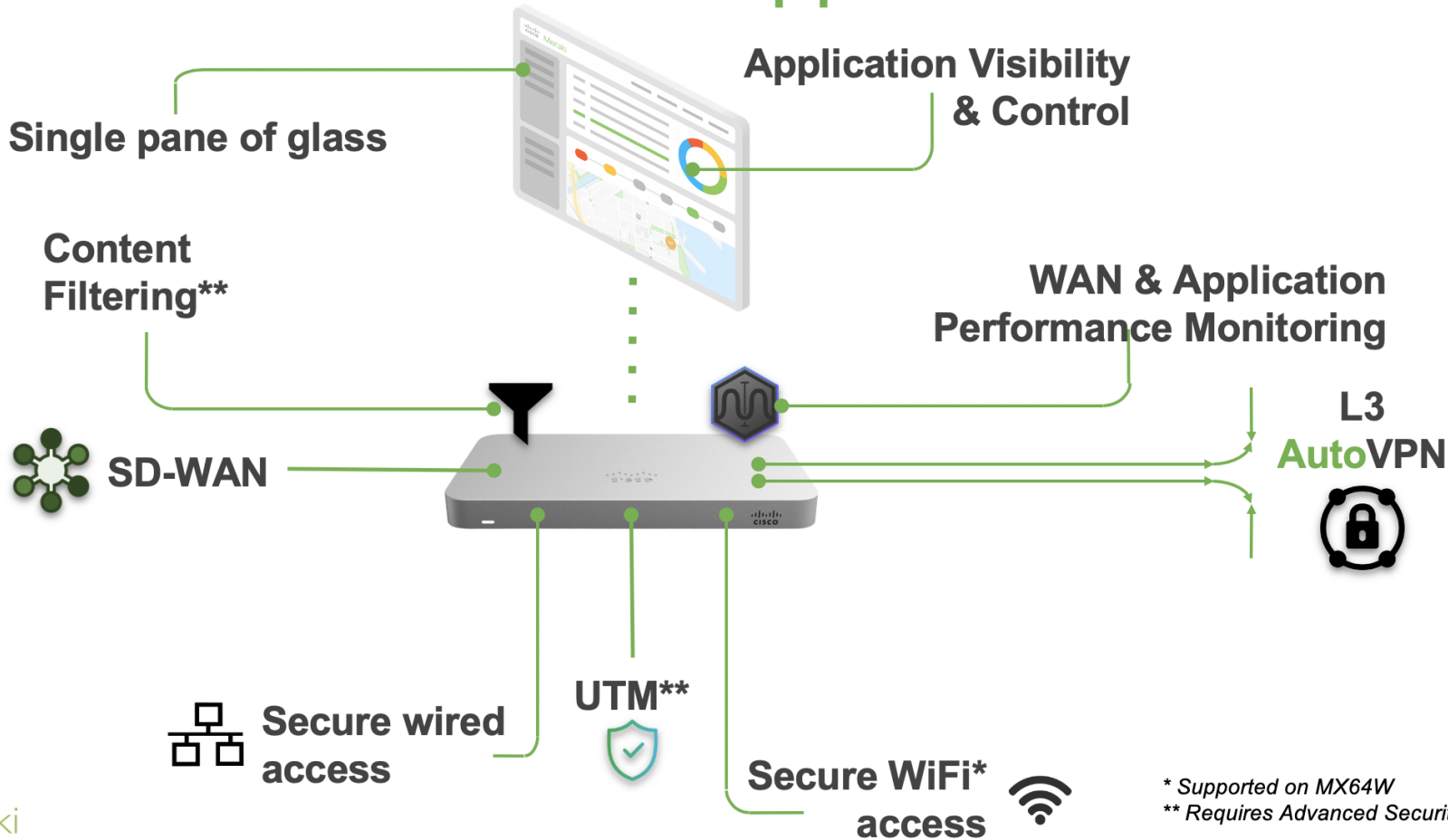
Then Expand



Agenda

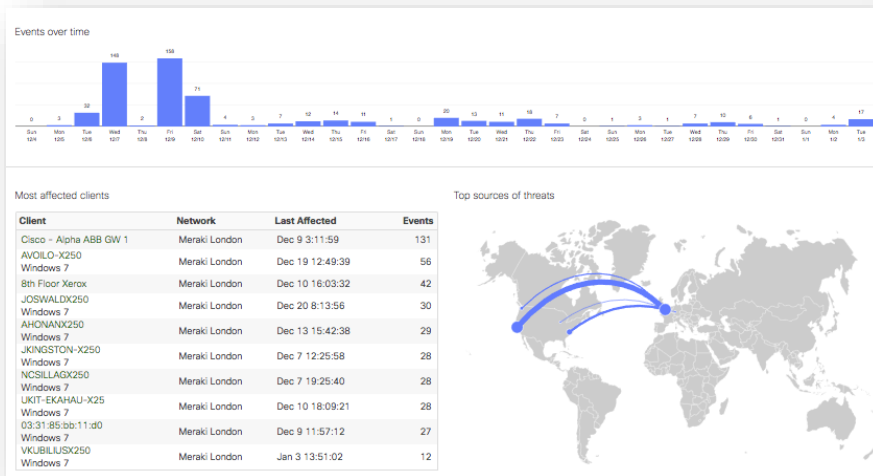
- História
- Talos
- Firepower
- AnyConnect
- ISE
- WSA
- ESA
- AMP
- StealthWatch
- Umbrella
- CloudLock
- Duo
- **Meraki**

Meraki MX Appliance



Funcionalidades de Segurança

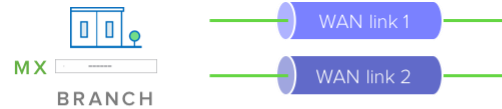
Next Generation Firewall	Application aware firewalling
Intrusion Prevention (IPS)	Based on Cisco Snort
URL Content Filtering	With over 80 categories and over 4 billion categorized URLs
Geo Based Security	Allow or block traffic by country
Malware Protection	Cisco AMP and Threat Grid
Automatic Updates	Software and security updates delivered from the cloud.
PCI Compliance	PCI 3.2 certified cloud management backend



Redundância de Links

Dual active VPN

Load balance your VPN traffic over two WAN links



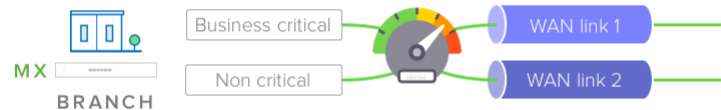
Policy-based Routing (PbR)

Select the preferred path for traffic based on protocol, port, source and destination IP, or even application



Dynamic path selection

Select the best VPN tunnel for traffic automatically based on performance



Auto VPN tunnels

Serviços



- Professional Services
Design das soluções Cisco,
implementação e otimização



- Support Services
Mais conhecido como TAC.
Engajamento contínuo com o cliente.



- Learning Services
Treinamentos e-learning, self-paced,
com instrutores ou customizados.

Pergunta 3

- Qual solução você estaria mais interessado em testar na rede da sua empresa?

- A. Firepower
- B. Umbrella
- C. ISE
- D. WSA ou ESA
- E. StealthWatch

Faça suas
perguntas agora!



Use o painel
Perguntas e Respostas ou Q&A
para enviar suas perguntas.

Nosso especialista responderá ao vivo ⁸¹

Ask me Anything

Até a próxima sexta-feira, 26 de Junho de 2020.

Link para o evento: https://bit.ly/AMA_1806



Fabio Carneiro
Consulting Security
Engineer



Nilton Maia
Consulting Security
Engineer

Participe em nossas Redes sociais



Twitter

- @Cisco_Support
- @CiscoDoBrasil

Facebook

- Hey Cisco
<http://bit.ly/csc-facebook>
- Cisco Do Brasil
<https://www.facebook.com/CiscoDoBrasil/>
- Cisco Portugal
<https://www.facebook.com/ciscoporugal/>

Saiba mais sobre os próximos eventos

Convidamos você a visitar nossas canais

YouTube

- Cisco Comunity
- <http://bit.ly/csc-youtube>



App

- Cisco Technical Support



LinkedIn

- Cisco-Community
- <http://bit.ly/csc-linked-in>



Saiba mais sobre os próximos eventos

A Cisco também tem Comunidades em outros idiomas!

Se você fala Inglês, Espanhol, Francês, Japonês, Russo ou Chinês, lhe convidamos a conhecer nossas Comunidades



[Cisco Community](#)
Inglês

[Comunidad de Cisco](#)
Espanhol

[Communauté Cisco](#)
Francês

[思科社区](#)
Chinês

[Сообщество](#)
[Cisco](#)
Russo

[シスコのコミュニティ](#)
Japonês

Por favor, tome 10 segundos
para responder nossa enquete de
múltipla escolha ao finalizar o evento!

Sua opinião é muito importante para
continuar melhorando!



*Obrigado por ser parte dessa
experiência!*

