



Small Team, Small Budget, Immense Security Requirements

Best Practices for Securing Your Campus

Welcome!

AGENDA

- **Speaker Introductions and NFF Overview**
- **Small Team and Small Budget Challenges**
- **University of the District of Columbia Case Study**
- **Must Have Minimum Security Portfolio**
- **Meraki Security Portfolio**
- **Capture The Flag Mini-Lab**
- **Kahoot! (<https://kahoot.it/>)**
- **Questions and Answers**

SPEAKERS

- **Chris Peabody – Chief Strategy Officer, Networking For Future (NFF)**
- **Mike Rogers – Education Practice Lead, NFF**
 - **Former Executive Director IT, University of the District of Columbia**
- **Keyonna Brown – Cisco Security TSA**
- **Jiana Vargem – Cisco Meraki Specialist**
- **Lauren Sands – Cisco Meraki Solutions Engineer**
- **Yvonne Andersen – Cisco Territory Account Manager**
- **Gina Pappagallo – Cisco Virtual Account Manager**

OVERVIEW

Networking For Future, Inc. (NFF)

- > Founded in 1996
- > Headquartered in Washington, DC
- > 130+ Employees
- > ISO 9001:2015 Certified
- > 77% of workforce hold industry certifications

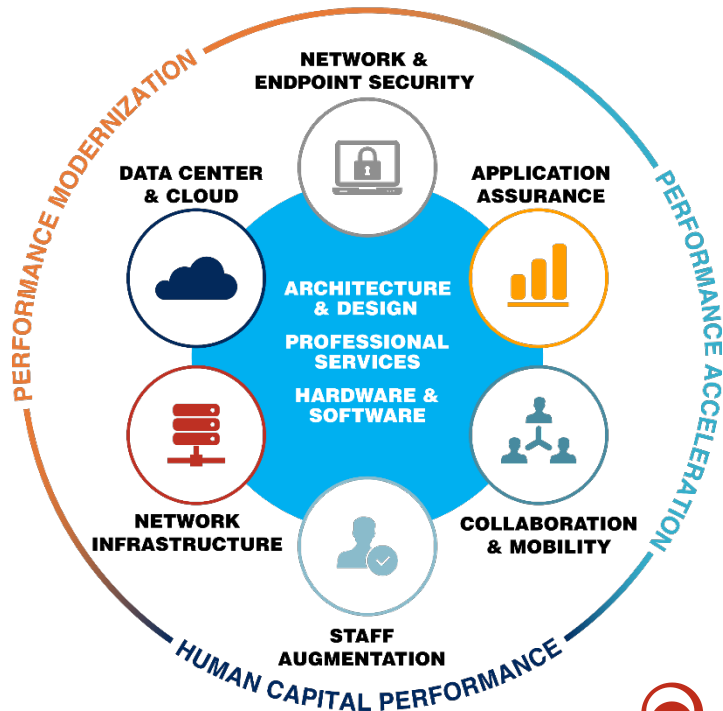


CISCO OUTSTANDING
SOLUTIONS PARTNER
OF THE YEAR 2016



CISCO TOP-FIVE
MID-ATLANTIC SLED
PARTNER 2019 & 2020

IT Business Solutions





Small Team and Small Budget Challenges

Chris Peabody
Chief Strategy Officer
Networking For Future (NFF)

The way we
do business is
changing.



THERE ARE INCREASING DEMANDS ON SECURITY TEAMS

Business Evolution



Unlimited
devices



Transition to
the cloud



Distributed
workforces

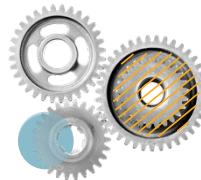


Digital
transformation

Security Pressures



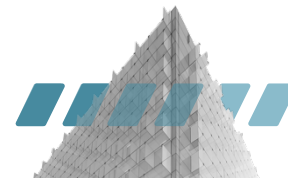
Too little
visibility



Too little
integration



Too few
experts

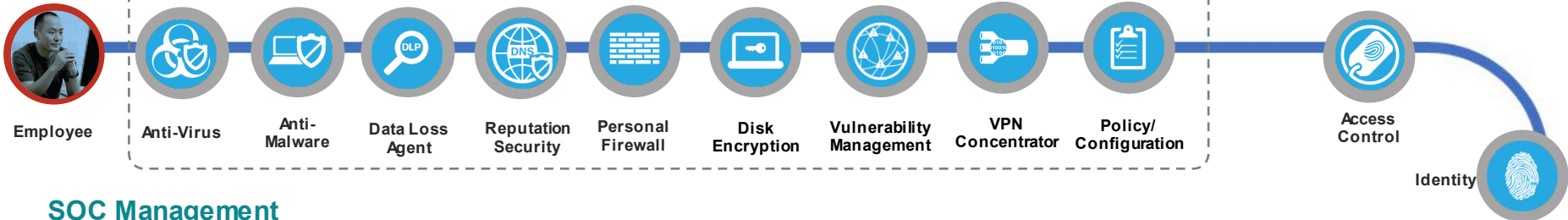


Too much
exposure

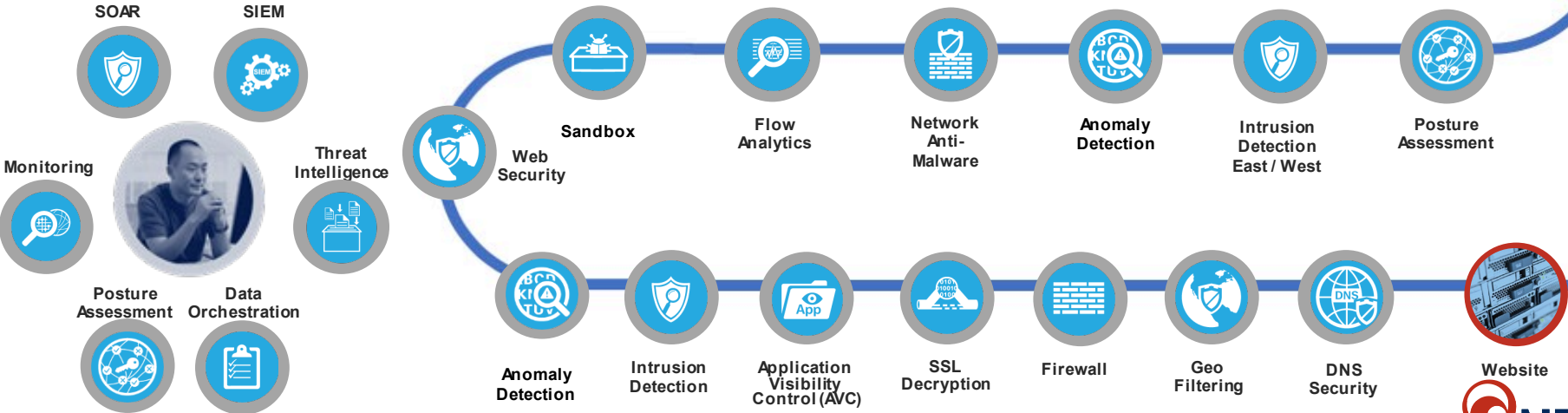
DEFENSE IN DEPTH ON YOUR CAMPUS IS COMPLICATED!



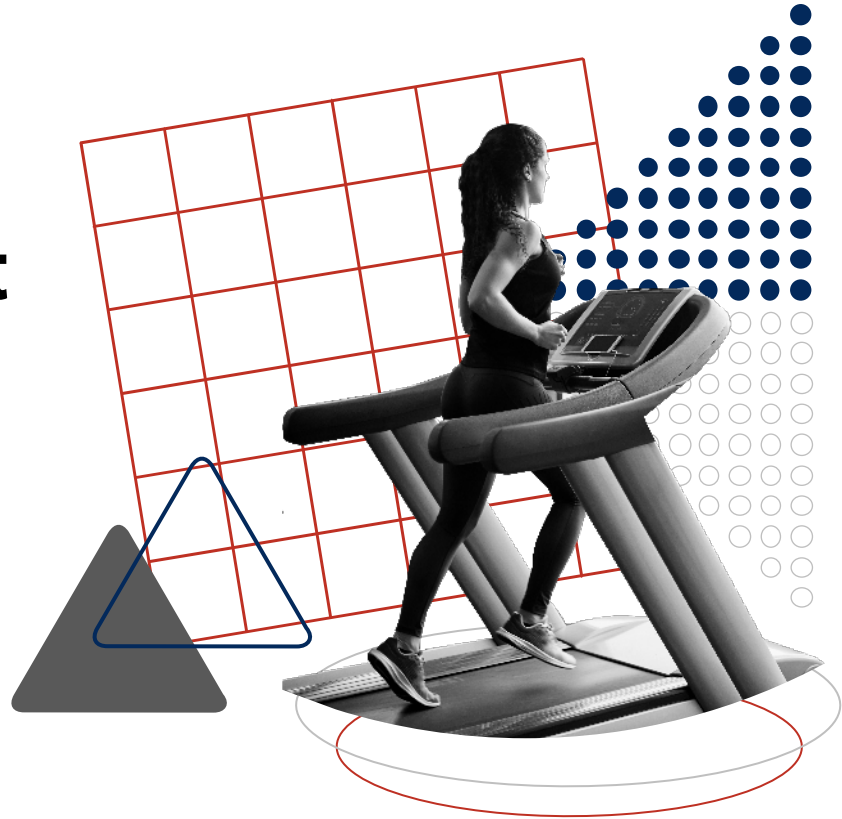
ENDPOINT



SOC Management



**You're doing your best
to keep up, but it's a
never-ending grind.**



BIG SCHOOL / SMALL SCHOOL SAME SECURITY REQUIREMENTS

Challenge

- ✓ **Regardless of the size of your school, budget or staff, all institutions have the same security needs and require comprehensive network and security architecture, engineering and ongoing operational support.**

BIG SCHOOL / SMALL SCHOOL SAME SECURITY REQUIREMENTS

What You Don't Need

- ✓ **Big budgets**
 - ✓ Start with a free high level security assessment from Cisco
 - ✓ Request a more granular network and security assessment from NFF
 - ✓ SecureX and Talos are free with purchase of any single Cisco security solution
- ✓ **All the answers**
 - ✓ Find trusted partners to help find the right path for your campus
- ✓ **A large staff**
 - ✓ Integrated, simple to manage solutions reduce the need for large security teams

BIG SCHOOL / SMALL SCHOOL SAME SECURITY REQUIREMENTS

What You Need – An NFF and Cisco-Enabled Easy Button



NFF

- ✓ You need an experienced support team
- ✓ What do you have and what is the status of your IT eco-system
- ✓ Ongoing real-time visibility and alerting



Cisco and Meraki

- ✓ Secure, robust, reliable and integrated hardware and software solutions



Security Transformation: University of the District of Columbia

Mike Rogers

Education Practice Lead, Networking For Future

Former Executive Director IT, University of the District of Columbia



Security Transformation: University of the District of Columbia



University of the District of Columbia (UDC) Overview

- Established by Abolitionist Myrtilla Miner in 1851
- Only Public University in the Nation's Capital
- Committed to a Mission of Education, Research, and Community Service

Where We Started Our Security Journey

- "Flat" Network – Little to no separation of network users / devices
- No Threat Inspection – Unable to see / address bad actors
- No Identity – Unable to determine who / what is on the network

Where We Are Today On Our Security Journey

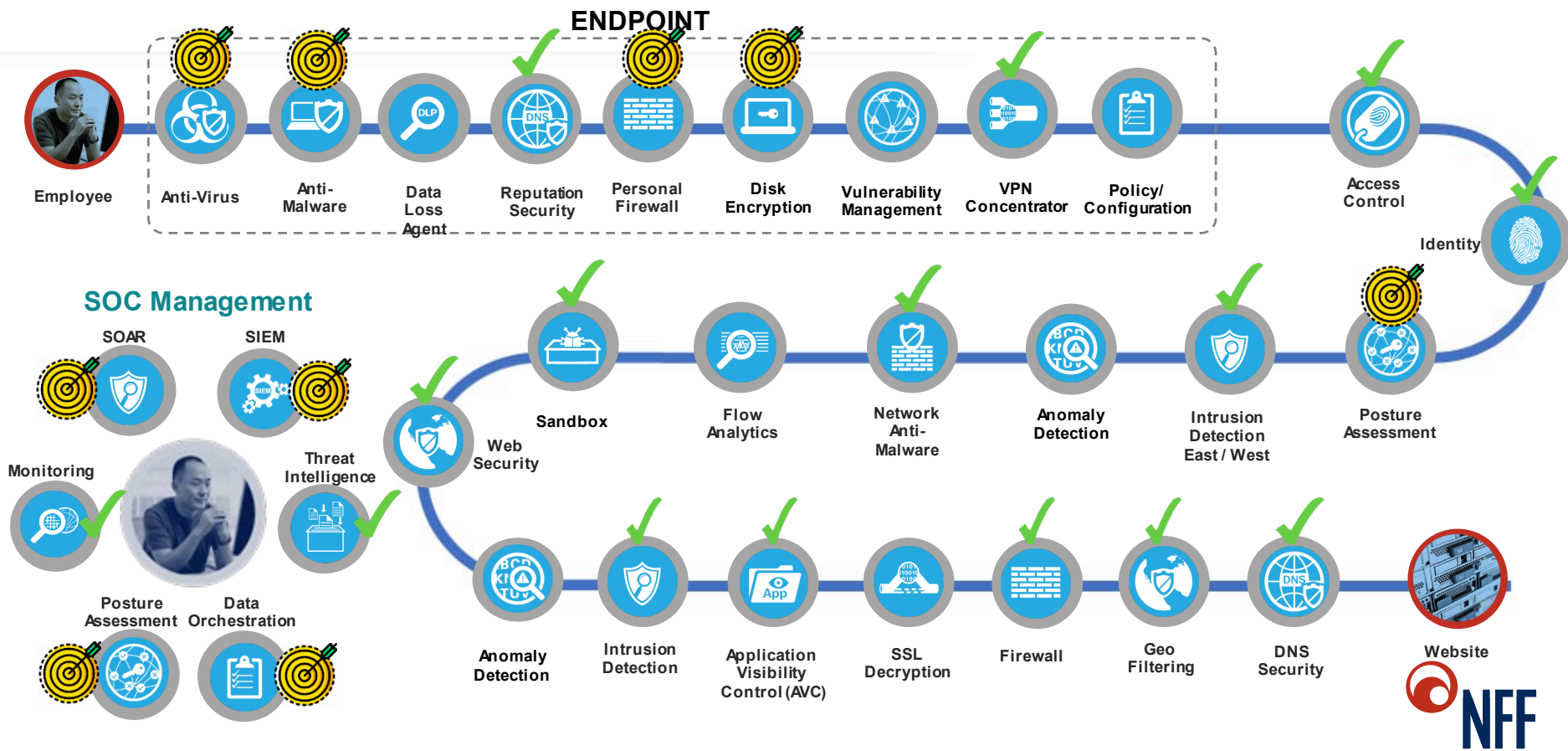
- Macro and Micro Segmentation
- Threats Mitigated at Multiple Layers (IPS / Malware / DNS)
- End-to-End Visibility of Who and What is on the Network

What's Left On Our Security Journey

- Utilize Segmentation to Further Restrict Access
- Endpoint Security Management
- Multi-Factor Authentication
- Automation – Turn the data to quick action



UDC CASE STUDY MAPPED TO DEFENSE IN DEPTH



MIKE'S TOP SECURITY TIPS

- ✓ **Get Data First**
- ✓ **Triage Weak Points**
- ✓ **Intelligence and Response Come Next**
- ✓ **Make It Easy on Your Users**
- ✓ **Inform, But Don't Spam**
- ✓ **Prevent Hurdles**

Must Have Minimum Security Portfolio

Best Practices for Building a Secure Campus

Keyonna Brown

Cisco Security TSA

Cisco Systems

Taylor Tenca

Virtual Sales Specialist

Cisco Systems

Must Have Minimum Security Portfolio

Next Generation Endpoint and DNS Layer Security

Keyonna Brown

Technical Solutions Specialist – SLED East

4-13-2022



Agenda

- What are the minimum security must haves – and why?
- What is Cisco Umbrella?
- What is Secure Endpoint?
- Next steps for Umbrella and AMP
- What is Duo security?
- Next steps for Duo

Why is cloud security so important today?

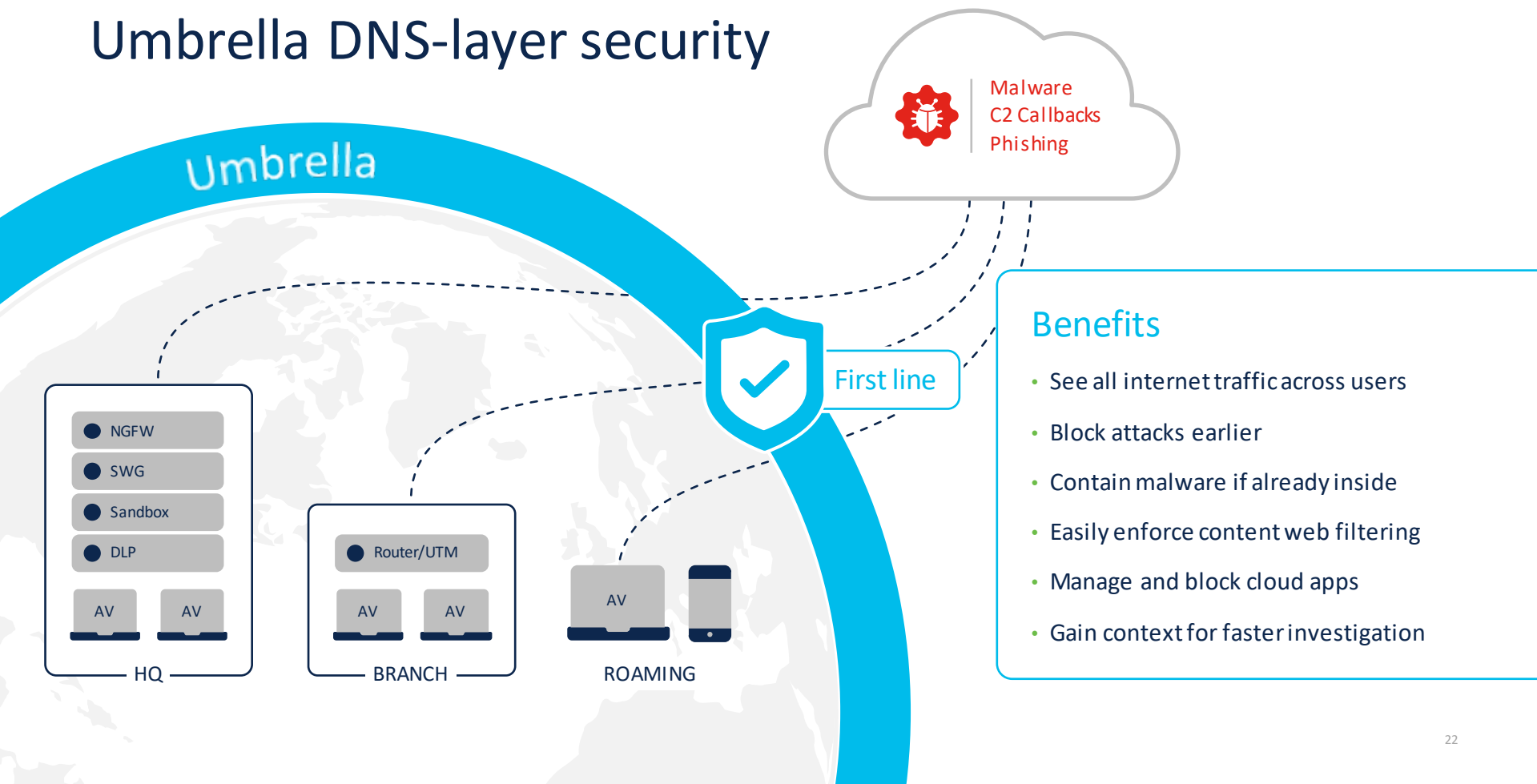
- ▶ Ease of use deployment
- ▶ Intuitive administration
- ▶ Cloud provider responsibility vs consumer responsibility
- ▶ Increasing lead times on physical appliances
- ▶ Resource limitations on virtual appliances



What is our first security
must-have solution?



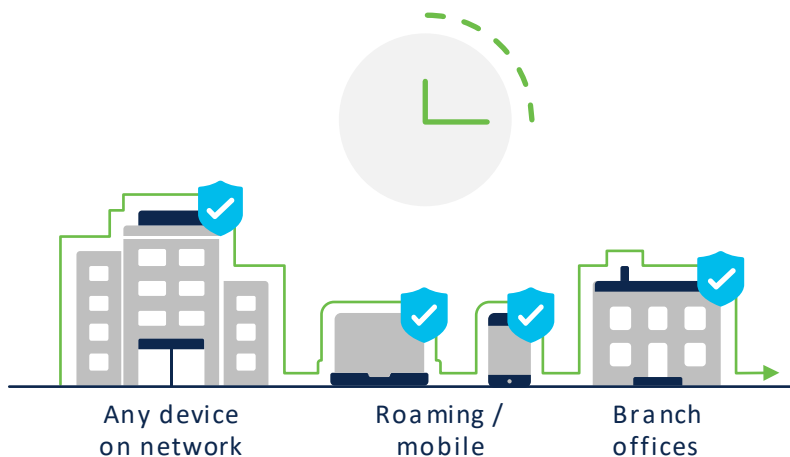
Umbrella DNS-layer security



Large, global footprint



Enterprise-wide coverage in minutes



On-network coverage

- With one setting change
- Integrated with Cisco SD-WAN, Cisco ISR 1K and 4K series, Cisco Meraki MR, and Cisco WLAN controllers

Off-network laptop coverage

- With Secure VPN (AnyConnect) client integration
- Or with any VPN using lightweight Umbrella client
- Or with Umbrella Chromebook client

Off-network mobile coverage

- With Cisco Security Connector

Built into foundation of the internet

Destinations

Original destination or block page



Safe
Original destinations



Blocked
Modified destination

Security controls

- DNS layer enforcement
- Risky domain inspection through proxy
- SSL decryption available

Selective proxy
Deeper inspection

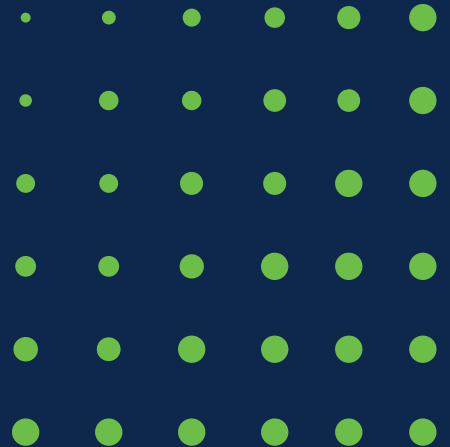


Internet traffic

On and off-network



What is our second
security must-have
solution?



The Cisco Secure Endpoint solution

Secure your endpoints while turbocharging your security operations



Stop Threats Before Compromise

Quickly detect advanced attacks such as ransomware with multifaceted prevention, attack surface reduction, and posture assessments.

Get the security expertise you need with endpoint detection and response managed by a team of dedicated Cisco experts or your SOC team.



Remediate Faster and More Efficiently

Decrease incident response time by up to 97% with advanced Endpoint Detection and Response (EDR) and built-in Extended Detection and Response (XDR) capabilities.

Drastically reduce detection and response times with Cisco specialists that quickly investigate and remediate threats



Maximize Your Security Operations

Improve your security operations effectiveness by up to 86% and simplify your security by eliminating complexity and enhancing SecOps productivity

Focus on the most important threats and gain always-on security operations with accelerated EDR

Prevent

One-to-One Signatures

Fuzzy Finger-printing

Machine Learning

Device Flow Correlation

Exploit Prevention

System Processes Protection

Malicious Activity Protection

Detect

Vulnerable Surface Detection

Low Prevalence

Local Signature Detection

Indicators of Compromise

Respond

Endpoint Isolation

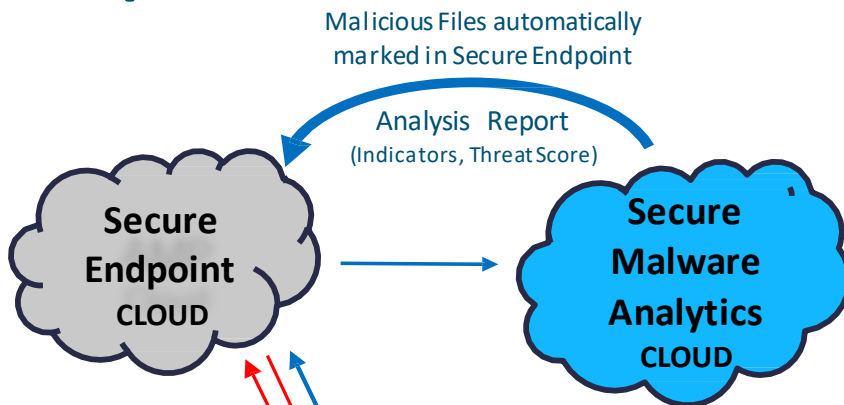
Orbital Search

How does Secure Endpoint work?

Public Cloud

Information stored in the Cloud:

- Endpoint Information, Files
- Policies & Custom Detections
- File Trajectory, Root Cause
- Reporting, IOC Scans



Information stored in TG:

- Files and Device GUID
- Analysis Results and Reports

Your Organizations' Perimeter

Disposition
(unknown, malicious, clean, block)

File Reputation Check
(includes 1-1 SHA256, Ethos, Spero, DFC)

Analysis Request
(includes the file)

File Fetch
(suspicious file)

Retrospection and Policy Updates
via periodic updates

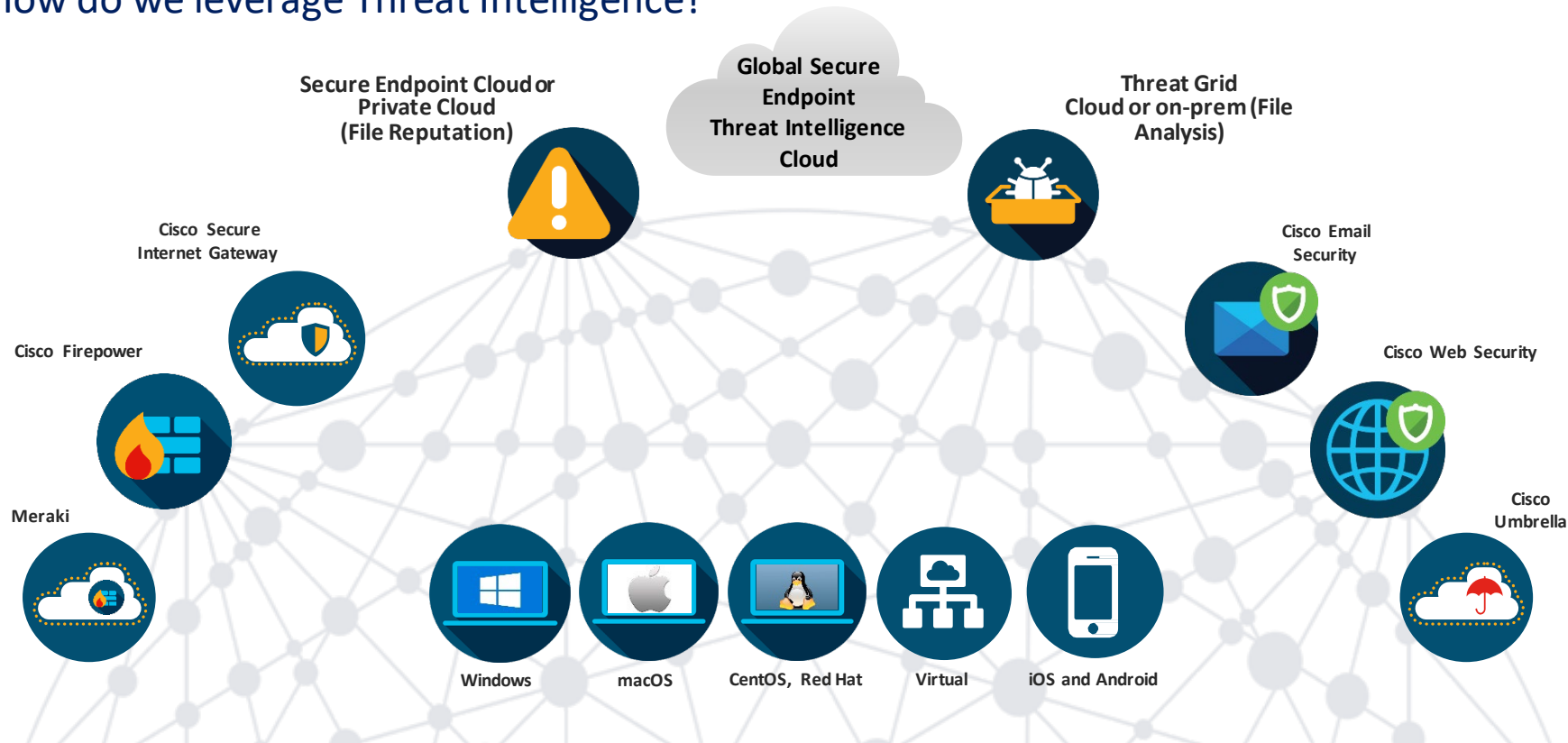


Secure Endpoint Connector
(Endpoint)

← File Analysis File
← Reputation

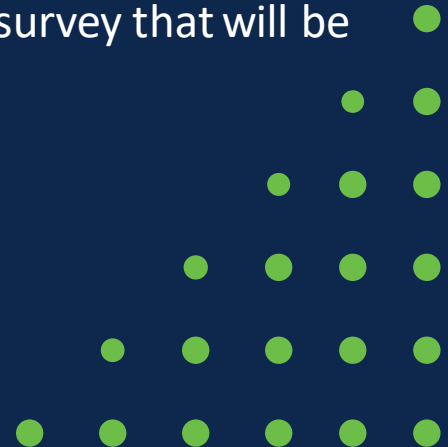
Secure Endpoint Everywhere Architecture

How do we leverage Threat Intelligence?



Next Steps

- ▶ Ask your questions in the Q&A section!
- ▶ If you would like to see one or both of these solutions in action – let us know!
- ▶ Please complete the survey that will be shared afterwards



References:

- Secure Endpoint at-a-glance:
 - <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/at-a-glance-c45-731874.html>
- Umbrella at-a-glance:
 - <https://learn-umbrella.cisco.com/datasheets/cisco-umbrella-at-a-glance>
- Secure Endpoint licensing:
 - <https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/licensing.html>
- Umbrella licensing:
 - <https://umbrella.cisco.com/products/umbrella-enterprise-security-packages>

Security at all Levels with Duo Security

Taylor Tenca

Virtual Sales Specialist

4-13-2022



Duo Security

Access Security for Everyone, from Any Device, Anywhere



Security at All Levels

How Duo protects your users and applications in 5 steps



Duo is Agnostic

All authentication types can be protected with one solution

Several Auth Methods: Protect all your users easily



Push



**Soft
Token**



SMS



**Phone
Call**



U2F



Wearables



Biometrics



**HW
Tokens**

Out-of-the-box: Protect all your apps easily



VPNs



Windows



**Cloud
Apps**



**Custom
Apps**



Web Apps



SSO



Unix SSH



Legacy

Duo for Free?

Duo 30 day free trial to get acquainted to this security

Why Try Duo?

Duo is easy to set up and use. With Duo, you can:

- Meet compliance requirements with multi-factor authentication.
- Get full visibility into every endpoint accessing your applications.
- Check your users' device health with advanced device trust features.
- Set up cloud-based SSO with the flip of a switch.
- Customize security policies to fit your business.
- And much more.

<https://duo.com/trial>



Meraki Security Portfolio

Jiana Vargem

Cisco Meraki Specialist

Cisco Systems

David Sherman

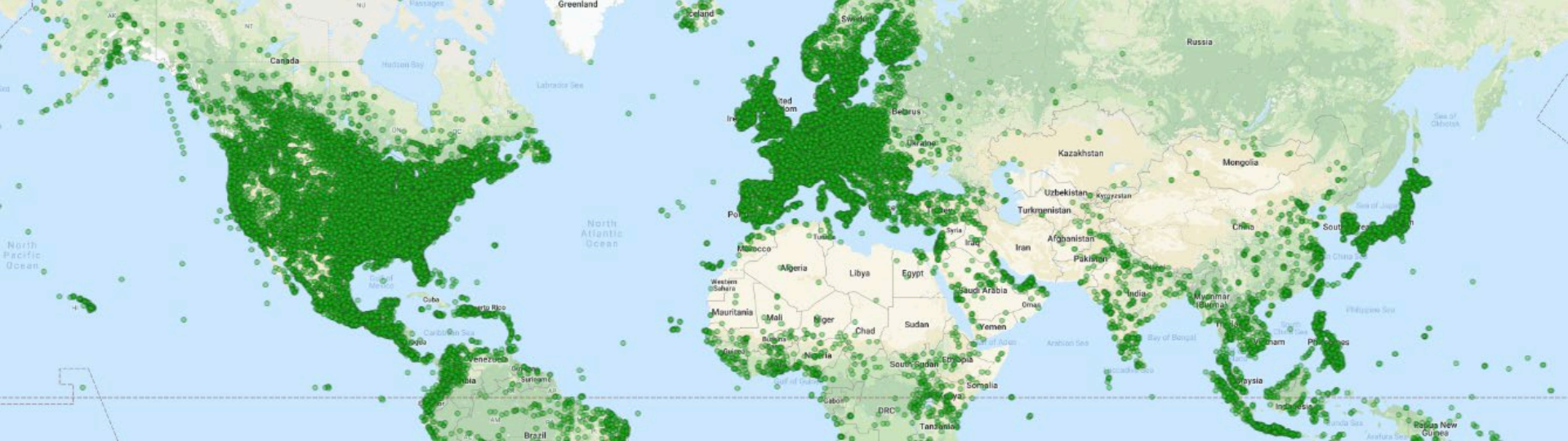
Cisco SLED Account Manager

Cisco Systems



Meraki

Jiana Vargem
DC, MD, VA
David Sherman
KY, WV, TN



Built on the Industry's Most Trusted Cloud Infrastructure



10+ years experience
scaling cloud infrastructure

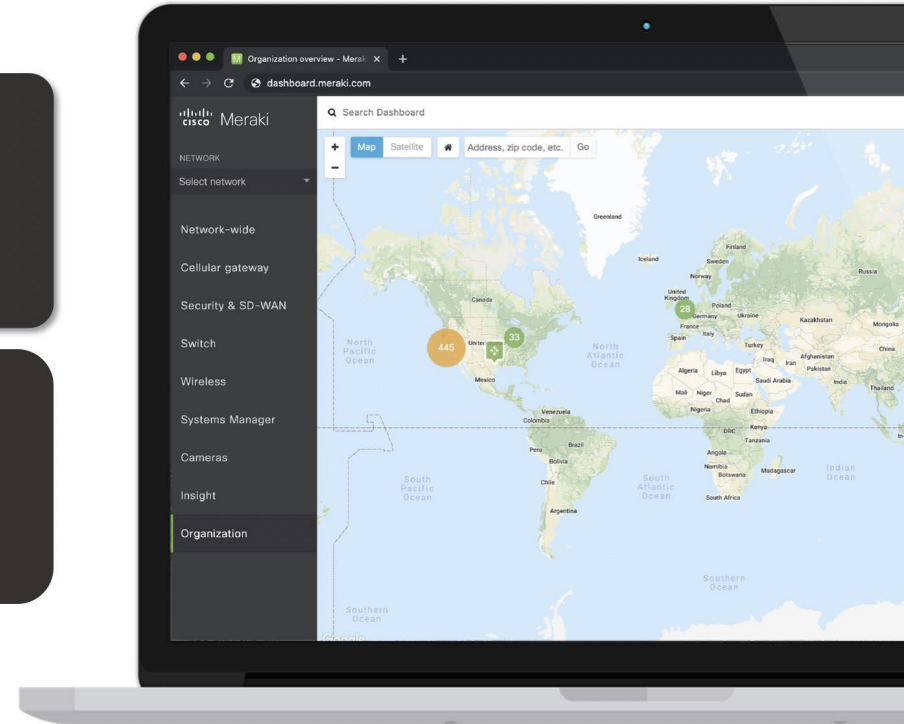


Served 500,000+
customers globally



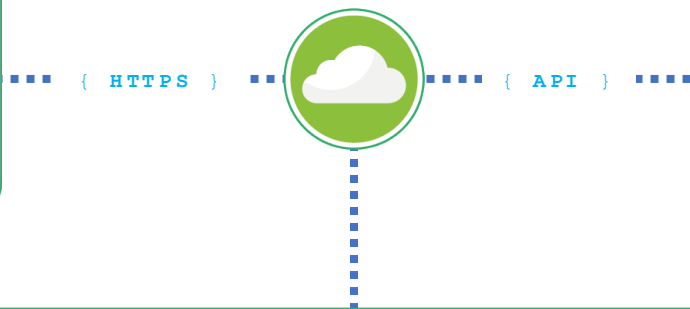
Proven in 20,000+
location deployments

A Complete Cloud-Managed IT Portfolio

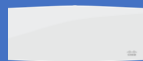
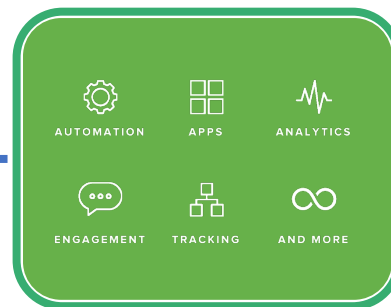


A Platform Approach to SD-WAN

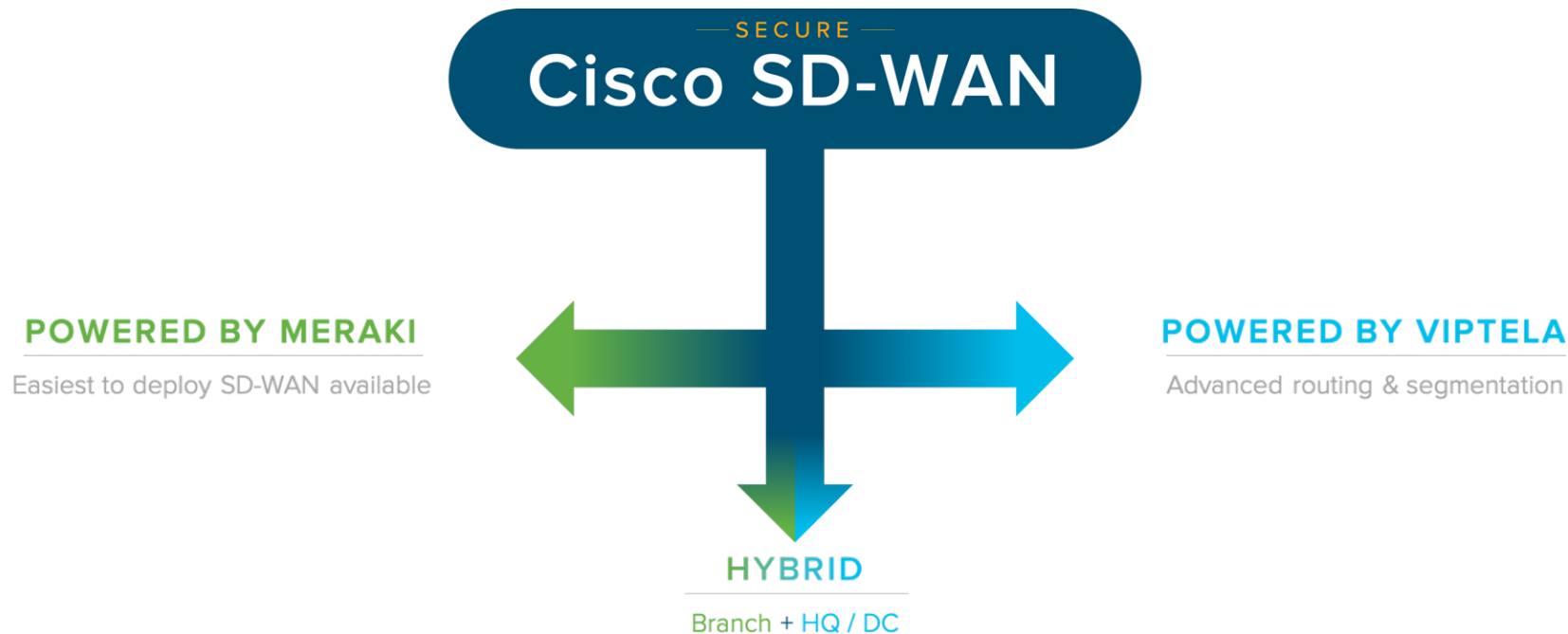
**OUT-OF-THE-BOX
MANAGEMENT & ANALYTICS**



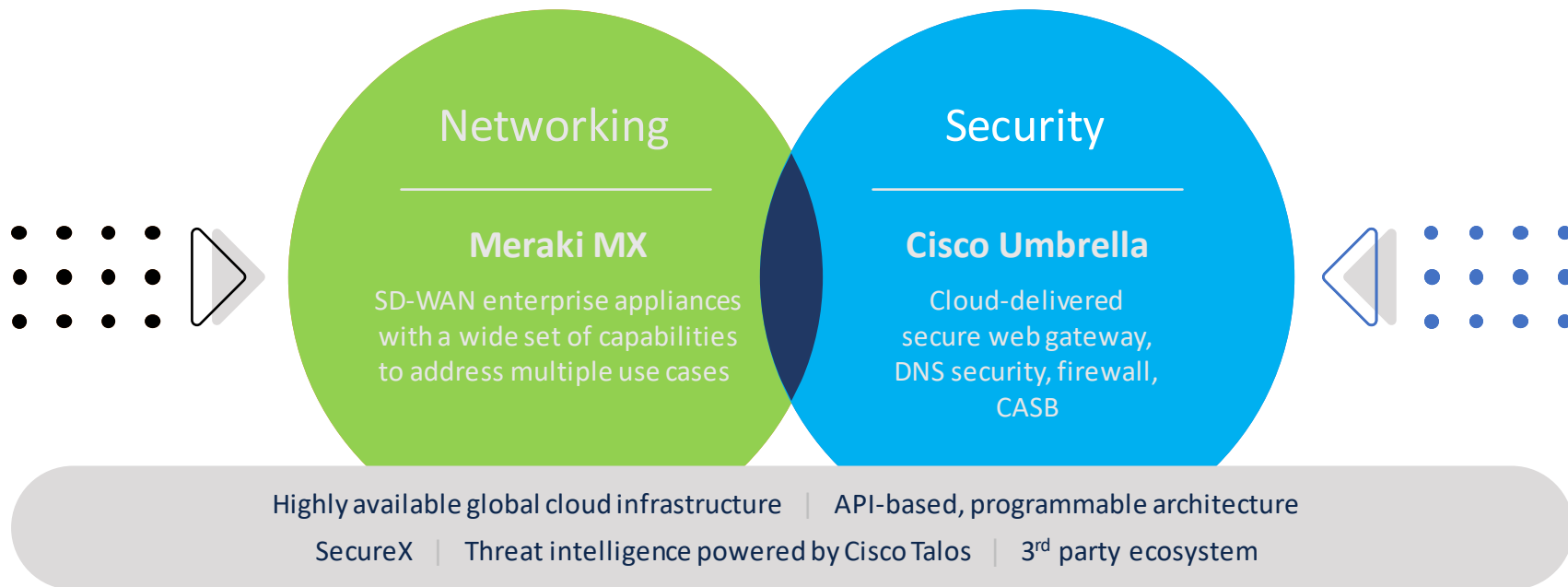
**DIGITAL BUSINESS
POWERED BY MERAKI**



A Complete Market Leading Solution



Cisco delivers on SASE convergence





Industry leading SD-WAN meets industry leading security



Meraki MX

On-prem security and SD-WAN

- Monitor and block malware and malicious traffic
- Restrict unauthorized users
- Prevent unwanted content or applications
- Firewall incoming traffic and VLAN to VLAN traffic
- Use secure site-to-site/in-tunnel VPN
- Detect and prevent intrusions (IDS/IPS)



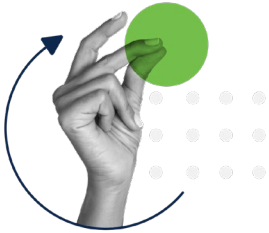
Cisco Umbrella

Cloud-native security

- Secure users at the edge with the best detection
- Increased reliability and performance with the speed and scale of the cloud
- Easily extend protection off-network
- Reduce the time, money, and resources required to identify and remediate threats

Meraki MX and Cisco Umbrella integration

A simple and flexible way to deploy Umbrella across MX devices



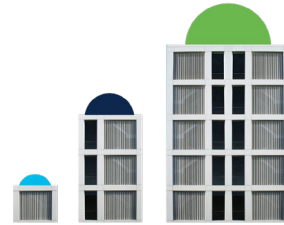
Simple

- Fast protection of users across your distributed network with simple, flexible deployment options
- Higher security efficacy with less effort and less resources



Secure

- Multiple layers of security from a single, cloud-native service
- Flexible policy enforcement for any use case
- Off-network protection using Umbrella without a VPN
- Continuous protection with automatic failover



Scalable

- Consistent high-performance security for multi-cloud demands
- SSL decryption at a scale not possible with on-prem hardware



Capture The Flag

Lauren Sands

Cisco Meraki Solutions Engineer

Cisco Systems

Jiana Vargem

Cisco Meraki Specialist

Cisco Systems

click on "Login here" and provide right credentials

← → ↻ 🏠 <https://try.meraki.letsplayctf.io/login> ⋮ ☆ 📄 🌐 🌐 ☰

cisco Capture the Flag - Meraki [Login](#) [Registration](#) [Scores](#) [FAQs](#)

🔒 Authentication Required


🔑 Login

[Don't Have an account? Sign Up](#) [Forgot your password?](#)

[Contact Us](#) | [Privacy Policy](#) | [Cookie Policy](#) | [Trademarks](#) | © 2021 Cisco and/or its affiliates. All rights reserved.

[Privacy - Terms](#)

read incoming transmission from boss

 Capture the Flag - Meraki

HomeMissionsScoresFAQs

masterchief

Incoming transmission

> Establishing secure communication channel, please wait...\

***** Begin secure message *****

Greetings Agent masterchief

> I am your new employer. You may call me MangoMan.

> I hope you're well rested. We have a lot of work to do.

> I have several assignments which require your... "special skill set".

> Should You choose to accept this quest, You can get more information about this quest and view your current missions by going to the "MISSION BRIEFING ROOM" (here we shall call it "HOME").






> This message will self-destruct immediately after you move out of this page.

> GOOD HUNTING!

- MangoMan


***** End of transmission *****

Go to the Mission Briefing Room




Contact Us | Privacy Policy | Cookie Policy | Trademarks | © 2021 Cisco and/or its affiliates. All rights reserved.

explore home portal

 Capture the Flag - Meraki

Home Missions Scores FAQs

masterchief



Welcome masterchief

Player	Current Level	Flags Captured	Hints Taken	Score
masterchief	Intro	0	0	0

Game Information

Welcome to the Cisco Meraki - Capture The Flag game! Our aim is to enhance your cloud skills learning and exploring Cisco's Meraki platform.

During the game, you will be challenged to get information from the Cisco Meraki dashboard, implement clever security and routing configurations, leverage API resources, interpret artistic data visualizations, and delve into the power of automation. Make your claim and have some fun in the cloud.

Good luck!

How to Play


You will be presented with several 'Missions', where each mission is a set of challenges or 'Tasks' (also known as 'Flags'). By solving a challenge, you will have 'Captured the Flag' for that challenge and be rewarded with points. When a set of challenges (flags) is finished, you will have completed that mission. The level of difficulty may vary between Missions. There are Missions for

About Write-ups


It would not be a gaming / learning experience for you and others if you share / publish answers about CTF online in any form. Hence to keep the fun experience alive, we request you not to do so. However we do love to hear what you like in any shape or form on Social Media or directly to us via the [Contact Us](#) option.

Mission Progress


Level: Intro




CTF Warm up mission








Cloud Networking - Cisco Meraki (dCloud) 2.0



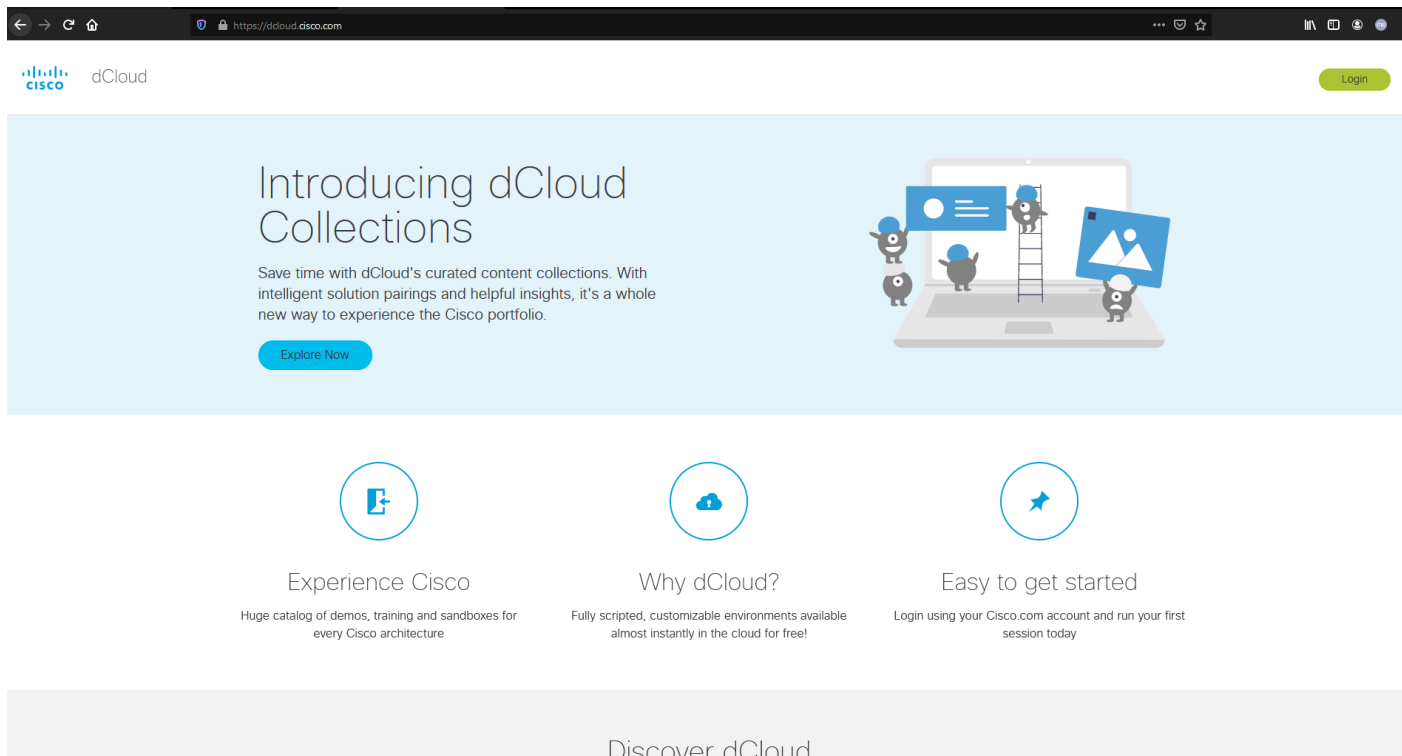
What the Wi-Fi? (dCloud) 2.0



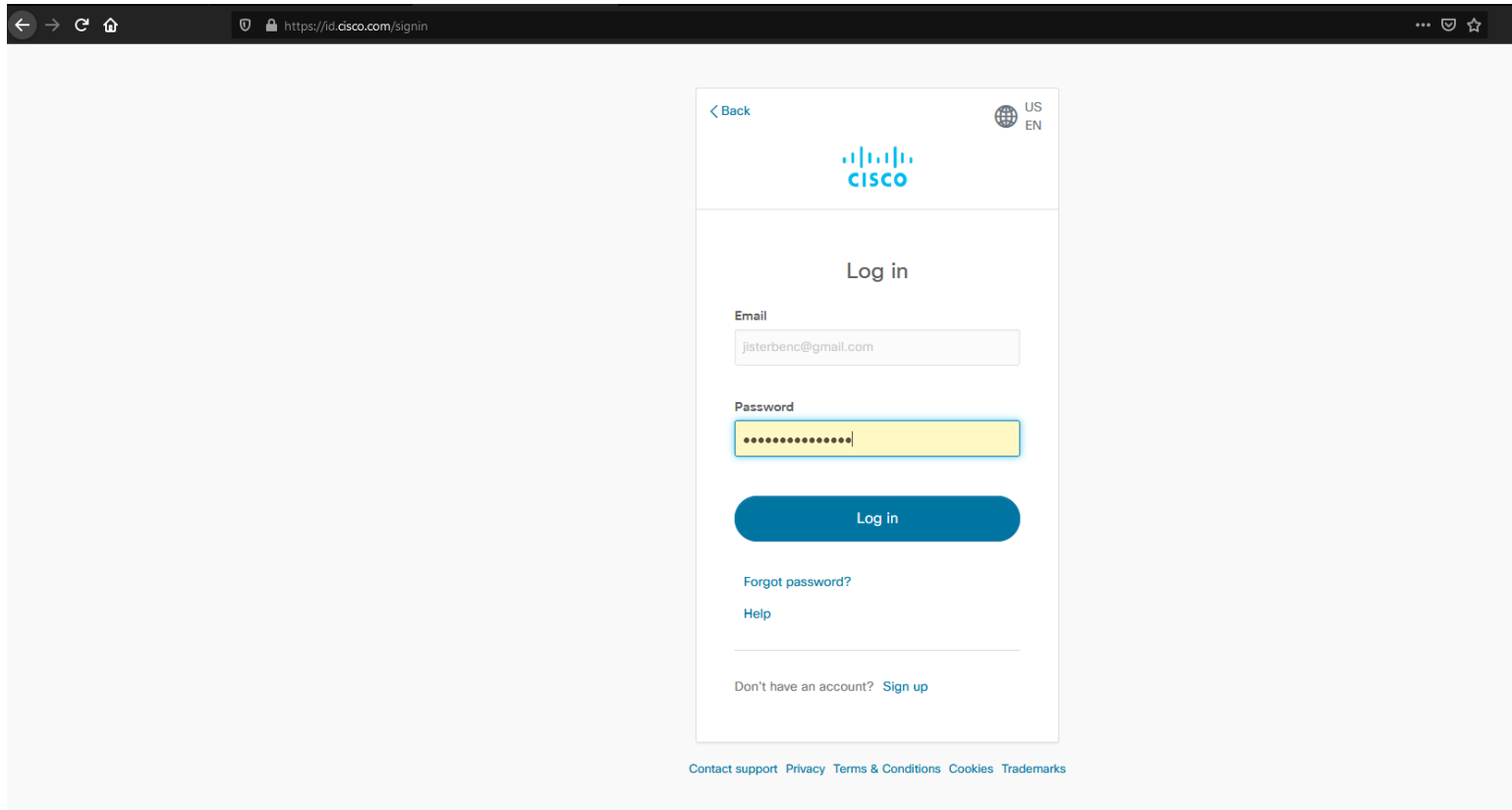
Troubleshooting and Assurance (dCloud) 2.0



- you will have to access a special Meraki dashboard to look for the flags
- this is under <https://dcloud.cisco.com/>
- if you don't have a cisco.com account already, please make sure to create one (it's FREE)




login there



The screenshot shows a web browser window with the address bar displaying `https://id.cisco.com/signin`. The page content is a login form for Cisco Meraki. At the top of the form, there is a '< Back' link on the left, the Cisco logo in the center, and a globe icon with 'US' and 'EN' on the right. The main heading is 'Log in'. Below this, there are two input fields: 'Email' with the value 'jjsterbenc@gmail.com' and 'Password' which is masked with dots. A blue 'Log in' button is positioned below the password field. Underneath the button are two links: 'Forgot password?' and 'Help'. At the bottom of the form, there is a link 'Don't have an account? Sign up'. Below the entire form, there is a footer with links: 'Contact support', 'Privacy', 'Terms & Conditions', 'Cookies', and 'Trademarks'.

< Back

US
EN



Log in

Email

jjsterbenc@gmail.com

Password

.....

Log in

[Forgot password?](#)

[Help](#)

Don't have an account? [Sign up](#)

[Contact support](#) [Privacy](#) [Terms & Conditions](#) [Cookies](#) [Trademarks](#)

hit search button and click “View” on Intro to the Cisco Meraki Platform - Instant Demo v1

Intro to the Cisco Meraki Platform - Instant Demo v1

ID: intro-to-the-cisco-meraki-platform-v1 Published Date: 19-Feb-2021 14:48 Instant Demo Meraki Enterprise Networks
Cisco Meraki Wireless LAN Security & SD-WAN Switching Mobility Management English

This instant demo introduces those new to the Cisco Meraki platform to the basics of how a simple, secure, intelligent, cloud-managed networking platform can give your business the flexibility and agility to handle everything from explosive growth to new and challenging flexible work environments and everything in between. If you are interested to see how Cisco Meraki can transform your business, this instant demo is for you.

NOTE: Please download the guide from the **Related Documents** link below and click **View** to access the demo.

★ Favorite  Copy  [Related Documents](#)

[View](#)

you should land in the organizational overview of the dashboard you need to capture the flags!

Mission - CTF Warm up mission

https://n149.meraki.com/San-Francisco-sy/h/w3YTpdcv/manage/organization/overview#t=network

Announcements Help cmp_meraki_demo

Search Dashboard

Map Satellite Address, zip code, etc. Go

Greenland Iceland Sweden

Hide table

NETWORK

San Francisco

Network-wide

Security & SD-WAN

Switch

Wireless

Systems Manager

Cameras

Environmental

Insight

Organization

17

Networks

Search... 10 networks Over the last week: 91 clients, 312.61 GB

CSV +

	Usage	Devices	Clients	Name	Tags	Network type	Offline devices	Template
<input type="checkbox"/>	None	2	0	Sydney - PhysicalSecurity	Retail	Combined	0	
<input type="checkbox"/>	180.51 GB	16	62	San Francisco	Campus	Combined	0	
<input type="checkbox"/>	34.28 GB	2	7	Sydney	Retail	Combined	0	Retail Stores
<input type="checkbox"/>	83.44 GB	11	18	London	Branch	Combined	0	
<input type="checkbox"/>	None	1	0	Datacenter-CA	Datacenter	Appliance	0	
<input type="checkbox"/>	4.81 GB	1	1	Teleworker Hedy Lamarr	Teleworker	Appliance	0	Teleworkers-MX
<input type="checkbox"/>	4.82 GB	1	1	Teleworker Louis Pasteur	Teleworker	Appliance	0	Teleworkers-MX
<input type="checkbox"/>	1.36 GB	1	1	Teleworker Elijah McCoy	Teleworker	Appliance	0	Teleworkers-MX
<input type="checkbox"/>	3.40 GB	1	1	Teleworker Blaise Pascal	Teleworker	Appliance	0	Teleworkers-MX
<input type="checkbox"/>	None	1	0	Teleworker Mary Anderson	mrOnly Teleworker	Wireless	0	Teleworkers-MR-only

Colombia Ecuador Peru Bolivia Paraguay Chile Argentina Uruguay

Brazil

South Atlantic Ocean

Angola Zambia Mozambique Zimbabwe Botswana South Africa

Kenya Tanzania

Madagascar

Indian Ocean

Malaysia Indonesia Papua New Guinea

Australia

4

Google

- Let's go back to the CTF mission portal
- you should have two tabs open during the entire game,
- one for the Meraki dashboard and the other for the CTF portal
- click now on the "CTF Warm Up" mission
- you won't need the Meraki dashboard for this one, it's just to get used to the GUI explore both flags in there

Flags on this Mission

1. Cloud Networking platform
2. The platform

[How to Connect to the Game Environment](#)

[Scroll to Top](#)

CTF Warm up mission

[Return to Missions](#)

***** Begin secure message *****

This is a Cisco Meraki CTF warm up mission. You are just going to get familiar with CTF structure of the tasks, how to input the flags, and how to get additional help to your mission.

Enjoy

Overall Difficulty: easy
Approx Time to Complete: 00H:30M

***** End secure message *****

This game is played by connecting to a real game environment which is different for each mission.

Here is [How to Connect](#) to the game environment for this mission.

- Flags / Tasks -

1	Cloud Networking platform	+	0 Attempts	10 Points
2	The platform	+	0 Attempts	10 Points


- Once you are done warming up it's time to go after the real deal
- click on "Return to Missions" to go back to missions portal

The screenshot displays the Cisco Meraki Missions portal. At the top, a green navigation bar includes the Cisco logo, the text "Capture the Flag - Meraki", and links for Home, Missions, Scores, and FAQs. A user profile for "masterchief" is in the top right. The main content area is titled "Missions" and shows a "Level: Intro" section. This section contains four mission cards, each with a thumbnail image and a title:

- CTF Warm up mission**: The thumbnail shows a screenshot of a network dashboard with various charts and data.
- Cloud Networking - Cisco Meraki (dCloud) 2.0**: The thumbnail shows a person sitting at a table in a meeting room, with a "Samba Systems" logo visible in the background.
- What the Wi-Fi? (dCloud) 2.0**: The thumbnail shows a diagram of a Wi-Fi network with a central router icon connected to several mobile devices (laptop, smartphone, tablet).
- Troubleshooting and Assurance (dCloud) 2.0**: The thumbnail shows a network diagram with various icons representing different network components and a laptop displaying a network map.

On the right side of the screen, there is a vertical sidebar with social media icons for Email, a megaphone, Twitter, LinkedIn, and a circular icon.

Click on the "Cloud Networking" one

 Capture the Flag - Meraki

[Home](#) [Missions](#) [Scores](#) [FAQs](#)

masterchief

Flags on this Mission

1. SFO Modus operandi
2. Know your network - SFO
3. The SFO Branch Connectivity
4. Let's Talk to SFO
5. Enforce company policy
6. Path of least resistance
7. Install me wi-fi
8. Captive Wi-Fi - SFO
9. Open for business
10. Customize my Signal
11. Needle in a haystack - Wi-Fi edition
12. Vision 2020
13. Walled Vision
14. Searching
15. Automate your world
16. Responsive alerting
17. Tracking users with APIs
18. Org Identity
19. Tunnelled access
20. Date my DC


[How to Connect to the Game Environment](#)

[Scroll to Top](#)

Cloud Networking - Cisco Meraki (dCloud) 2.0

Return to Missions

***** Begin secure message *****



Samba Systems

Mango Systems has continued to grow in its mission to serve its customers. As part of that growth, an acquisition was made that expanded its presence to other locations around the world. Samba Systems was born.

Despite revenue and customer growth, the IT team has stayed the same size. Company leadership challenged the IT team to open 14 new offices and conform to the corporate standard in 45 days. Luckily, Mango Systems has a secret weapon for its new Samba division: Cisco Meraki.

Your mission is to review the Samba Systems setup, familiarize yourself with the new sites, and make sure everything is correct before the IT leadership presents to the board at the 40-day mark - ahead of schedule.

Good luck!

Overall Difficulty: Easy

Approx Time to Complete: 01H:00M

***** End secure message *****

This game is played by connecting to a real game environment which is different for each mission.

Here is [How to Connect](#) to the game environment for this mission.

- Flags / Tasks -





1

SFO Modus operandi

+

0 Attempts

10 Points



- You are now on your own
- use your expertise on the Meraki Dashboard to capture as many flags as possible
- if you get stuck, you may request a “hint” (provided in most flags), if that still does not work move on to next flag
- there’s no precise order in which you may capture the flags, it is better to start from first ones though as they are generally easier
- how many points you score depends on:
 - time taken to capture a flag
 - amount of flags captured
 - number of attempts to capture a flag
 - number of hints taken
- Proctor will share leaderboard by the end of the event

Go get ‘em !

Kahoot!

Yvonne Andersen

Cisco Territory Account Manager
Cisco Systems

Gina Pappagallo

Cisco Virtual Account Manager
Cisco Systems

KAHOOT! LOGIN

- Go to: <https://kahoot.it/>
- Enter Game PIN

Final Thoughts

Questions and Answers
(submit via chat)

**Your performance improvement
is our measure of success.**

Thank You!