cisco Live!

chrivand@cisco.com

@ChriscoDevNet

#CiscoLive

The bridge to possible

MSSP for Dummies

How to cope with (and automate) security events from all your customers?

Christopher van der Made, Security Developer Advocate
@ChriscoDevNet

BRKDEV-2002

Agenda

- What is a Managed Security Services Partner (MSSP)?
- What is required for a MSSP?
- What Cisco solutions fit these requirements?
  - SHORT DEMOS
- Use case: managing Secure Endpoint events for multiple tenants.
  - LONG DEMO
- Closing

What is a Managed Security Services Partner (MSSP)?

WORKING HERE IS A LOT MORE FUN
SINCE WE STARTED OUTSOURCING OUR STRESS!
memegenerator.net

Customers Need Help with Security

Organizations lack the resources necessary to respond to advanced threats on the endpoint

Lack of Available Security Talent

Lack of Available Budget

Evasion Techniques Advancing

Diverse Endpoint Ecosystems

Needs and Challenges MSSPs Face

Challenges

- Inefficient service creation and ongoing operations
- Increasingly competitive environment
- Differing customer needs
- Flexibility to adjust services quickly and efficiently

Needs

- Improved management and visibility/interoperability
- Vendors who are easy to do business with
- Flexible licensing models
- Minimal upfront capital investments

What do MSSP’s set out to do?

- Drive monetization of new services;
- Offer fast and agile deployment;
- Integrate products seamlessly;
- Manage customers efficiently;
- Prove your ongoing value to customers;
- Protect customers from advanced threats.

What is required for a MSSP?

What is the most important for a MSSP?

Scale your MSSP offering!

Scale your MSSP offering!

Multitenancy

Comprehensive Reporting

API integrations

Easy service creation

Extra MSSP offering!

Extra MSSP offering!

What Cisco solutions fit these requirements?

The Cisco MSSP Portfolio*

SM

STEALTHWATCH CLOUD

Secure Access Platform

Secure Endpoint

Prevent, detect, and respond to advanced threats while continuously monitoring file behavior to uncover stealthy attacks

Umbrella Cloud Edge

Provide protection against threats on the Internet across all devices, even when users are off the corporate network

Meraki Systems Manager

Manage and control mobile and desktop devices, onboard new devices, and automate application of security policies

Secure Cloud Analytics

Provides behavioral analytics across your network to help you improve threat detection and achieve a stronger security posture.

Secure Access by Duo

Provides remote access solutions and protects existing IT infrastructure, making it easy for employees and contractors to gain remote access when remote working.

**not exhaustive, all cloud and all quick wins…*

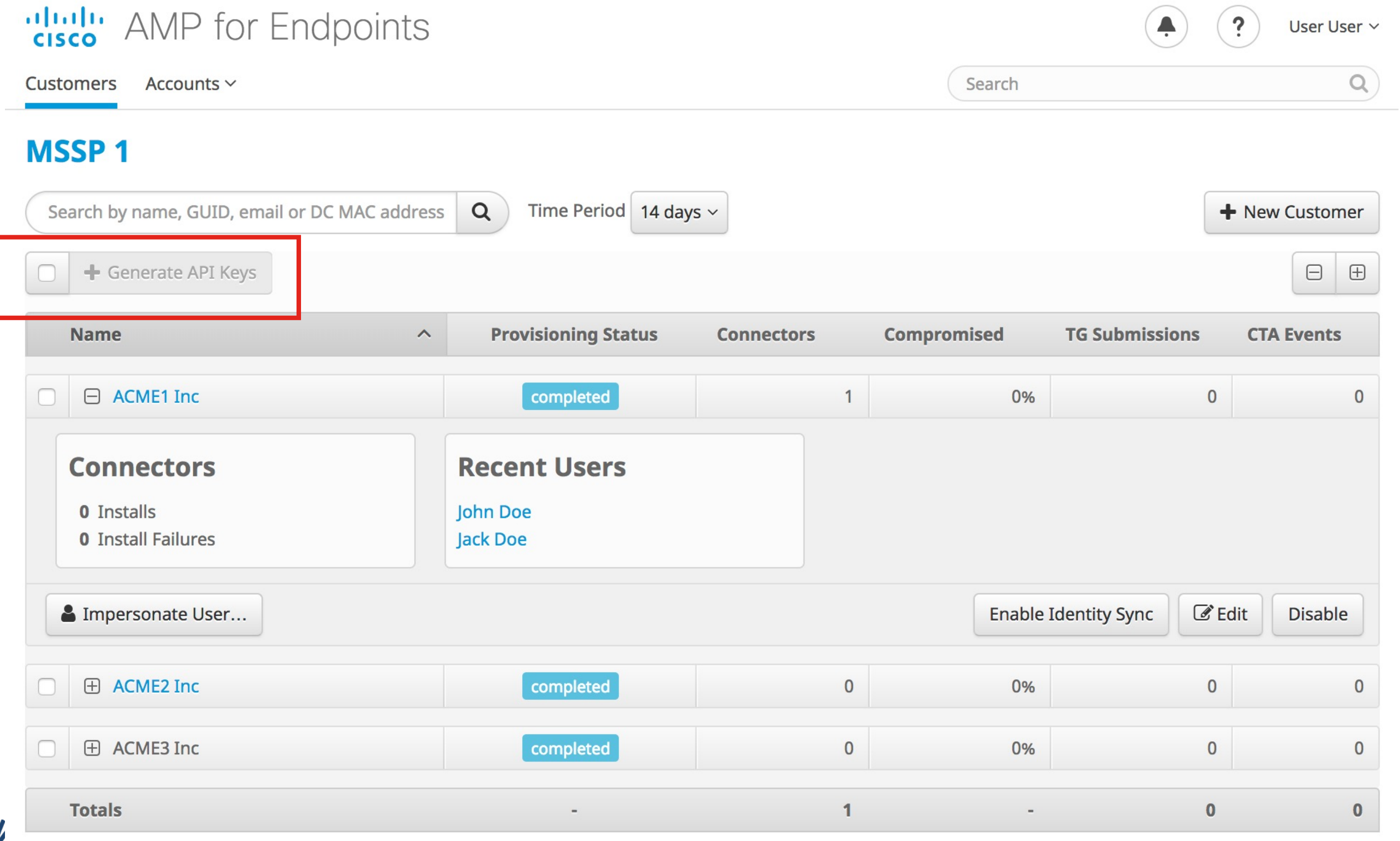
AMP for Endpoints

~~AMP for Endpoints~~ Cisco Secure Endpoint!

Secure Endpoint – Overview

- Cloud Managed, subscription-based SaaS
- Protects Windows, Mac, Linux, Android and iOS
- AMP Everywhere: integrated architecture with intelligence sharing
- Prevention, Detection, and Response in a single security agent (connector)
- Public or private cloud deployment options

Secure Endpoint - MSSP Console



MSSP 1

	Name	Provisioning Status	Connectors	Compromised	TG Submissions	CTA Events
□	⊟ ACME1 Inc	completed	1	0%	0	0
□	⊞ ACME2 Inc	completed	0	0%	0	0
□	⊞ ACME3 Inc	completed	0	0%	0	0
	Totals	-	1	-	0	0

Connectors

0 Installs
0 Install Failures

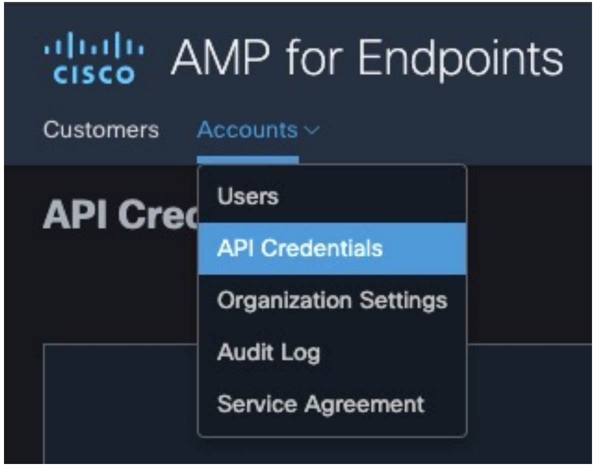
Recent Users

John Doe
Jack Doe

New: Secure Endpoint MSSP API!

- Create new tenant: **POST** to <base_url>/v1/mssp/customers
- Get status all tenants: **GET** to <base_url>/v1/mssp/customers
- Get status single tenant **GET** to <base_url>/v1/mssp/customers/<email-admin>
- Disable tenant: **DELETE** to <base_url>/v1/mssp/customer
- **Check MSSP console guide for more info!**

Scale your MSSP offering!

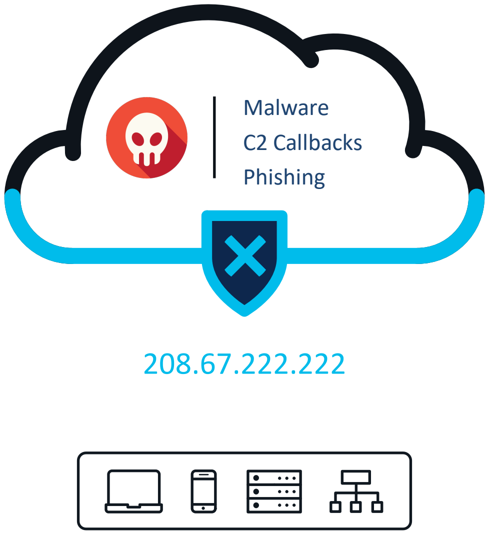


Demo Video, please check recording...

Umbrella

Cisco Umbrella

- Cloud security platform



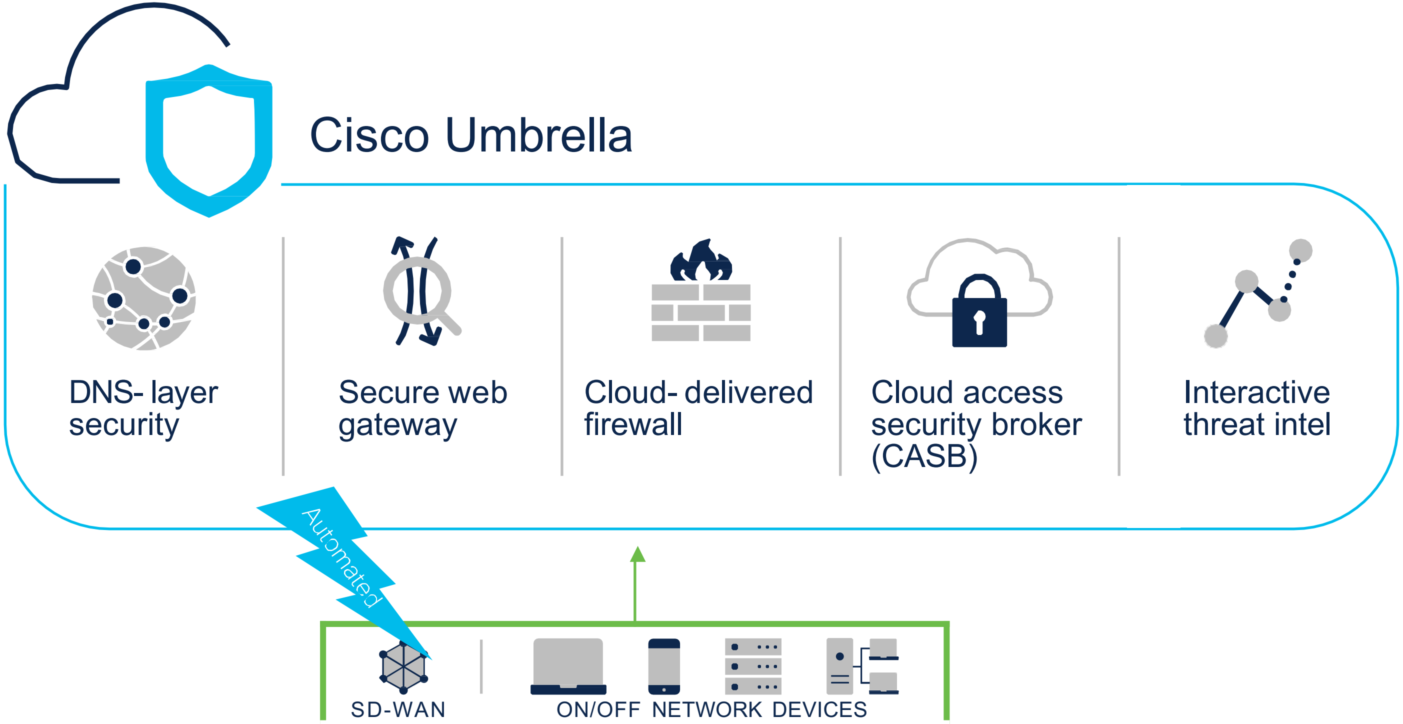
Built into the foundation of the internet

Intelligence to see attacks before launched

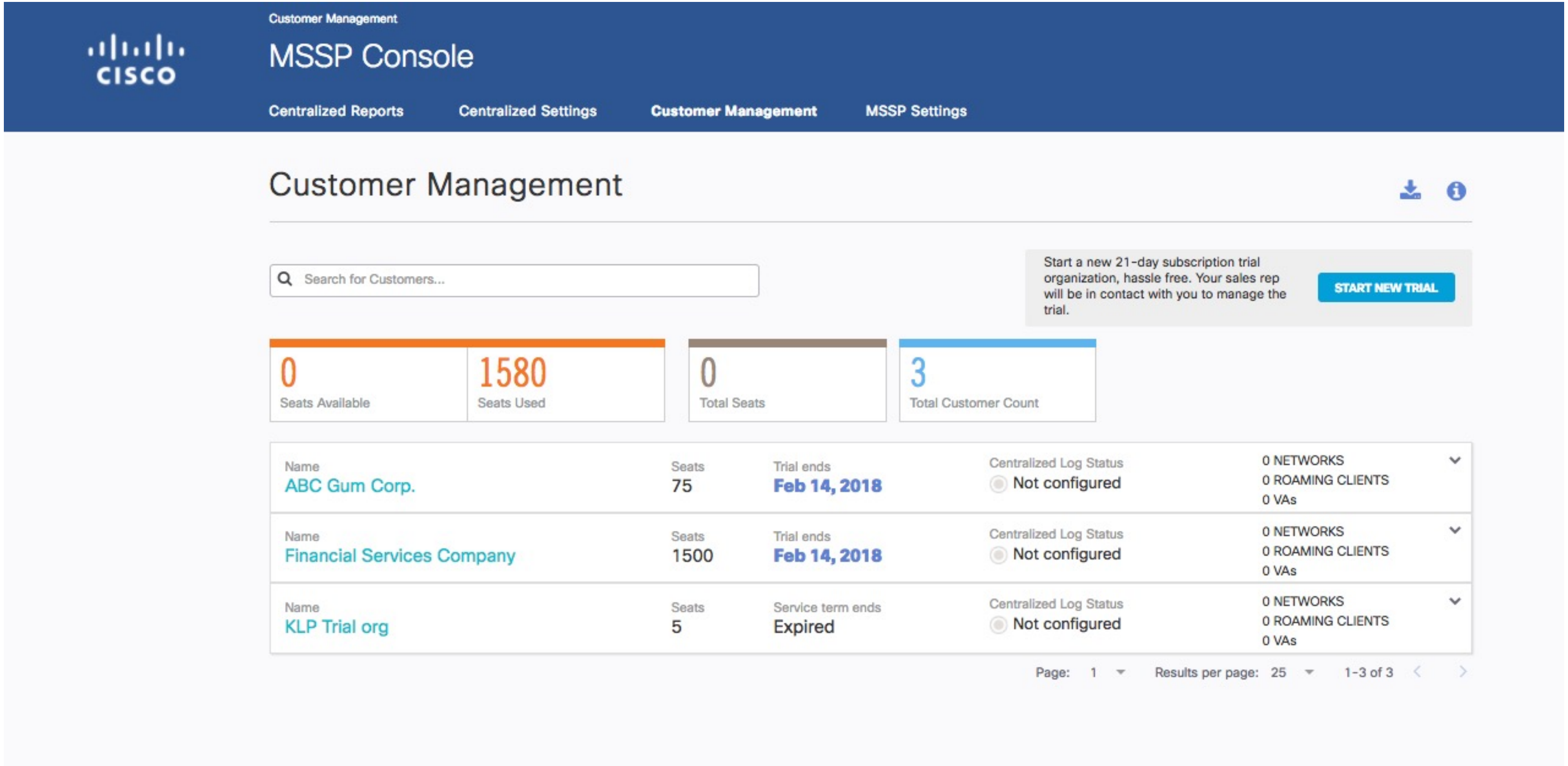
Visibility and protection everywhere

MSSP -wide deployment in minutes

Integrations to amplify existing investments


Cisco Umbrella
DNS- layer security
Secure web gateway
Cloud- delivered firewall
Cloud access security broker (CASB)
Interactive threat intel
Automated
SD-WAN
ON/OFF NETWORK DEVICES

Umbrella for MSSPs Console



Customer Management

MSSP Console

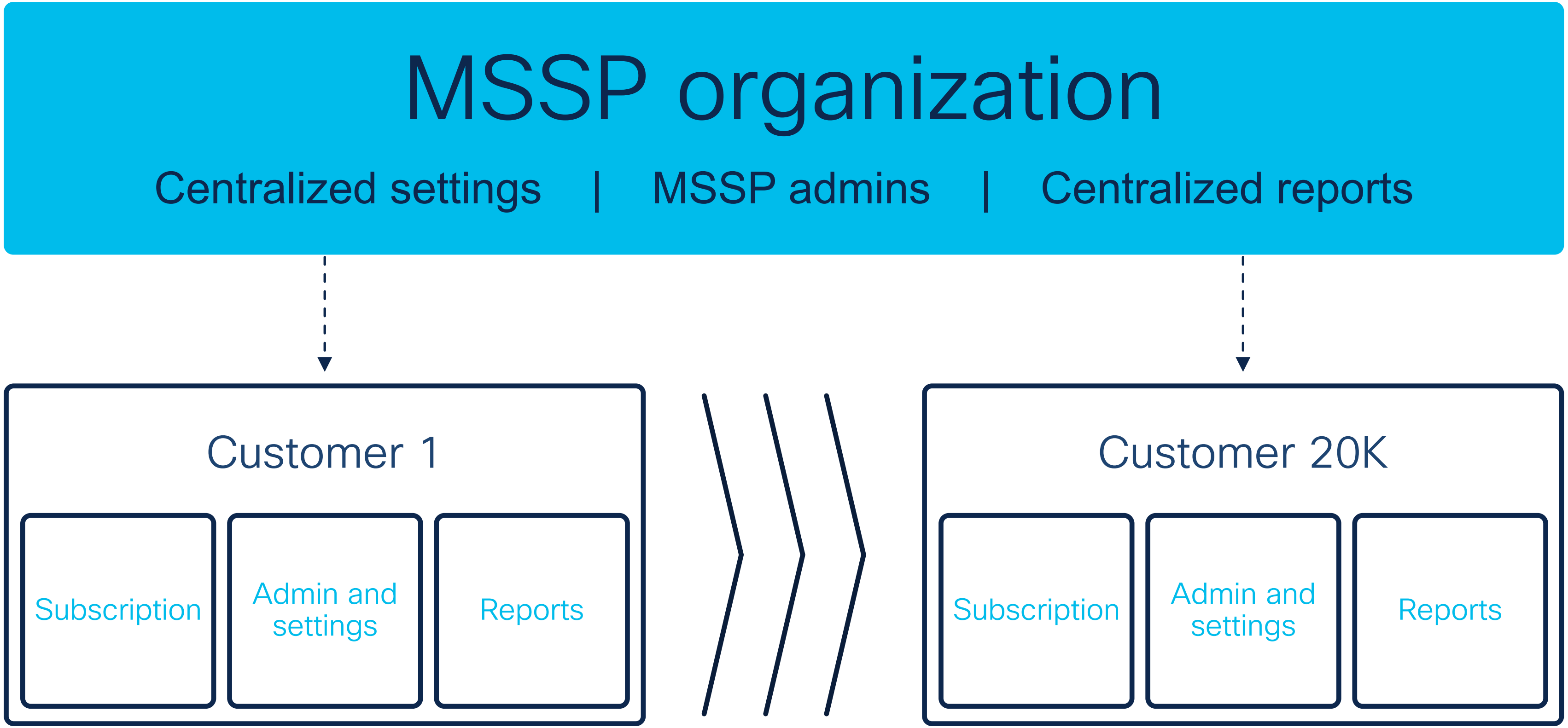
Customer Management

Start a new 21-day subscription trial organization, hassle free. Your sales rep will be in contact with you to manage the trial.

0	1580	0	3
Seats Available	Seats Used	Total Seats	Total Customer Count

Name	Seats	Trial ends / Service term ends	Centralized Log Status	
ABC Gum Corp.	75	Trial ends Feb 14, 2018	Not configured	0 NETWORKS 0 ROAMING CLIENTS 0 VAs
Financial Services Company	1500	Trial ends Feb 14, 2018	Not configured	0 NETWORKS 0 ROAMING CLIENTS 0 VAs
KLP Trial org	5	Service term ends Expired	Not configured	0 NETWORKS 0 ROAMING CLIENTS 0 VAs

Page: 1 Results per page: 25 1-3 of 3



MSSP organization

Centralized settings | MSSP admins | Centralized reports

Customer 1

Subscription

Admin and settings

Reports

Customer 20K

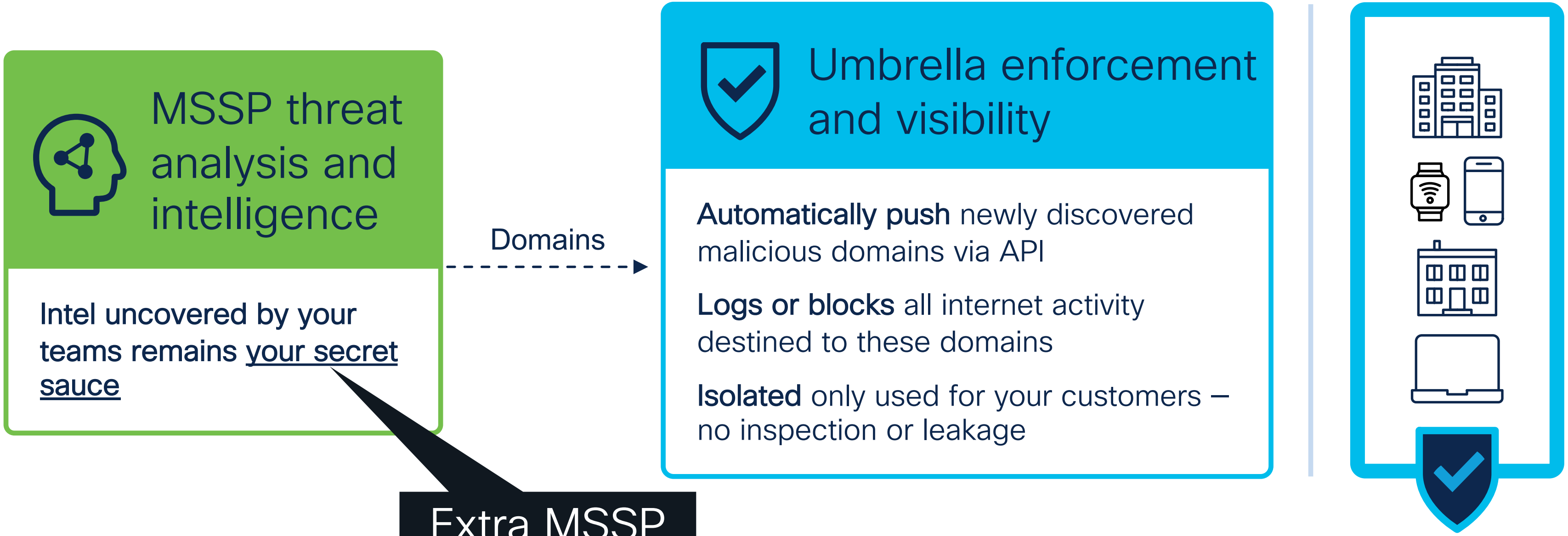
Subscription

Admin and settings

Reports

Leverage the APIs to enforce your intelligence

Protect your customers while keeping your intellectual property secret



MSSP threat analysis and intelligence

Intel uncovered by your teams remains your secret sauce

Domains

Umbrella enforcement and visibility

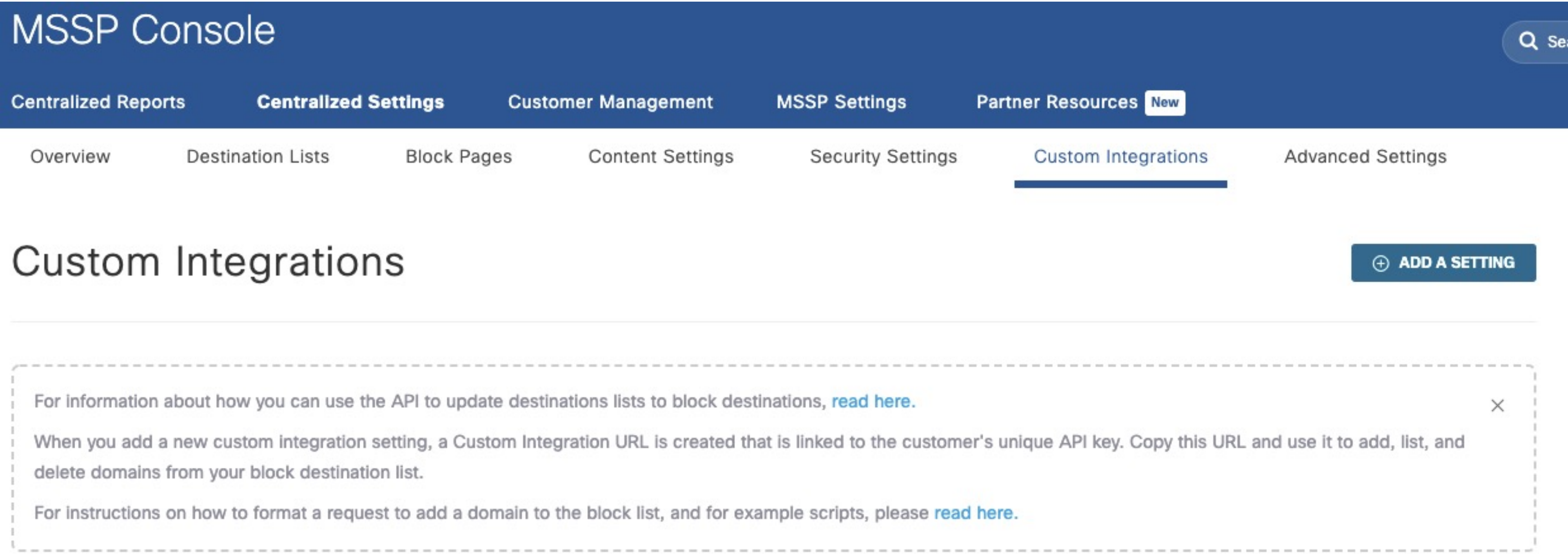
Automatically push newly discovered malicious domains via API

Logs or blocks all internet activity destined to these domains

Isolated only used for your customers – no inspection or leakage

Extra MSSP offering!

Centralized “Secret Sauce” API



Custom Integrations

For information about how you can use the API to update destinations lists to block destinations, read here.

When you add a new custom integration setting, a Custom Integration URL is created that is linked to the customer's unique API key. Copy this URL and use it to add, list, and delete domains from your block destination list.

For instructions on how to format a request to add a domain to the block list, and for example scripts, please read here.

Demo Video, please check recording...

Use more APIs!

- POST /serviceproviders/{serviceProviderId}/customers/{customerId}/apikeys
  - *Create a management API Key for your customers*
- *GET /v2/providers/{msporganizationid}/requests-by-org*
  - Gets summary counts of all requests within timeframe
- *GET /v2/providers/{msporganizationid}/requests-by-destination*
  - Gets summary counts of all requests within timeframe
- *GET /v1/organizations/{ConsoleID}/security-summary*
  - This endpoint currently returns the summary of security data for the last 24 hours for all your child organizations. Importantly, it also provides the organization Id of each child organization; this is used later in the security activity details report.
- Much more: https://docs.umbrella.com/umbrella-api/reference#service-providers

Scale your MSSP offering!

Meraki Systems Manager

Meraki Systems Manager Features

PROVISION

- Setup
- Grant Wifi/VPN access
- Configure Email
- Push Apps and Software
- Apply Restrictions

MONITOR

- Global visibility
- See installed software and security profile
- Track stolen/lost devices
- Troubleshoot devices

SECURE

- Dynamic / conditional network and data (email/apps) access
- Recover stolen devices
- Remotely wipe devices
- ISE, AnyConnect, CSC, Cisco Integration

Systems Manager For MSSPs

- No upfront investment required
- No hosting / maintenance requirements
- No minimum purchase needed
- Rich APIs for integration into existing helpdesk / ticketing solutions
- Complementary product with Cisco ISE
- Supports value added networking and full UEM / MDM services
- No additional costs for future features and services
- Easy to learn, maintain and scale

Stealthwatch Cloud

~~Stealthwatch Cloud~~ Cisco Secure Cloud Analytics

Stealthwatch Cloud: network security monitoring across your customers' hybrid environments

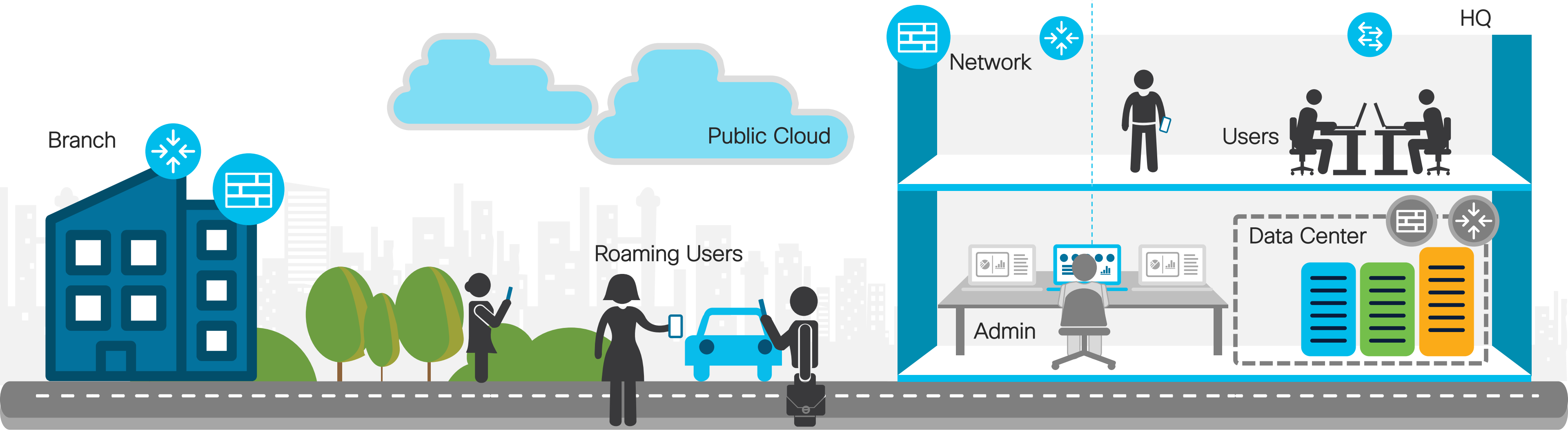
KNOW every host

OBSERVE every interaction

Understand what is NORMAL

Be alerted to CHANGE

Respond to THREATS quickly



Stealthwatch Cloud is built for MSSPs

Month-to-month, multi-tenant offering

No upfront capital expenditure

Develop and offer services quickly

No need to invest in infrastructure or provision accounts

Easily integrate into your workflow tools

Duo MFA

~~Duo MFA~~ Secure Access by Duo

Workforce

How to Verify Trust

Verify users' identities

WITH

Multi-factor authentication (MFA)

Gain device visibility & establish trust

WITH

Endpoint health & management status

Enforce access policies for every app

WITH

Adaptive & role-based access controls

Duo MSP features

- MSP Console
  - *Multi-tenant console*
  - *Self-provision accounts and users*
  - *Custom config and policies per tenant*
- MSP Buying Program
  - *Monthly billing*
  - *Pay-as-you-go*
  - *Consolidated billing and reporting*
- MSP Business Support
- APIs and many integrations!

Overview Duo API’s

- Duo Auth API
  - *The Auth API is a low-level, RESTful API for adding strong two-factor authentication to your website or application.*
- **Duo Accounts API** [not enabled by default, contact support]
  - *The Accounts API allows a parent account to create, manage, and delete other Duo Security customer accounts.*
- **Duo Admin API** [not enabled by default, contact support]
  - *The Admin API provides programmatic access to the administ ive functionality of Duo Security's two-factor authentication platf*
- [Other hidden API’s for integration partners]

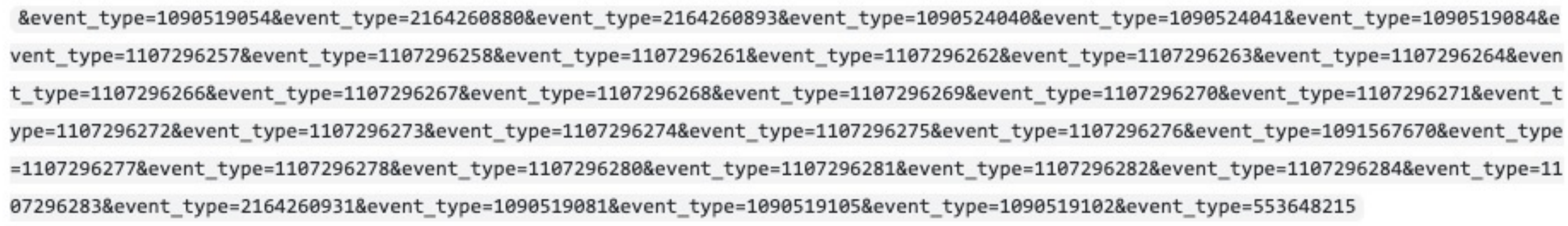
Scale your MSSP offering!

Use case: managing Secure Endpoints events for multiple tenants.

What events are important?

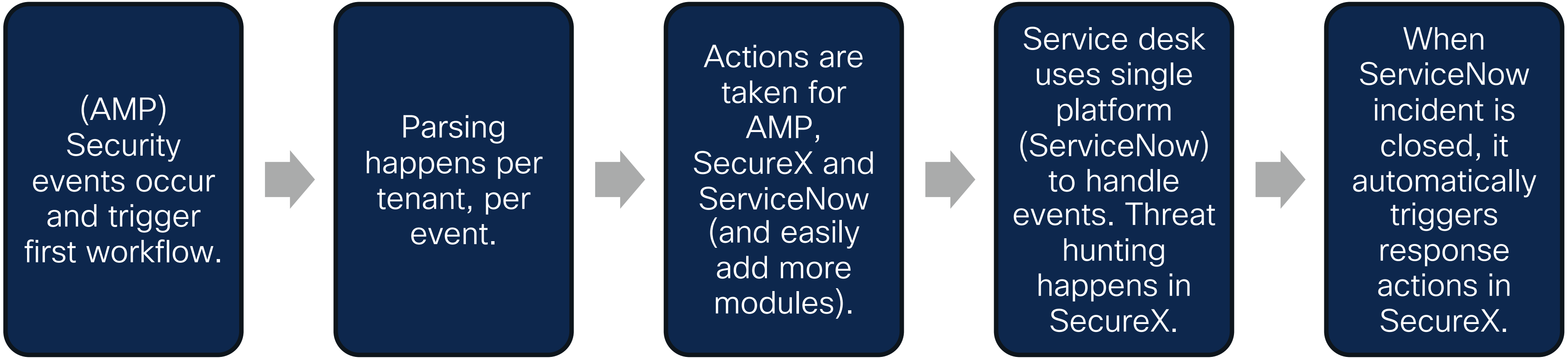
What events ~~are important~~ require human intervention?

Do you agree with me?



```
&event_type=1090519054&event_type=2164260880&event_type=2164260893&event_type=1090524040&event_type=1090524041&event_type=1090519084&e
vent_type=1107296257&event_type=1107296258&event_type=1107296261&event_type=1107296262&event_type=1107296263&event_type=1107296264&even
t_type=1107296266&event_type=1107296267&event_type=1107296268&event_type=1107296269&event_type=1107296270&event_type=1107296271&event_t
ype=1107296272&event_type=1107296273&event_type=1107296274&event_type=1107296275&event_type=1107296276&event_type=1091567670&event_type
=1107296277&event_type=1107296278&event_type=1107296280&event_type=1107296281&event_type=1107296282&event_type=1107296284&event_type=11
07296283&event_type=2164260931&event_type=1090519081&event_type=1090519105&event_type=1090519102&event_type=553648215
```

Let’s check out a specific example…



(AMP) Security events occur and trigger first workflow.

Parsing happens per tenant, per event.

Actions are taken for AMP, SecureX and ServiceNow (and easily add more modules).

Service desk uses single platform (ServiceNow) to handle events. Threat hunting happens in SecureX.

When ServiceNow incident is closed, it automatically triggers response actions in SecureX.

https://developer.cisco.com/codeexchange/github/repo/chrivand/amp-mssp-events-to-snow

LONG DEMO…

https://developer.cisco.com/codeexchange/github/repo/chrivand/amp-mssp-events-to-snow

Demo Video, please check recording...

Closing

What is the most important for a MSSP?

Scale your MSSP offering!

Scale your MSSP offering!

Multitenancy

Comprehensive Reporting

API integrations

Easy service creation

Extra MSSP offering!

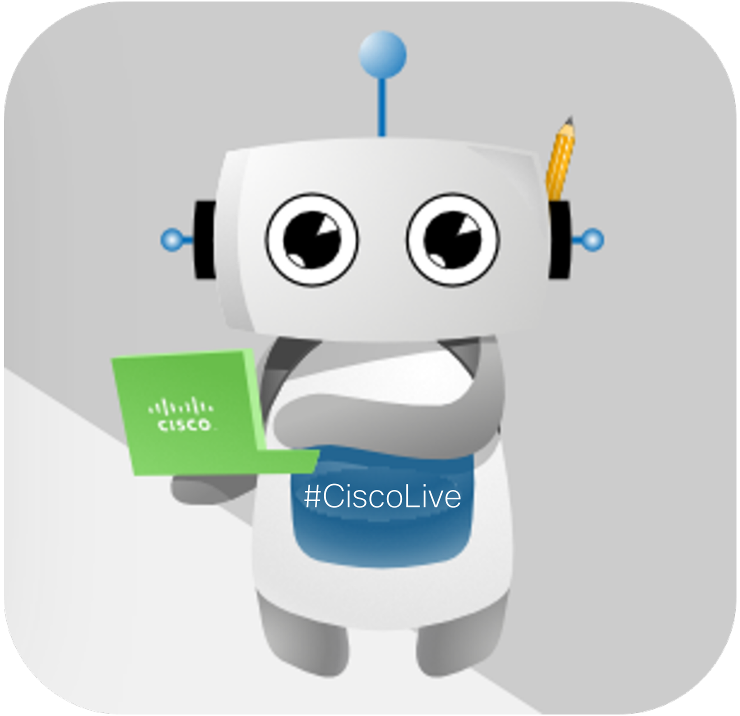
Extra MSSP offering!

Handy links

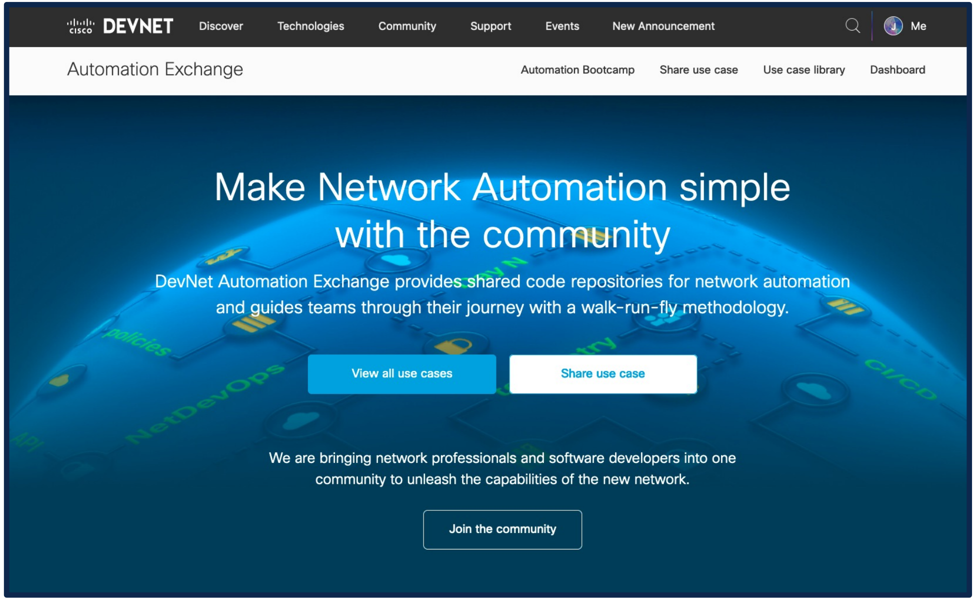
- **Cisco MSSP central**: https://www.cisco.com/c/en/us/solutions/service-provider/service-provider-security-solutions/mssp.html
- **AMP API docs:** https://api-docs.amp.cisco.com/
- **Umbrella MSSP**: https://docs.umbrella.com/mssp-deployment/docs/welcome
- **Duo MSSP**: https://duo.com/partnerships/managed-service-providers
- **Stealthwatch Cloud API docs**: https://developer.cisco.com/docs/stealthwatch/cloud/
- **Cool project to check out:** https://github.com/drnop/RTCaaS
- **For licensing and contractual stuff**: go to your account representative…

DevNet Resources

- Code of demo: https://developer.cisco.com/codeexchange/github/repo/chrivand/amp-mssp-events-to-snow
- Continue learning with SecureX orchestration: https://developer.cisco.com/securex/orchestration/
- Special Cisco Live DevNet offers: cs.co/devnetoffers



Automation Exchange



Make Network Automation simple with the community

DevNet Automation Exchange provides shared code repositories for network automation and guides teams through their journey with a walk-run-fly methodology.

We are bringing network professionals and software developers into one community to unleash the capabilities of the new network.

Start your network automation journey with DevNet!

Walk
Get visibility and insights into your network

Run
Activate policy and intent across different network domains

Fly
Proactively manage applications, users, devices with DevOps workflow

Find my code at: https://developer.cisco.com/network-automation/detail/9a0b42f1-71d3-11eb-aa44-aa8fea613d8b/

The bridge to possible

Thank you

cisco Live!

chrivand@cisco.com

@ChriscoDevNet

#CiscoLive