Secure Remote Access

Roger Courchesne – ESI
Malaurie Morin Proulx, Cisco

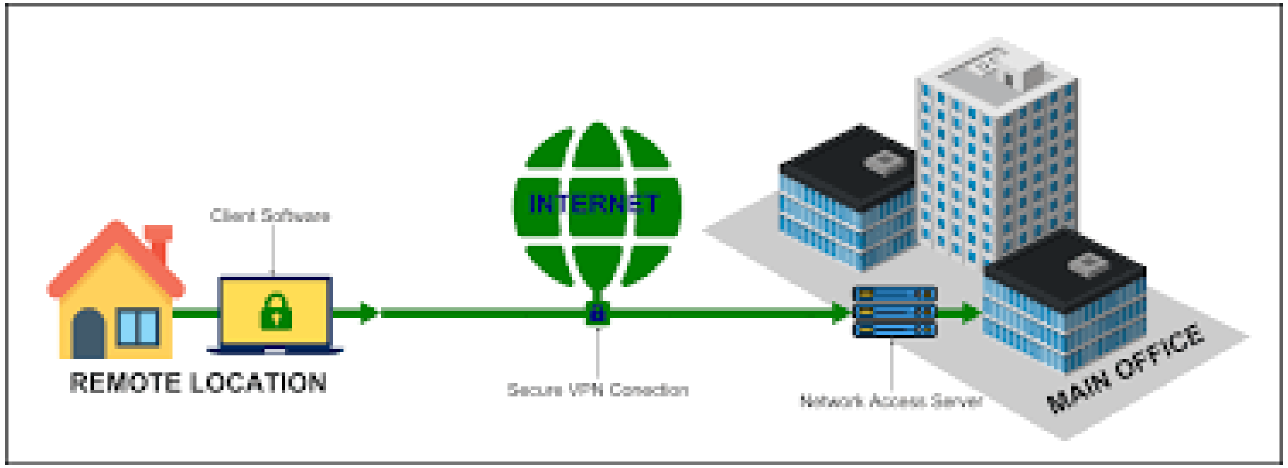
October 28 2020

AGENDA

- → What is telecommuting? - back to basics!
- → What are the ingredients of a good secure remote access solution?
- → What are the most used applications?
- → Basic connectivity
- → How to secure telecommuters with Cisco

DEFINING TELECOMMUTING

- It means performing professional duties away from the workplace (Ex. from home, chalet, etc.);
- Access to the tools, data, applications and colleagues, as if we were in the office;
- Teleworking was made possible by IT, high-speed internet access and security mechanisms
- Teleworking requires a discipline. It is often allowed since employees can perform their duties without compromising productivity



DEFINING TELECOMMUTING

WATCH OUT FOR DISTRACTIONS…

AND FOR THE DISTINCTION BETWEEN WORK AND HOME!

INGREDIENTS OF A GOOD REMOTE ACCESS SOLUTION

Disciplined employees

An IT infrastructure that can support teleworkers traffic

A device that complies with company standards

High speed Internet access

A secure access

WHAT ARE THE MOST FREQUENTLY USED APPS FOR TELEWORKERS?

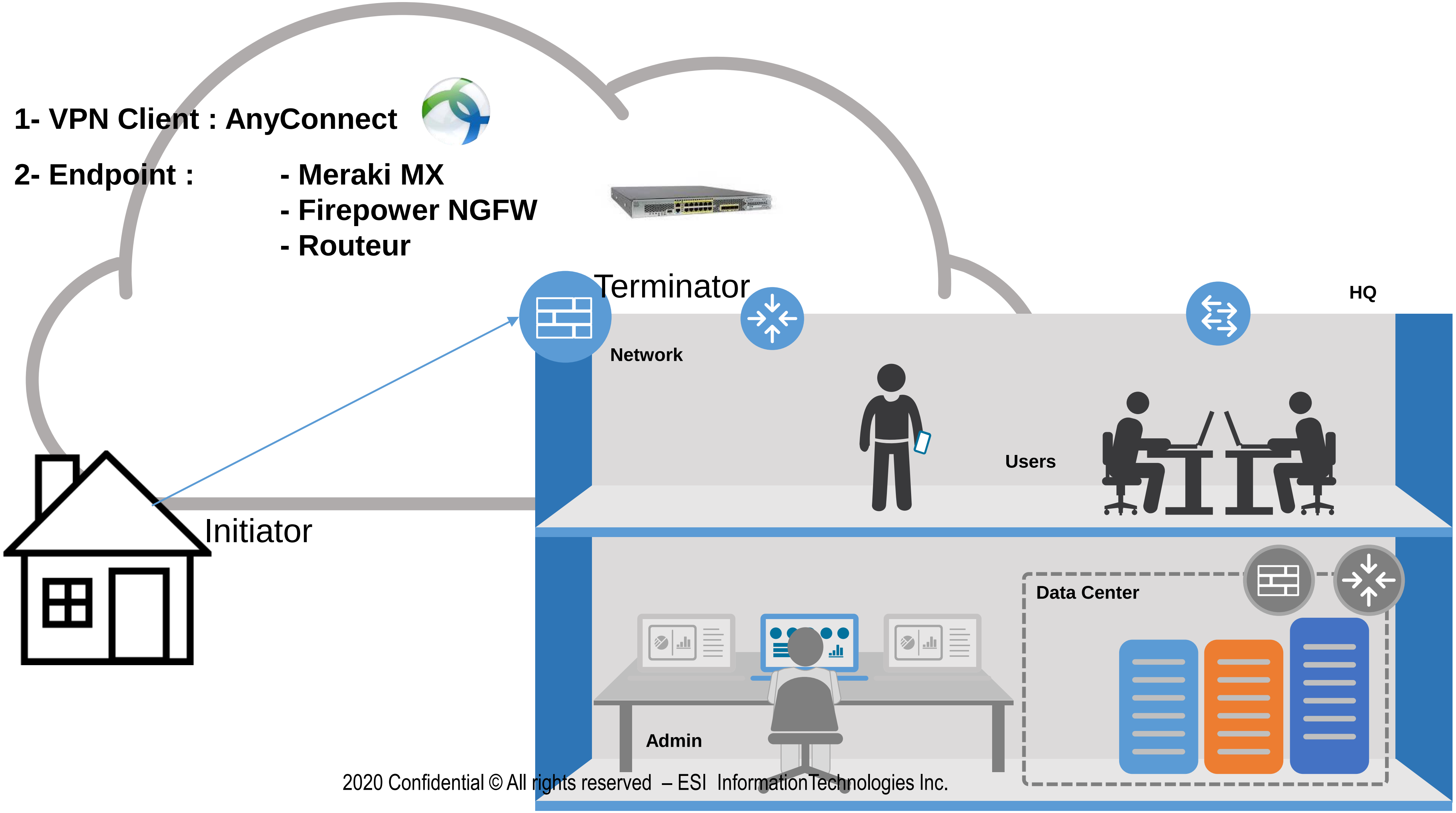
- Network servers containing shared corporate files
- The company intranet
- The “On and Off-Premise” apps:
  - The email server + employee directory
  - Timesheet, CRM, ERP (SAP, JD Edwards)
  - Project management, accounting software, expense account, invoicing ...
- Collaboration tools:
  - Webex Meeting, Webex Team, Microsoft Teams
  - Corporate IP telephony, videoconferencing
  - Call center applications ……

Basic Connectivity

Tunnel Initiator and Terminator

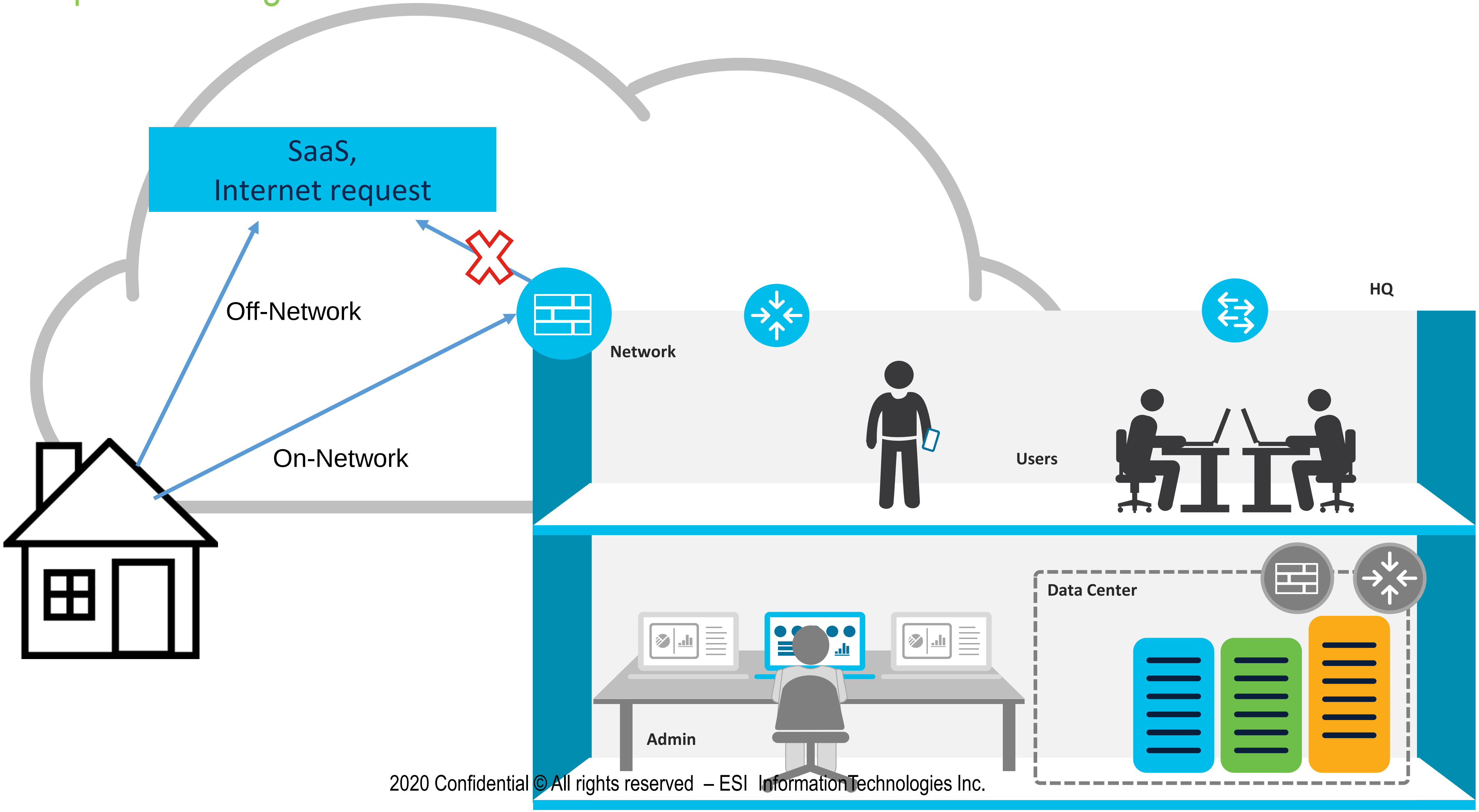
1- VPN Client : AnyConnect

2- Endpoint :
- Meraki MX
- Firepower NGFW
- Routeur

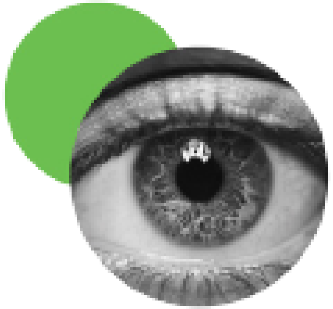


Basic Connectivity

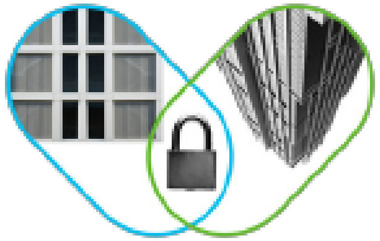
Split tunnelling



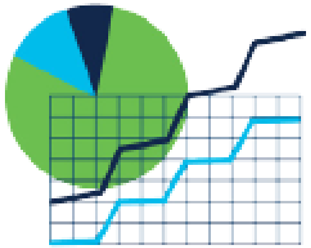
Main IT security pain points for remote access



→Gaps in visibility and security coverage

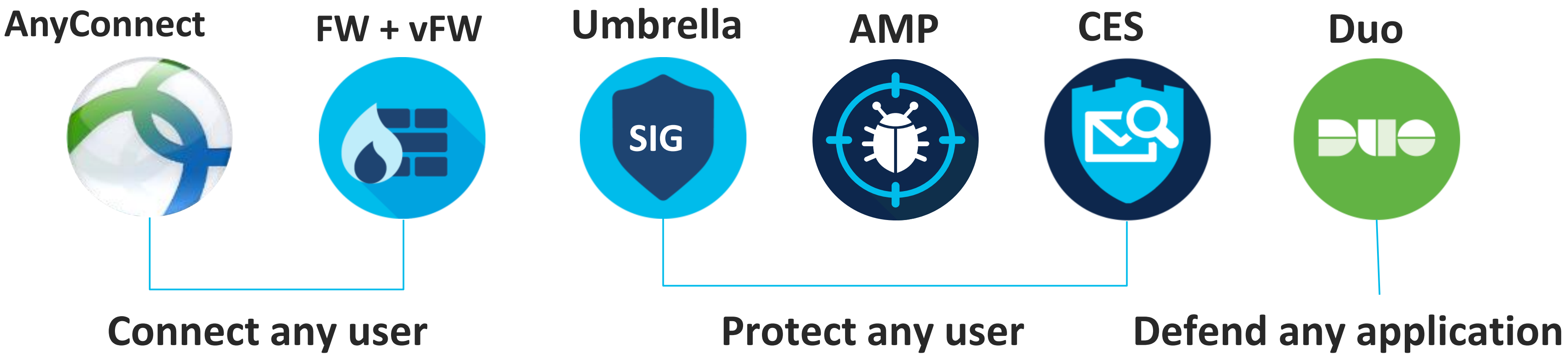


→Volume and complexity of security tools



→Limited budgets and security resources

How to secure teleworkers with Cisco solutions?



AnyConnect

FW + vFW

Umbrella

AMP

CES

Duo

Connect any user

Protect any user

Defend any application

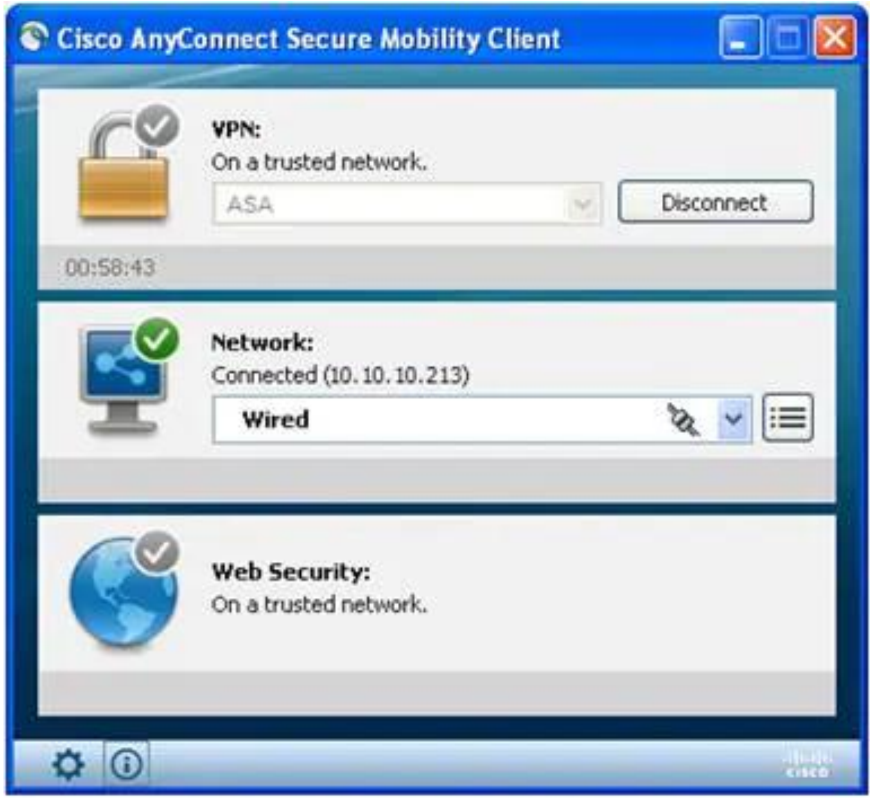
CISCO FIREWALL

- Appliance
  - Cisco Firewall ASA
  - Cisco FirePower (FTD)
  - Meraki MX Series
- Virtuel
  - ASAv et FTDv
  - ESXi et KVM, Azure et AWS
- We help you make the choice, the "sizing", the architecture, the installation / support.

CISCO VPN CLIENT: ANYCONNECT

→ Cisco Anyconnect Secure Mobility Client

- 1 – 3 or 5 year subscription
- 2 options: Annyconnect Plus or Apex
- PC: Windows, Mac, Linux
- Mobile: IOS, Android



Cisco AnyConnect Secure Mobility Client

VPN:
On a trusted network.
ASA

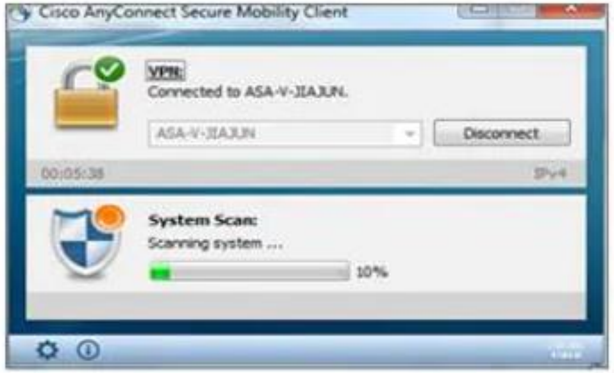
00:58:43

Network:
Connected (10.10.10.213)
Wired

Web Security:
On a trusted network.

Cisco VPN Client: Anyconnect - Features

- VPN IPSec remote access (IPSec Client)
- WSA ou Cloud Web Security integration
  - Built-in web security, malware threat defense, phishing protection, CCcb
- Cisco Umbrella roaming (on & off network)
  - Enforce security for roaming devices when the VPN is off
- Assist with AMP for endpoints (AMP Enabler)
  - Provides more proactive protection to further assure an attack is mitigated at the remote endpoint quickly
- Network Visibility Module (Apex)
  - Uncover potential behavior anomalies by monitoring app. usage
- Compliance and Remediation Module (Apex)
  - Validate the posture: antivirus, personal firewall, and antispyware


Cisco AnyConnect Secure Mobility Client

VPN:
Connected to ASA-V-JIAJUN.

ASA-V-JIAJUN

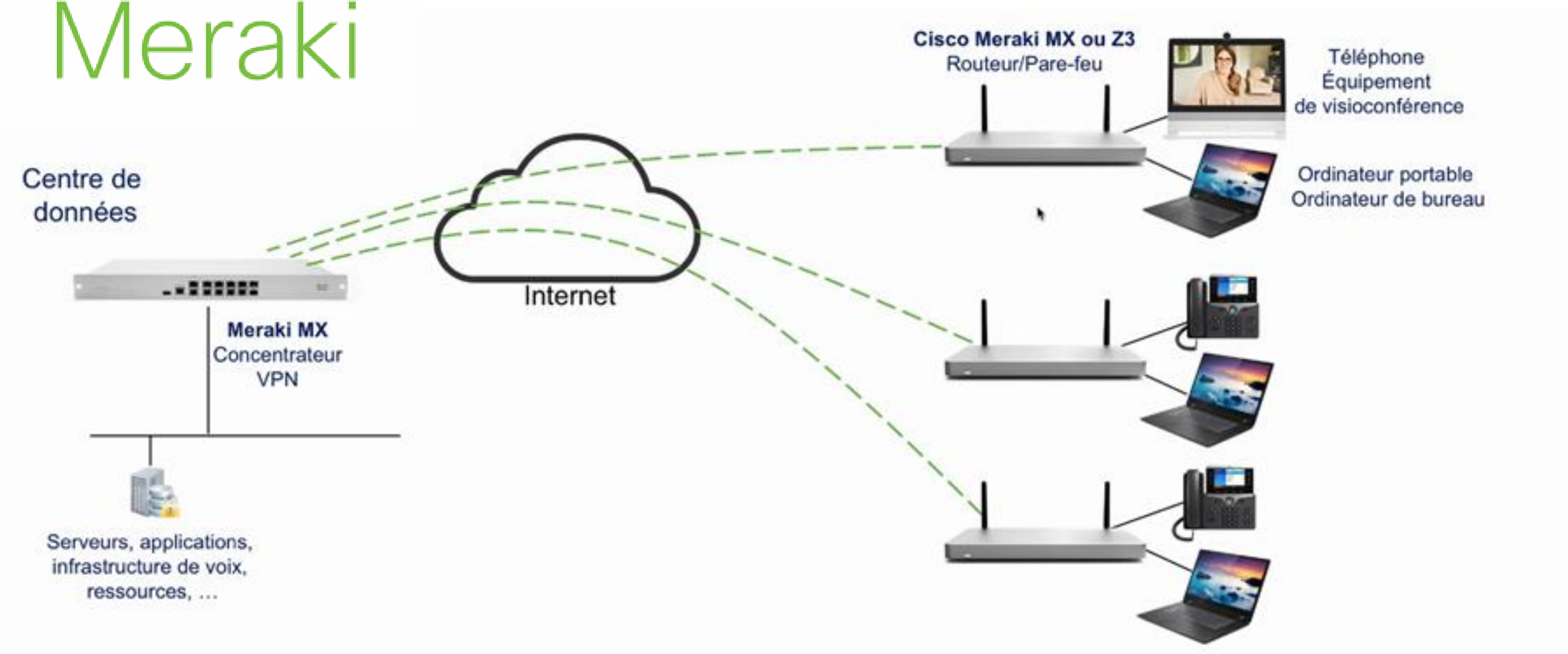
00:05:38

IPv4

System Scan:
Scanning system ...

10%

Specific to the Cisco Meraki product portfolio

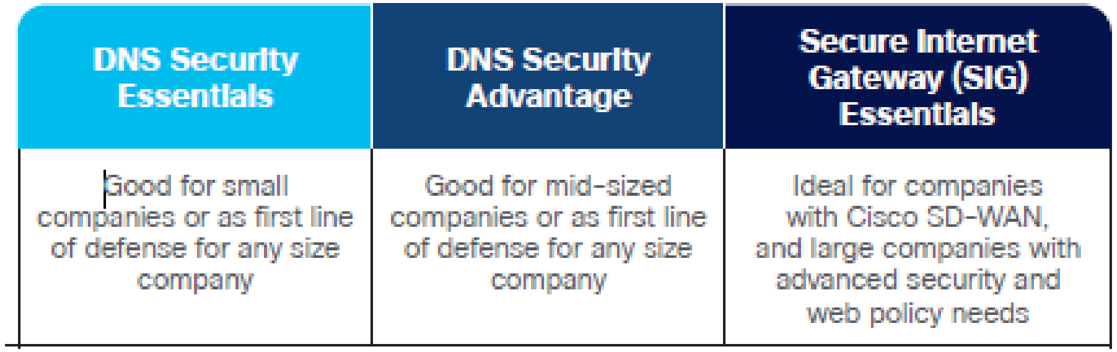


CISCO UMBRELLA

Secure Remote Working
Octobre 28, 2020
Roger Courchesne

Cisco Umbrella

- Acquisition de OpenDNS en 2015
- Offre une sécurité flexible,
  - « Cloud-Delivered Security », et considéré comme un « Cloud Access Security Broker" (CASB with SIG)
- Protection utilisateurs « On et Off Network »
- Licence
  - Essential
  - Advantage
  - Secure Internet Gateway

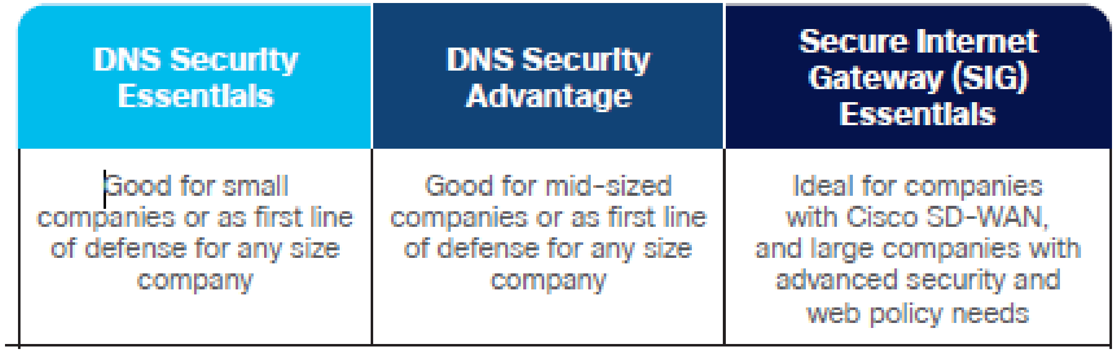


DNS Security Essentials	DNS Security Advantage	Secure Internet Gateway (SIG) Essentials
Good for small companies or as first line of defense for any size company	Good for mid-sized companies or as first line of defense for any size company	Ideal for companies with Cisco SD-WAN, and large companies with advanced security and web policy needs

Cisco Umbrelle Package Comparison

Cisco Umbrella

- Acquisition of OpenDNS in 2015
- Flexible security
  - Cloud-Delivered Security considered like a Cloud Access Security Broker (CASB with SIG)
- User protection on and out of the network
- Licenses:
  - Essential
  - Advantage
  - Secure Internet Gateway



DNS Security Essentials	DNS Security Advantage	Secure Internet Gateway (SIG) Essentials
Good for small companies or as first line of defense for any size company	Good for mid-sized companies or as first line of defense for any size company	Ideal for companies with Cisco SD-WAN, and large companies with advanced security and web policy needs

Cisco Umbrelle Package Comparison

Cisco Umbrella - Essential

CISCO
Cisco Umbrella

→ DNS Layer protection

SWG

- Blocks domains associated with phishing, malware, botnets, and other high risk categories (cryptomining, newly seen domains, etc.)
- Blocks requests to malicious and unwanted destinations before a connection is even established
- Stops threats over any port or protocol before they reach your network or endpoints
- Discovers and blocks shadow IT (by domain) with Apps Discovery report

ESI TECHNOLOGIES

Cisco Umbrella - Advantage

→ DNS (& IP) Layer protection

- Includes Essential features
- Blocks direct-to-IP traffic for CC callback that bypass DNS

→ Secure Web Gateway

- Selective proxy: URL inspection for suspicious domain by reputation
- Blocks URLs based on Cisco Talos & blocks files with AMP

→ Umbrella Investigate

- Allows the access to Investigate’s web console, interactive Threat Intelligence
- And allows the use of the Investigate On-Demand enrichment API

Cisco Umbrella – Secure Internet Gateway (SIG)

cisco

Cisco Umbrella

SWG

- → Visibility and control for all internet traffic across all ports and protocols… it's a full proxy!
- → Cisco Threat Grid cloud sandboxing to identify malicious behavior
- → Customizable IP, port, protocol, and application policies in the Umbrella dashboard
- → IPsec tunnel support to securely route traffic to cloud infrastructure
- → Automated reporting logs
  - › All this backed by Cisco Talos, threat intelligence teams
  - › With 100% uptime, Umbrella offers visibility and enforcement to protect users anywhere

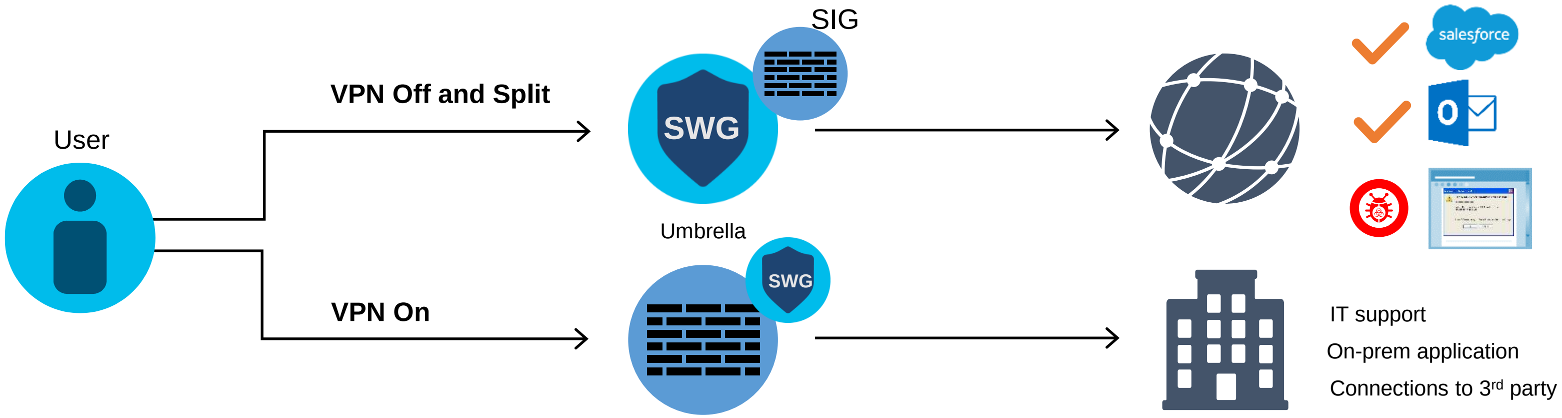
ESi TECHNOLOGIES

Cisco Umbrella

Flexible security protection on and off network

Consistent policies across remote locations

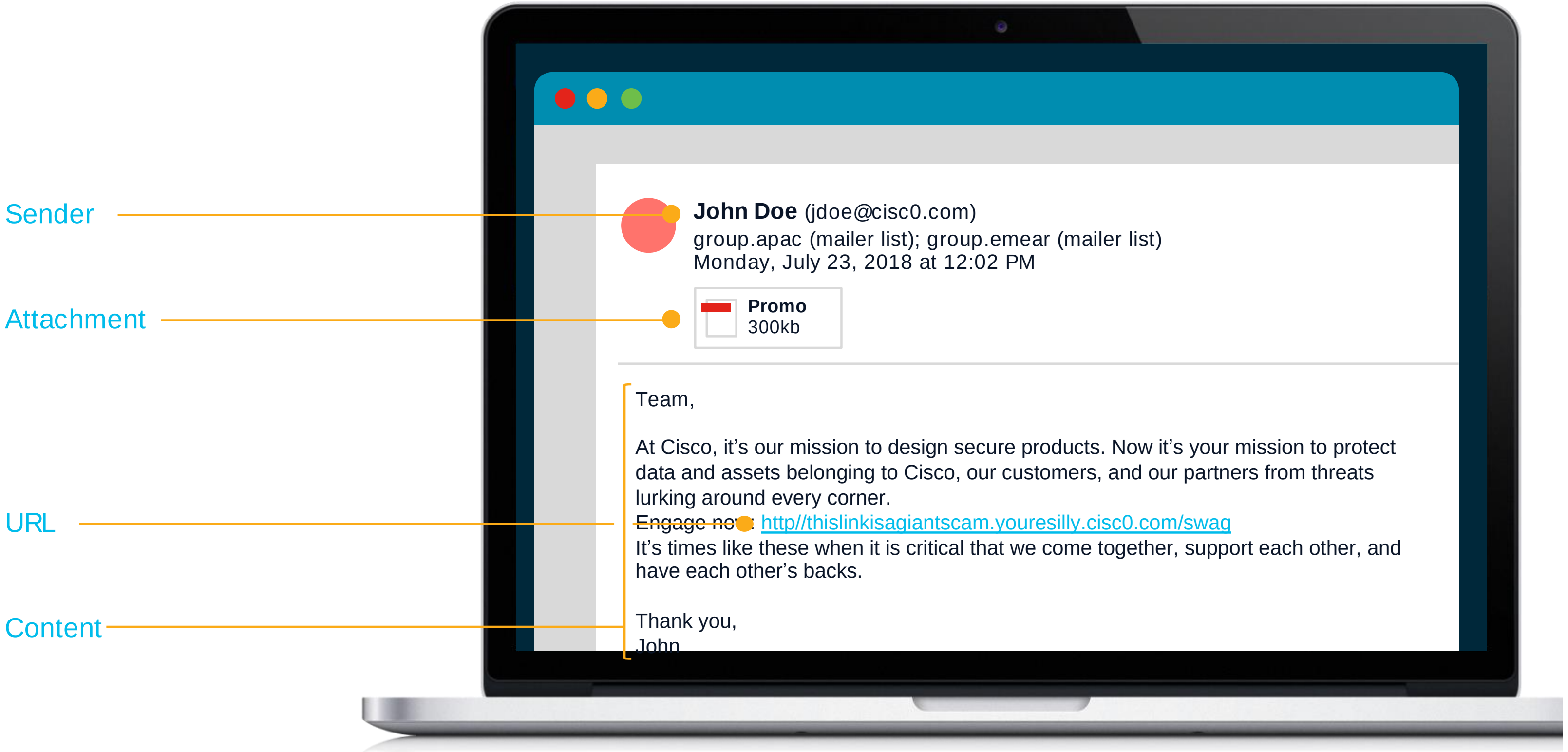
Better performance and user satisfaction everywhere



Cisco Cloud Email Security

Email: The first and last frontier

Still the # 1 threat vector



Sender

Attachment

URL

Content

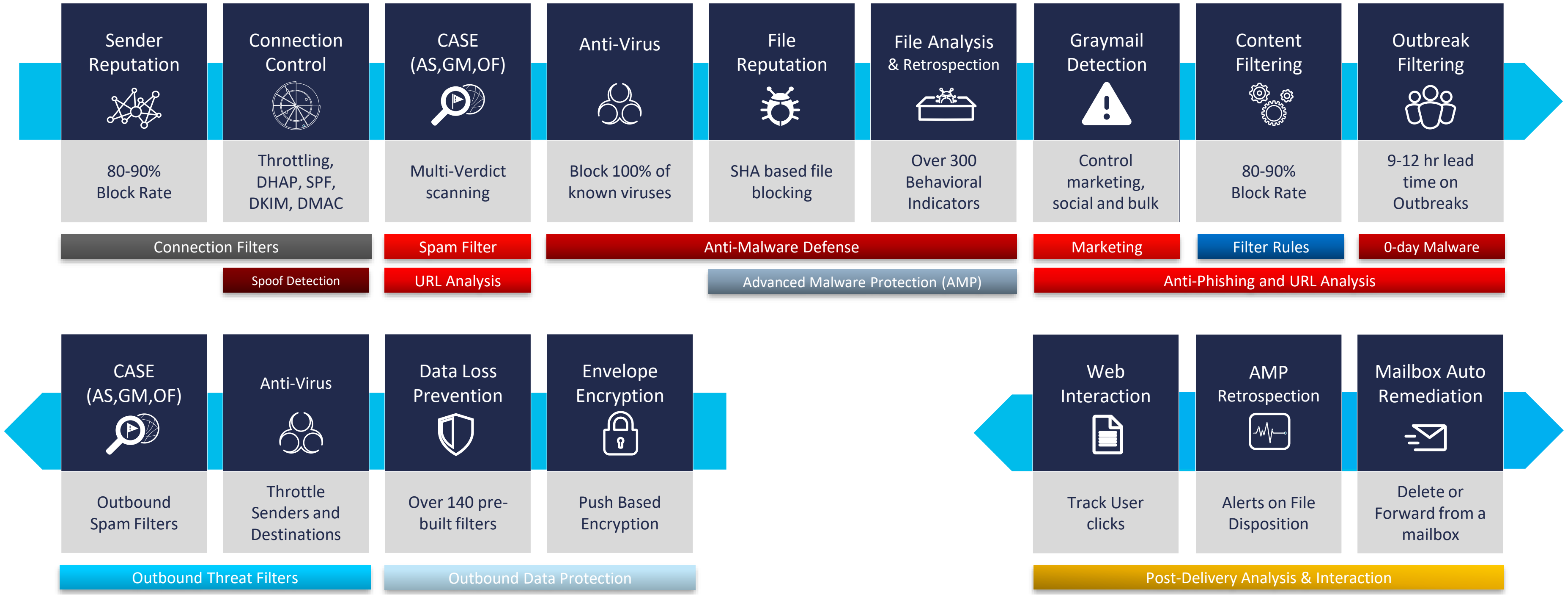
John Doe (jdoe@cisc0.com)
group.apac (mailer list); group.emear (mailer list)
Monday, July 23, 2018 at 12:02 PM

Team,

At Cisco, it's our mission to design secure products. Now it's your mission to protect data and assets belonging to Cisco, our customers, and our partners from threats lurking around every corner.
Engage now: http//thislinkisagiantscam.youresilly.cisc0.com/swag
It's times like these when it is critical that we come together, support each other, and have each other's backs.

Thank you,
John

Inbound and outbound email security



Sender Reputation — 80-90% Block Rate

Connection Control — Throttling, DHAP, SPF, DKIM, DMAC

CASE (AS,GM,OF) — Multi-Verdict scanning

Anti-Virus — Block 100% of known viruses

File Reputation — SHA based file blocking

File Analysis & Retrospection — Over 300 Behavioral Indicators

Graymail Detection — Control marketing, social and bulk

Content Filtering — 80-90% Block Rate

Outbreak Filtering — 9-12 hr lead time on Outbreaks

Connection Filters

Spoof Detection

Spam Filter

URL Analysis

Anti-Malware Defense

Advanced Malware Protection (AMP)

Marketing

Filter Rules

0-day Malware

Anti-Phishing and URL Analysis

CASE (AS,GM,OF) — Outbound Spam Filters

Anti-Virus — Throttle Senders and Destinations

Data Loss Prevention — Over 140 pre-built filters

Envelope Encryption — Push Based Encryption

Outbound Threat Filters

Outbound Data Protection

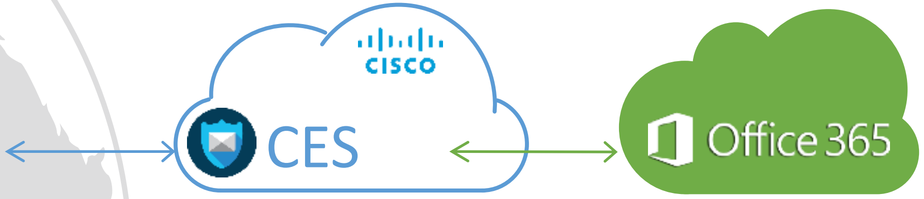
Web Interaction — Track User clicks

AMP Retrospection — Alerts on File Disposition

Mailbox Auto Remediation — Delete or Forward from a mailbox

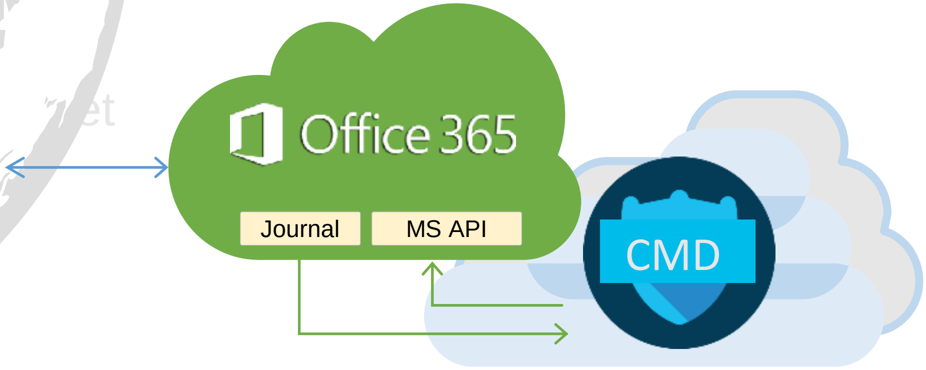
Post-Delivery Analysis & Interaction

Gateway vs. CESS



Cloud Email Security (Gateway)

1. MX record changed to CES address
2. CES scans messages and takes an action
3. Message is delivered



Cloud Mailbox Defense (CESS)

1. MX record is unchanged
2. Copy of each message is sent to CMD
3. CMD scans and remediates using an API

CMD: Cisco Mailbox Defense

Cisco Cloud Email Security

O365	Cisco Email Security w/ O365
Anti-spam filters	Anti-spam filters
Anti-virus protection	Anti-virus protection
Policy enforcement	Policy enforcement
Disaster recovery	Disaster recovery
Directory services	Directory services
Advanced threat protection	Graymail detection
Message tracking	Message tracking
	Outbreak Filters
	Email encryption
	Advanced Malware Protection
	Detailed reporting
	STIX and TAXI feeds
	Data loss prevention (DLP)

Cisco AMP: Advanced Malware Protection – Essential License

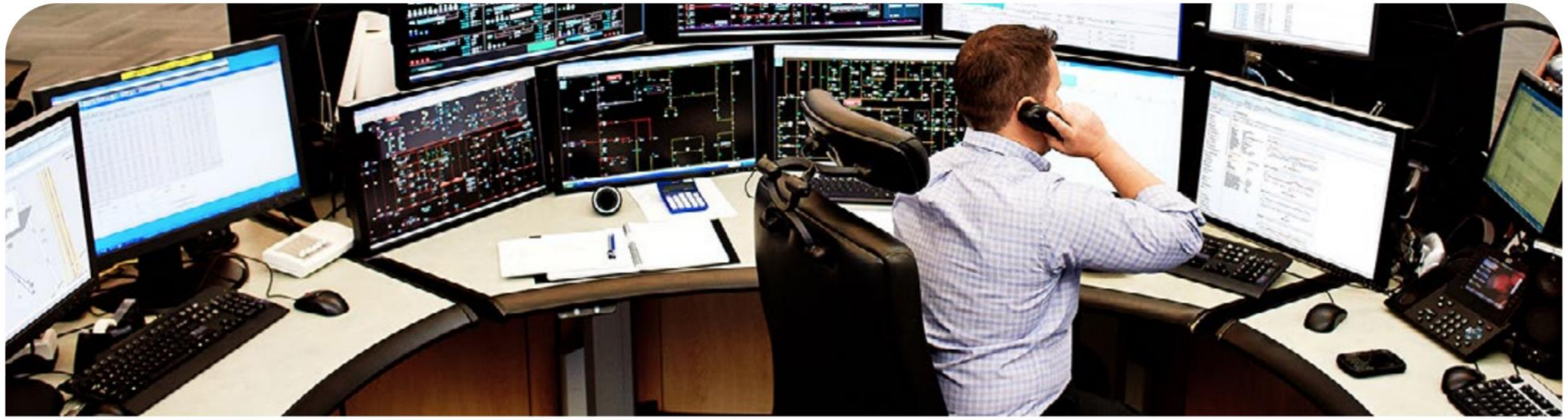
AMP for Endpoints

→ AMP for Endpoint : the last effective defense

- NGAV : it can replace your "Legacy Antivirus". He signature database resides locally on each endpoint
- Continuous Monitoring: monitors all endpoint activity and provides run-time detection and blocking abnormal behaviors
- Dynamic File Analysis: sandboxing environment, powered by Cisco Threat Grid, to analyze the behavior of suspect files
- Behavioral Monitoring: continually monitors all user and endpoint activity to protect against malicious behavior in real-time
- Vulnerability Identification: identifies vulnerable software across your environment to help reduce the attack surface
- Endpoint Isolation: capacity to isolate endpoints that have been compromised to stop threats from spreading

Cisco AMP: Advanced Malware Protection – Advantage License

AMP for Endpoints



- The highest level of AMP for endpoints and includes all capabilities offered in Essentials
  - + Advanced Search: Offers the ability to simplify security investigations, provides deep visibility into what happened on any endpoint at any given time
  - + Threat Grid Cloud: Provides an easy access to Cisco advanced malware analysis and threat intelligence portal

Cisco AMP (EDR/AV) Summary

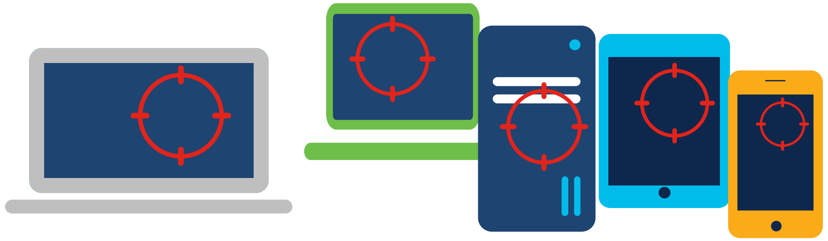
What is needed to detect and respond to all threats that can get in?

Deep Visibility

Be Context aware

Better Control

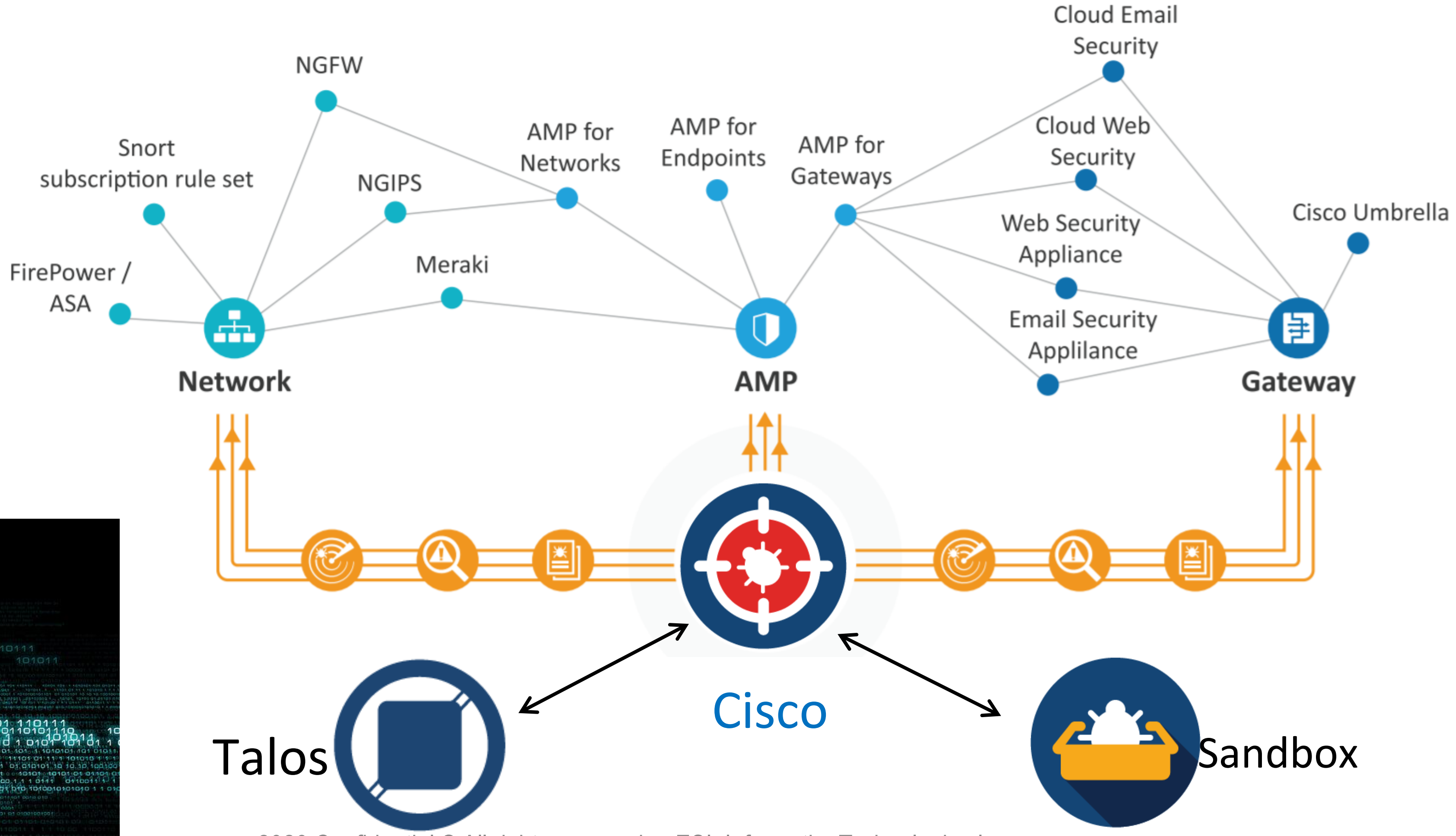
on the Endpoint



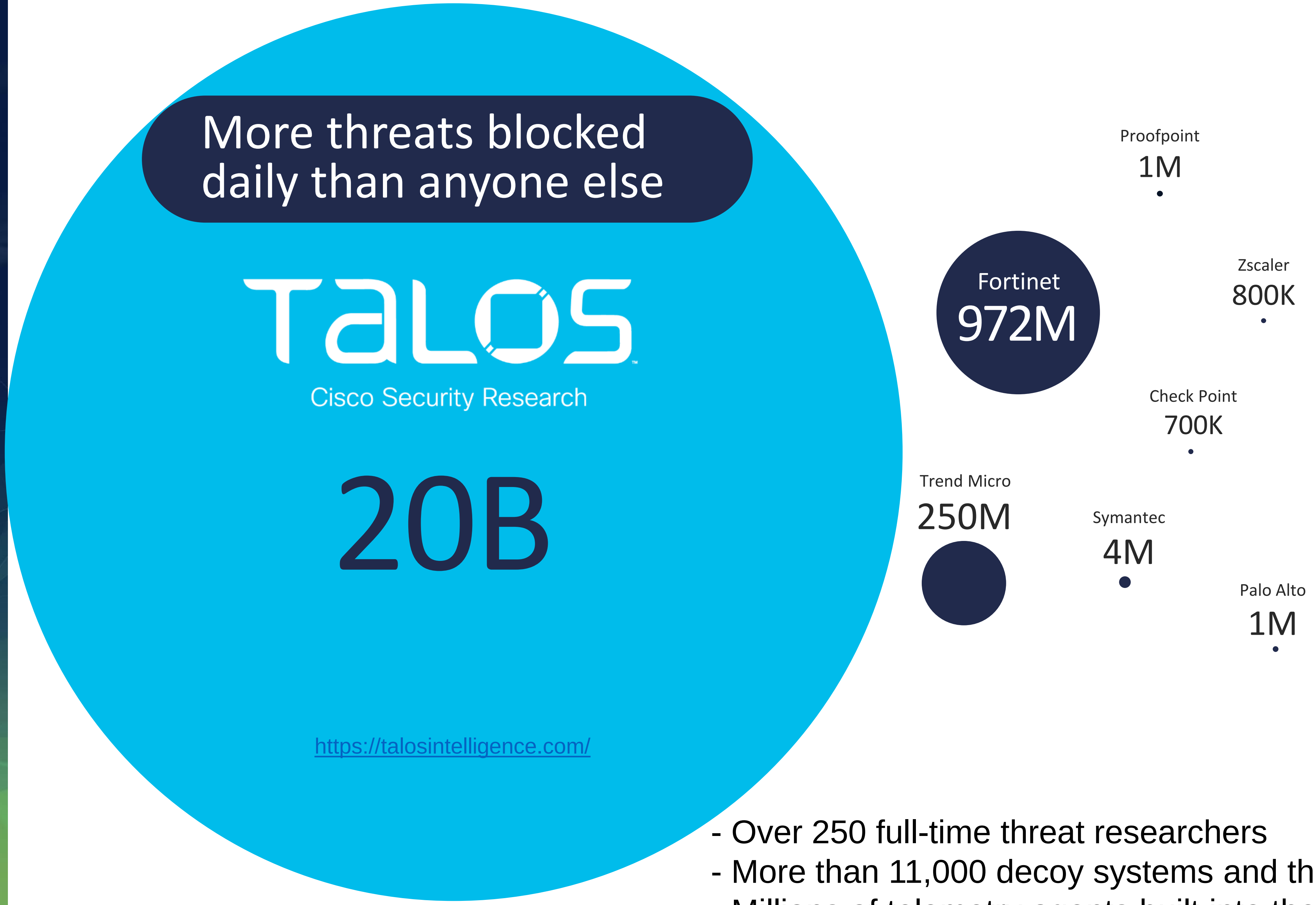
PC, Mac, Linux, Mobile

See once, block everywhere

Share intelligence across network, web, email and enpoints



More threats blocked daily than anyone else



https://talosintelligence.com/

- Over 250 full-time threat researchers
- More than 11,000 decoy systems and threat traps
- Millions of telemetry agents built into their products deployed across the globe

Cisco DUO

- 80% of security breaches involve compromised passwords [1]
- Modern, effective Multi-Factor Authentication
- Any apps, anytime, anywhere
- Duo protects your applications by using a second source of validation to verify user identity before granting access

Verify identity in seconds.

Protect any application on any device.

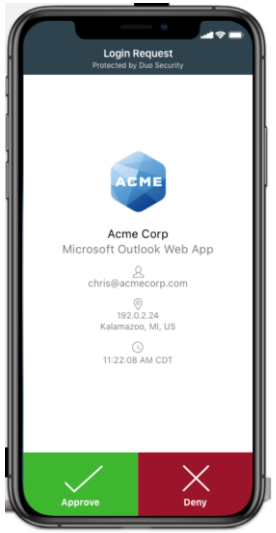
Easily deploy Duo in any environment.

2019 Data Breach Investigations Report, Verizon - via DBIR Interactive

Cisco DUO

Two-Factor Authentication methods

Supports every user: username/passord + 2FA



Login Request

Protected by Duo Security

Acme Corp

Microsoft Outlook Web App

chris@acmecorp.com

192.0.2.24

Kalamazoo, MI, US

11:22:08 AM CDT

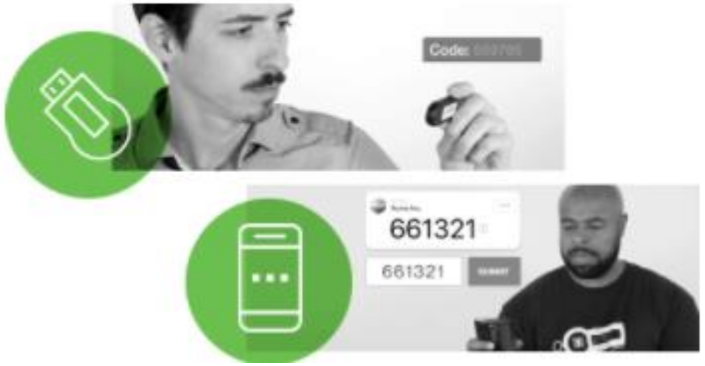
Duo Push

iOS, Android

U2F and Biometrics

macOS, Windows

Tokens and Passcodes



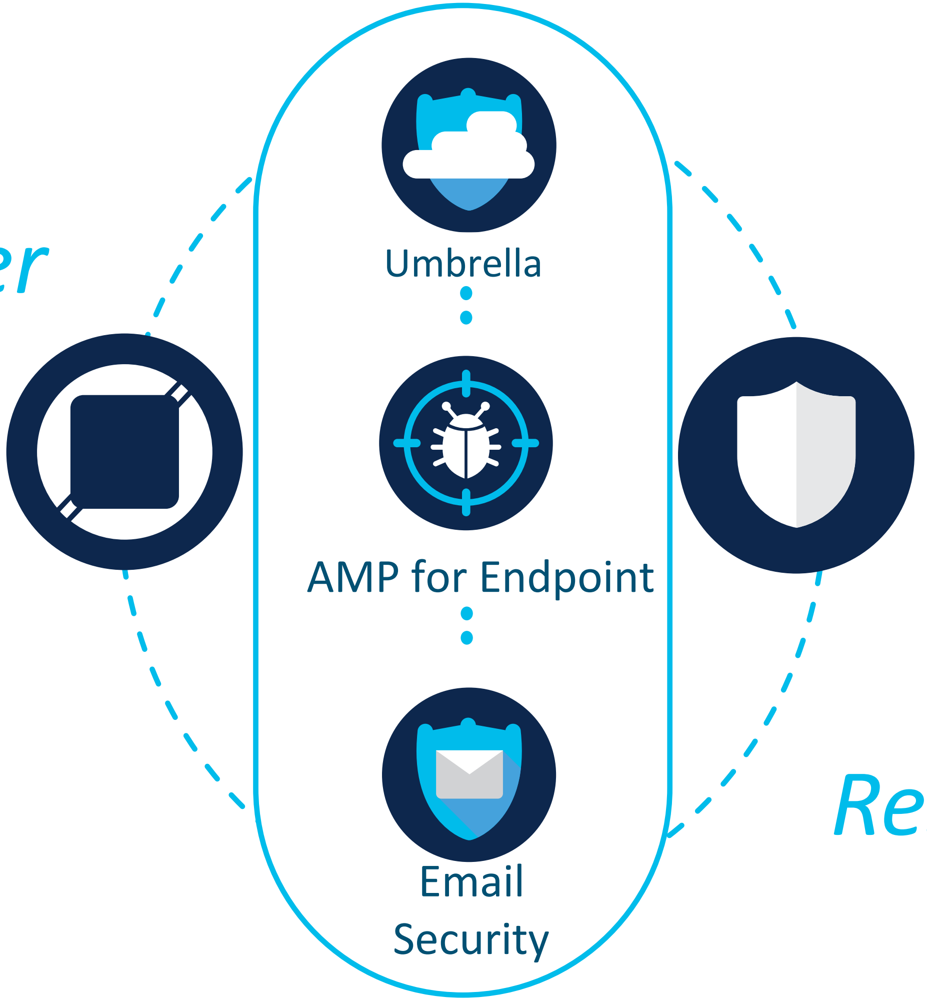
DUO DEMO TIME

https://demo.duo.com/

Need help?... The ESI support approach

Analysis & discovery	Architecture	Risk management	Operation Strategy
Existing solution Expansion Features	Partner solution Professional services, POC	Security solutions Alternatives	Document install. Easy to manage Training

Cisco’s Integrated Security Architecture

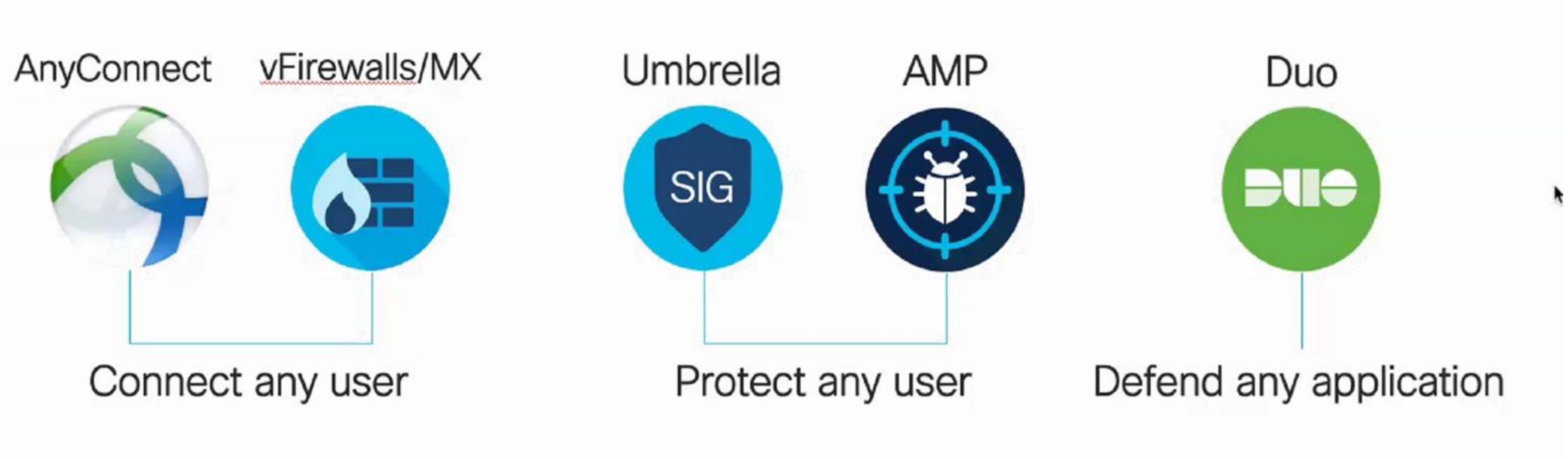


Defend better

Respond faster

Remember …

- → Ask for assistance with a secure telecommuting solution
- → Remember to protect your employees, whether or not they are connected to the network (Umbrella)
- → Have an email solution (CES)
- → Consider an NGAV or EDR (AMP)
- → Think about strong authentication (DUO)



Questions period

Thank you !