Cisco Security - Novinky

Tech Club Webinář

Andrej Jeleník - Systems Engineer

16. 06. 2020

Cisco **Secure Remote Worker** offer

Offers End July 1

Duo

Current Duo Customers
Allow customers to add unlimited additional users during offer period

New Customers
30-day evaluation with unlimited users, after which the customer will need to purchase 10% of the current user population for one year and allow customer to add unlimited users during the offer period only

AnyConnect/ NextGeneration Firewall

Current AnyConnect Customers
Allow customers to install additional users beyond their purchased limit during offer period

Current ASA/Firepower Customers Without AnyConnect
90-day evaluation of AnyConncet

New Customers
Significant discount program for ASAv30

90-day evaluation of AnyConnect

Cisco Umbrella

Umbrella

Current Umbrella Customers
Ability to exceed purchase user count during period

New Customers
90-day evaluation of Umbrella DNS Advanced or SIG

AMP for Endpoints

Current AMP for Endpoints Customers

Ability to expand usage of the product up to twice as many licensed endpoints during offer period

New Customers
60-day evaluation of AMP for Endpoints, up to 1000 endpoints during the offer period only

cisco Secure

FY21 Security Priorities

SecureX

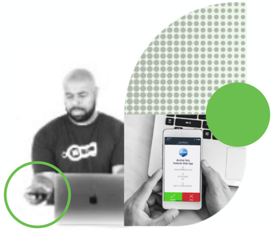
Platform Focus
SecOps (AMP, Email, TG)
EAs

Cloud Transition

NGFW, SIG, Secure SD-WAN, Branch Transformation

Secure Remote Worker

Duo, Umbrella, AnyConnect, AMP4E



Zero Trust

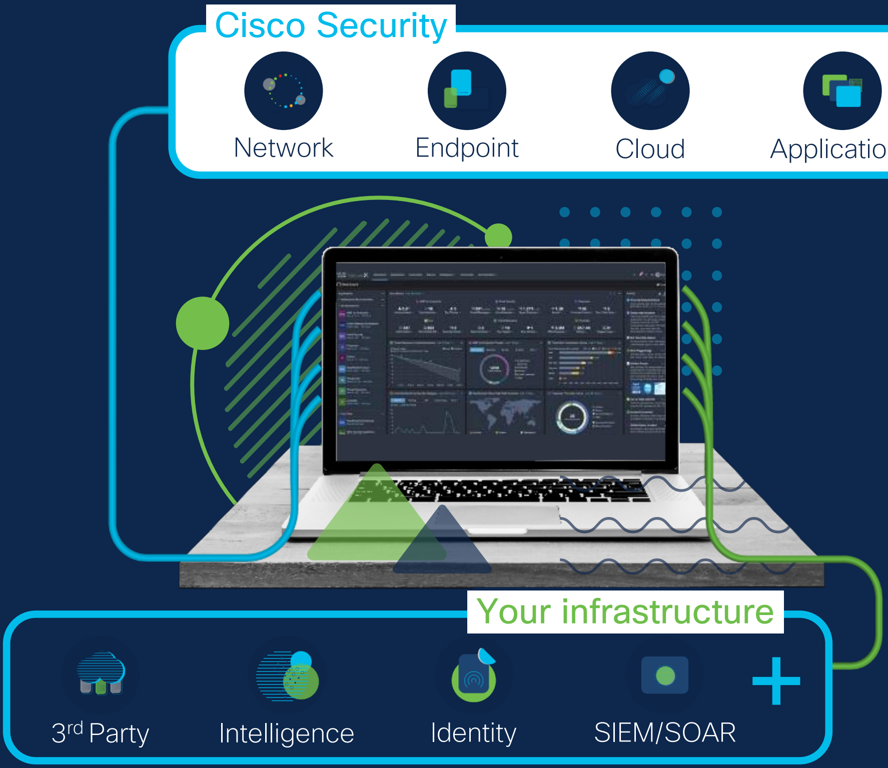
Duo, ISE, Tetration

Workload and Analytics

SWATCH, Tetration, AppDynamics

cisco Secure

Cisco SecureX - connecting with the **entire** security infrastructure



Cisco Security

Network

Endpoint

Cloud

Applications

Your infrastructure

3rd Party

Intelligence

Identity

SIEM/SOAR

+

Integrate everything in your environment to unify **visibility**, enable **automation**, and **strengthen security**

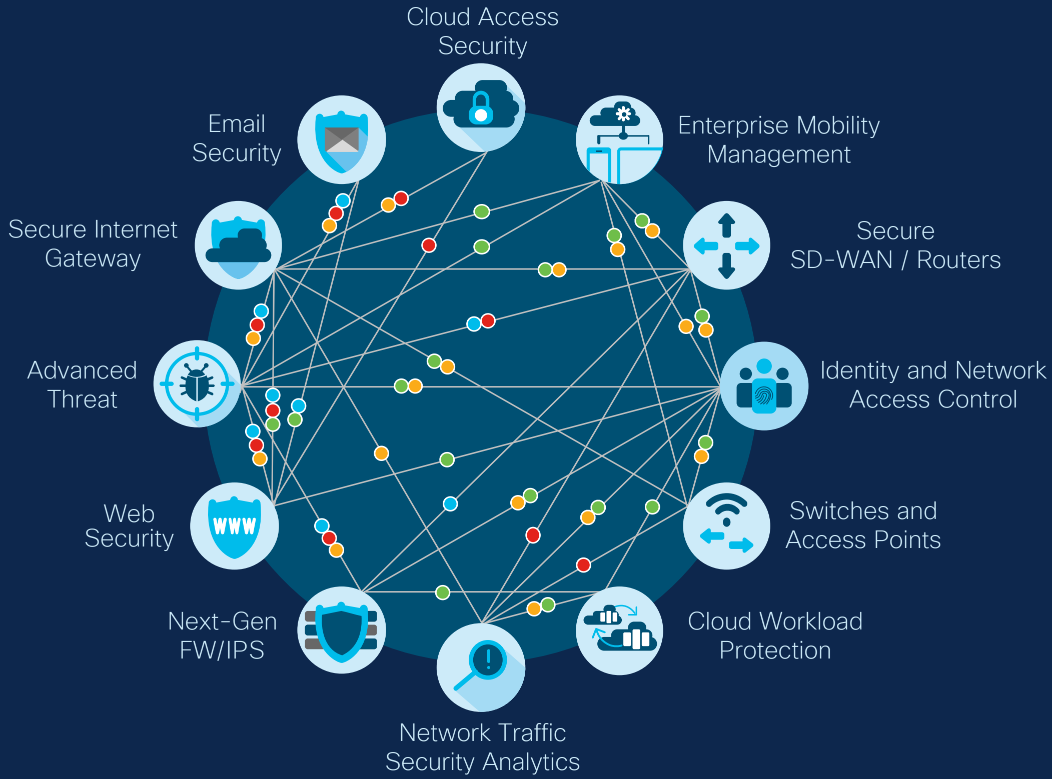
How Cisco Integrates Security

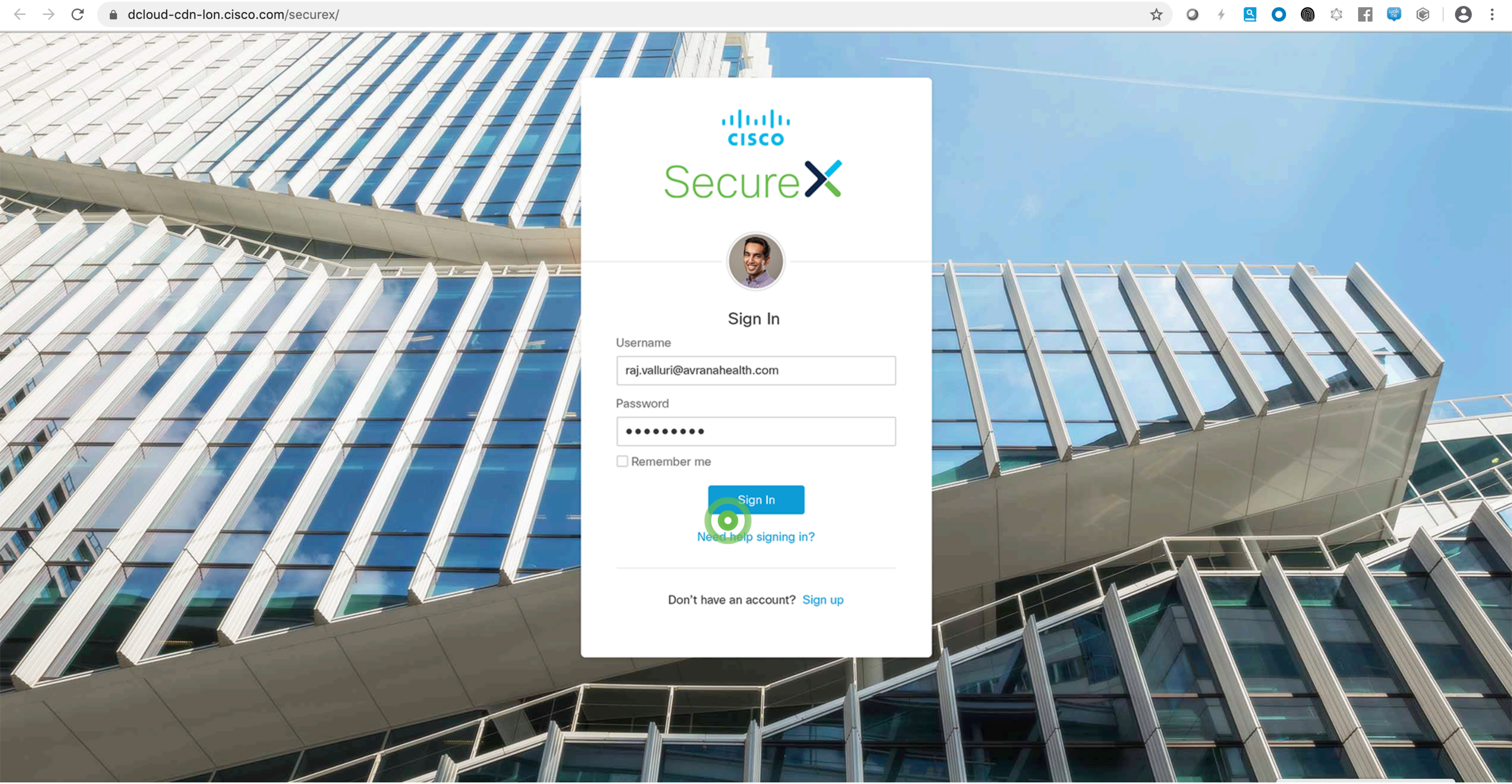
Threat Intel/Enforcement
Increased Threat Prevention

Event Visibility
Decreased Time to Detect

Context Awareness
Decreased Time to Investigate

Automated Policy
Decreased Time to Remediate


Cloud Access Security
Enterprise Mobility Management
Secure SD-WAN / Routers
Identity and Network Access Control
Switches and Access Points
Cloud Workload Protection
Network Traffic Security Analytics
Next-Gen FW/IPS
Web Security
Advanced Threat
Secure Internet Gateway
Email Security
WWW



dcloud-cdn-lon.cisco.com/securex/

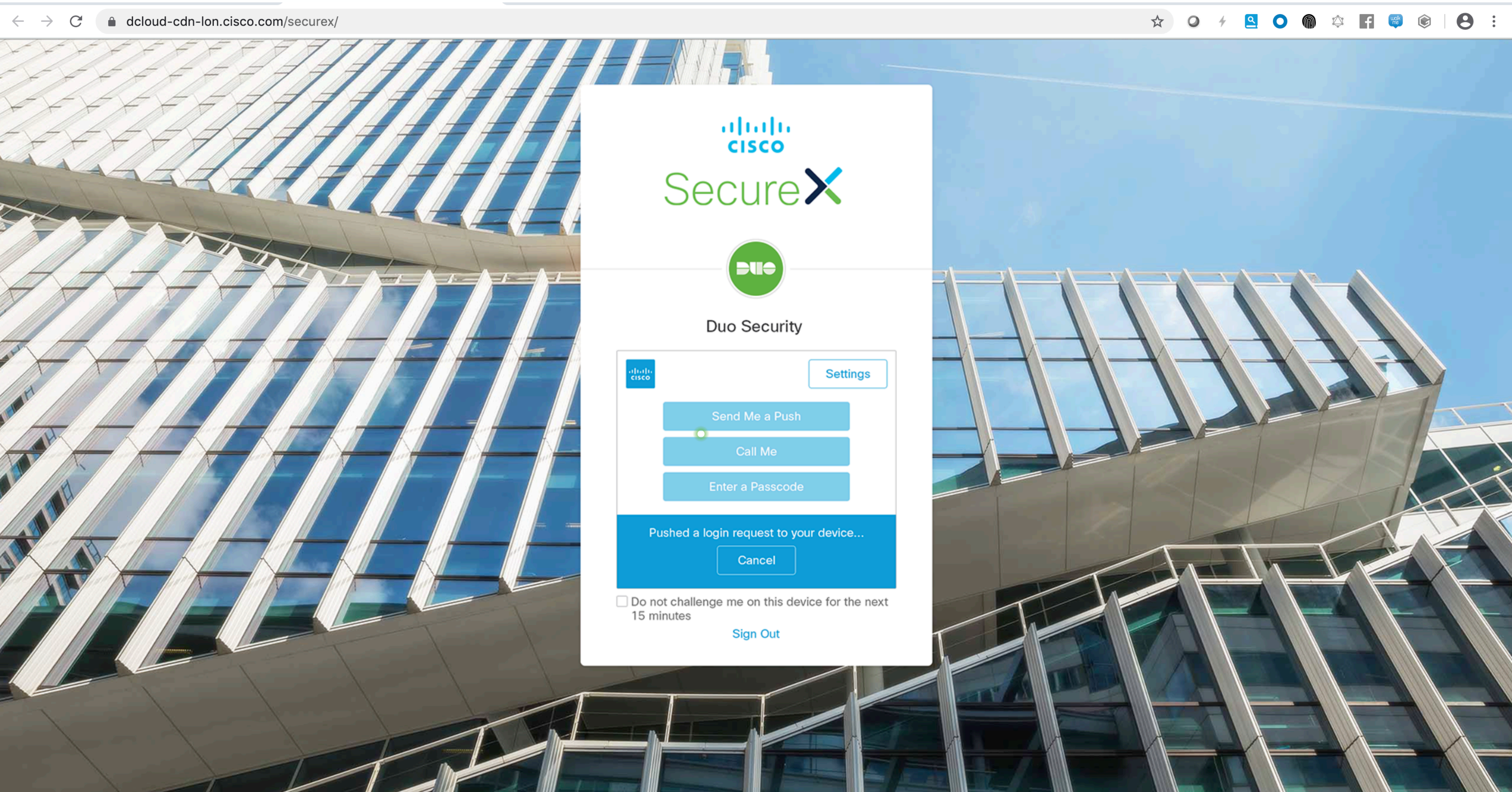
Sign In

Username

raj.valluri@avranahealth.com

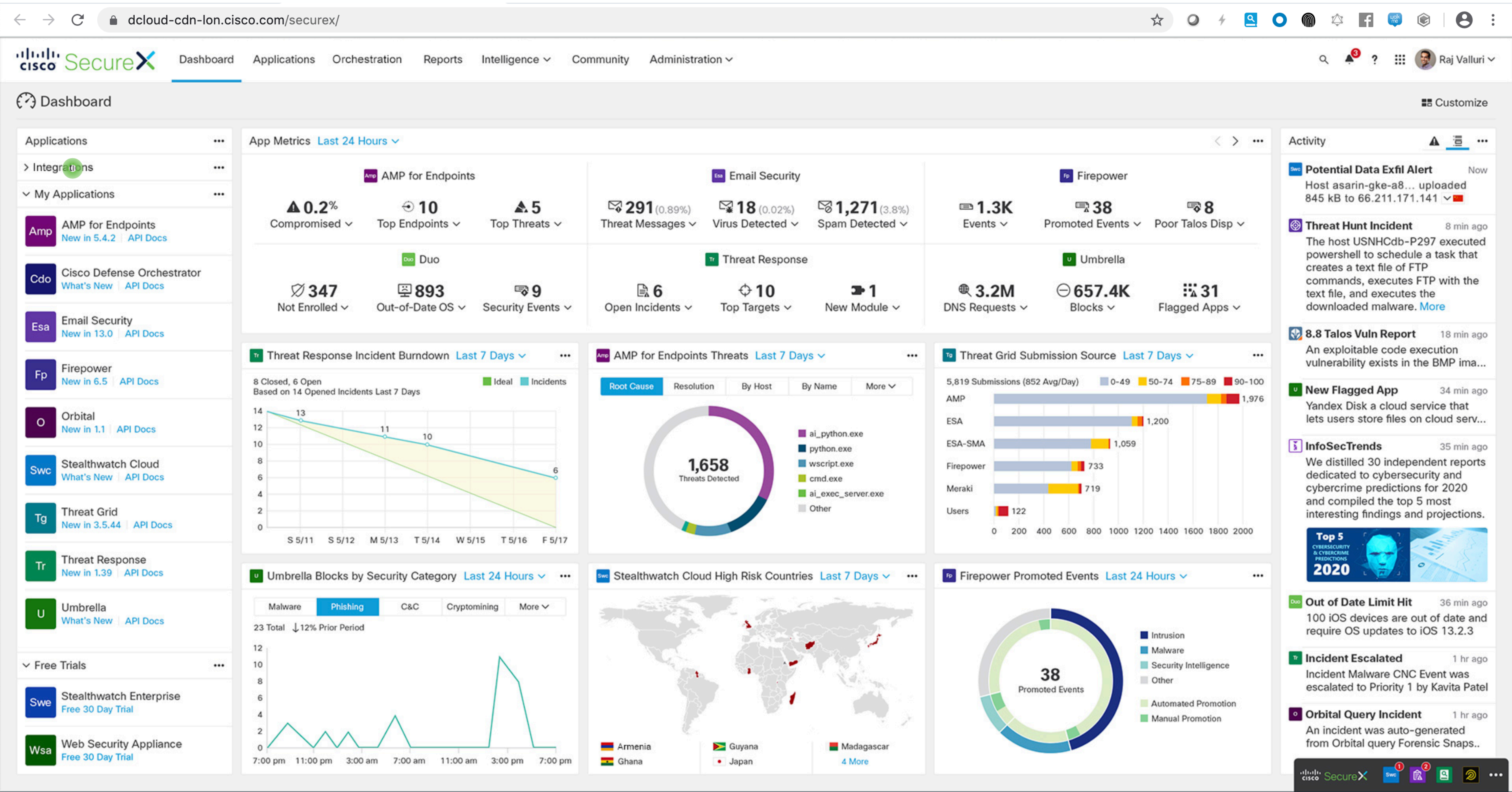
Password

••••••••••



Pushed a login request to your device...

□ Do not challenge me on this device for the next 15 minutes



Amp	AMP for Endpoints	New in 5.4.2 | API Docs
Cdo	Cisco Defense Orchestrator	What's New | API Docs
Esa	Email Security	New in 13.0 | API Docs
Fp	Firepower	New in 6.5 | API Docs
O	Orbital	New in 1.1 | API Docs
Swc	Stealthwatch Cloud	What's New | API Docs
Tg	Threat Grid	New in 3.5.44 | API Docs
Tr	Threat Response	New in 1.39 | API Docs
U	Umbrella	What's New | API Docs

Free Trials

Swe	Stealthwatch Enterprise	Free 30 Day Trial
Wsa	Web Security Appliance	Free 30 Day Trial

Potential Data Exfil Alert Now
Host asarin-gke-a8... uploaded 845 kB to 66.211.171.141

Threat Hunt Incident 8 min ago
The host USNHCdb-P297 executed powershell to schedule a task that creates a text file of FTP commands, executes FTP with the text file, and executes the downloaded malware. More

8.8 Talos Vuln Report 18 min ago
An exploitable code execution vulnerability exists in the BMP ima...

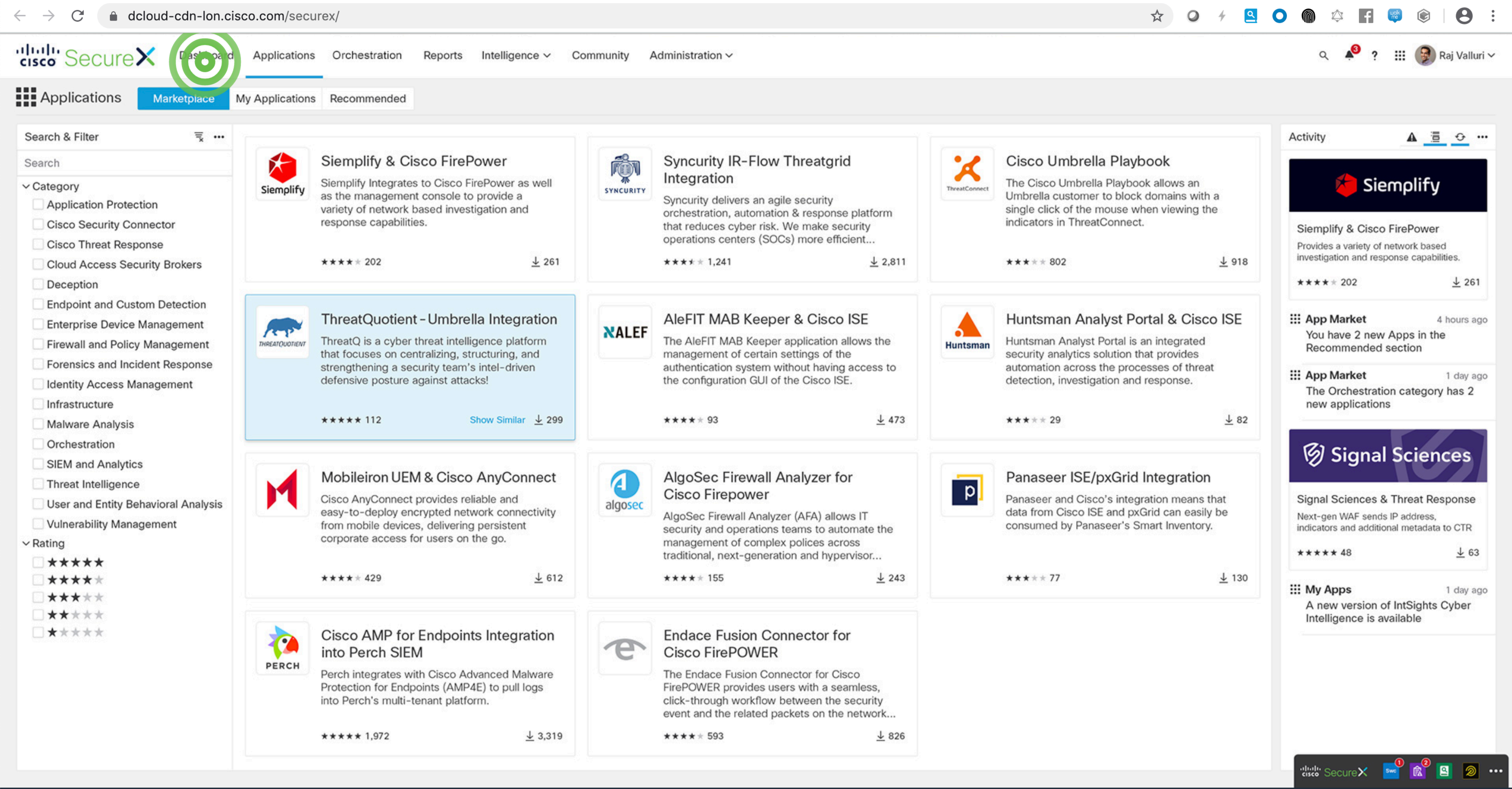
New Flagged App 34 min ago
Yandex Disk a cloud service that lets users store files on cloud serv...

InfoSecTrends 35 min ago
We distilled 30 independent reports dedicated to cybersecurity and cybercrime predictions for 2020 and compiled the top 5 most interesting findings and projections.

Out of Date Limit Hit 36 min ago
100 iOS devices are out of date and require OS updates to iOS 13.2.3

Incident Escalated 1 hr ago
Incident Malware CNC Event was escalated to Priority 1 by Kavita Patel

Orbital Query Incident 1 hr ago
An incident was auto-generated from Orbital query Forensic Snaps..



□ Application Protection
□ Cisco Security Connector
□ Cisco Threat Response
□ Cloud Access Security Brokers
□ Deception
□ Endpoint and Custom Detection
□ Enterprise Device Management
□ Firewall and Policy Management
□ Forensics and Incident Response
□ Identity Access Management
□ Infrastructure
□ Malware Analysis
□ Orchestration
□ SIEM and Analytics
□ Threat Intelligence
□ User and Entity Behavioral Analysis
□ Vulnerability Management

□ ★★★★★
□ ★★★★☆
□ ★★★☆☆
□ ★★☆☆☆
□ ★☆☆☆☆

Siemplify & Cisco FirePower
Siemplify Integrates to Cisco FirePower as well as the management console to provide a variety of network based investigation and response capabilities.
★★★★☆ 202 ⤓ 261

Syncurity IR-Flow Threatgrid Integration
Syncurity delivers an agile security orchestration, automation & response platform that reduces cyber risk. We make security operations centers (SOCs) more efficient...
★★★★☆ 1,241 ⤓ 2,811

Cisco Umbrella Playbook
The Cisco Umbrella Playbook allows an Umbrella customer to block domains with a single click of the mouse when viewing the indicators in ThreatConnect.
★★★☆☆ 802 ⤓ 918

ThreatQuotient - Umbrella Integration
ThreatQ is a cyber threat intelligence platform that focuses on centralizing, structuring, and strengthening a security team's intel-driven defensive posture against attacks!
★★★★★ 112 Show Similar ⤓ 299

AleFIT MAB Keeper & Cisco ISE
The AleFIT MAB Keeper application allows the management of certain settings of the authentication system without having access to the configuration GUI of the Cisco ISE.
★★★★☆ 93 ⤓ 473

Huntsman Analyst Portal & Cisco ISE
Huntsman Analyst Portal is an integrated security analytics solution that provides automation across the processes of threat detection, investigation and response.
★★★☆☆ 29 ⤓ 82

Mobileiron UEM & Cisco AnyConnect
Cisco AnyConnect provides reliable and easy-to-deploy encrypted network connectivity from mobile devices, delivering persistent corporate access for users on the go.
★★★★☆ 429 ⤓ 612

AlgoSec Firewall Analyzer for Cisco Firepower
AlgoSec Firewall Analyzer (AFA) allows IT security and operations teams to automate the management of complex polices across traditional, next-generation and hypervisor...
★★★★☆ 155 ⤓ 243

Panaseer ISE/pxGrid Integration
Panaseer and Cisco's integration means that data from Cisco ISE and pxGrid can easily be consumed by Panaseer's Smart Inventory.
★★★☆☆ 77 ⤓ 130

Cisco AMP for Endpoints Integration into Perch SIEM
Perch integrates with Cisco Advanced Malware Protection for Endpoints (AMP4E) to pull logs into Perch's multi-tenant platform.
★★★★★ 1,972 ⤓ 3,319

Endace Fusion Connector for Cisco FirePOWER
The Endace Fusion Connector for Cisco FirePOWER provides users with a seamless, click-through workflow between the security event and the related packets on the network...
★★★★☆ 593 ⤓ 826

Siemplify & Cisco FirePower
Provides a variety of network based investigation and response capabilities.
★★★★☆ 202 ⤓ 261

App Market 4 hours ago
You have 2 new Apps in the Recommended section

App Market 1 day ago
The Orchestration category has 2 new applications

Signal Sciences & Threat Response
Next-gen WAF sends IP address, indicators and additional metadata to CTR
★★★★★ 48 ⤓ 63

My Apps 1 day ago
A new version of IntSights Cyber Intelligence is available

SAFE: A Model for identifying flows

	HUMAN	DEVICE	NETWORK					APPLICATION
	Role	Client	Wired	Wireless	Analysis	WAN	Cloud	Server
Attackable Surface	Employee	Workstation	Wired Network	Wireless Connection	Analytic Engine	Public WAN	Public/Hybrid Cloud	Application
Threats	Rogue	Infection	Unauthorized	Rogue	Malware	Public Untrusted	Untrusted	Infection
Security Capabilities	Identity	Client-Based Security Posture Assessment	Firewall Intrusion Prevention Tagging	Wireless Intrusion Prevention (WIPS) Wireless Rogue Detection	Network Anti-Malware Flow Analytics Threat Intelligence	Virtual Private Network (VPN) Web Security Email Security	Cloud Security	Server-Based Security

Advanced Threat

Relentless Breach Defense

Save time by automating threat hunting and investigation with Orbital Advanced Search

- Key capabilities:

  Advanced search; pre-defined, customizable queries; forensics snapshot

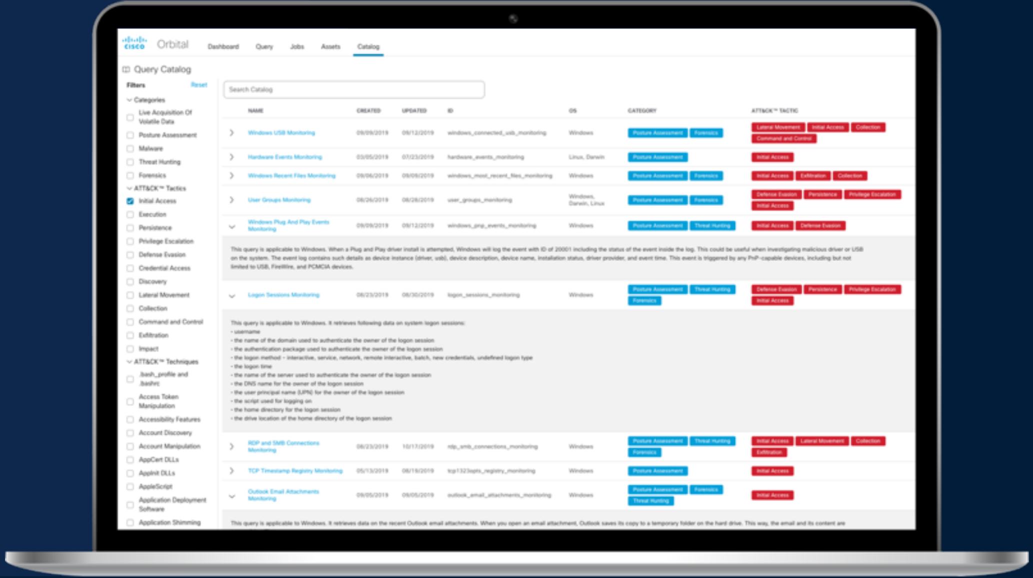
- Primary use cases:

  Threat hunting; IT operations enablement, and vulnerability and compliance tracking

- Benefits:

  Faster investigation leads to quicker response, and ultimately lower cost of the breach

- Seamless investigation and remediation with Cisco Threat Response



Query Catalog

Filters Reset

Search Catalog

Categories

- □ Live Acquisition Of Volatile Data
- □ Posture Assessment
- □ Malware
- □ Threat Hunting
- □ Forensics

ATT&CK™ Tactics

- ☑ Initial Access
- □ Execution
- □ Persistence
- □ Privilege Escalation
- □ Defense Evasion
- □ Credential Access
- □ Discovery
- □ Lateral Movement
- □ Collection
- □ Command and Control
- □ Exfiltration
- □ Impact

ATT&CK™ Techniques

- □ .bash_profile and .bashrc
- □ Access Token Manipulation
- □ Accessibility Features
- □ Account Discovery
- □ Account Manipulation
- □ AppCert DLLs
- □ AppInit DLLs
- □ AppleScript
- □ Application Deployment Software
- □ Application Shimming

NAME	CREATED	UPDATED	ID	OS	CATEGORY	ATT&CK™ TACTIC
Windows USB Monitoring	09/09/2019	09/12/2019	windows_connected_usb_monitoring	Windows	Posture Assessment Forensics	Lateral Movement Initial Access Collection Command and Control
Hardware Events Monitoring	03/05/2019	07/23/2019	hardware_events_monitoring	Linux, Darwin	Posture Assessment	Initial Access
Windows Recent Files Monitoring	09/06/2019	09/09/2019	windows_most_recent_files_monitoring	Windows	Posture Assessment Forensics	Initial Access Exfiltration Collection
User Groups Monitoring	08/26/2019	08/28/2019	user_groups_monitoring	Windows, Darwin, Linux	Posture Assessment Forensics	Defense Evasion Persistence Privilege Escalation Initial Access
Windows Plug And Play Events Monitoring	09/09/2019	09/12/2019	windows_pnp_events_monitoring	Windows	Posture Assessment Threat Hunting	Initial Access Defense Evasion

This query is applicable to Windows. When a Plug and Play driver install is attempted, Windows will log the event with ID of 20001 including the status of the event inside the log. This could be useful when investigating malicious driver or USB on the system. The event log contains such details as device instance (driver, usb), device description, device name, installation status, driver provider, and event time. This event is triggered by any PnP-capable devices, including but not limited to USB, FireWire, and PCMCIA devices.

NAME	CREATED	UPDATED	ID	OS	CATEGORY	ATT&CK™ TACTIC
Logon Sessions Monitoring	08/23/2019	08/30/2019	logon_sessions_monitoring	Windows	Posture Assessment Threat Hunting Forensics	Defense Evasion Persistence Privilege Escalation Initial Access

This query is applicable to Windows. It retrieves following data on system logon sessions:
- username
- the name of the domain used to authenticate the owner of the logon session
- the authentication package used to authenticate the owner of the logon session
- the logon method - interactive, service, network, remote interactive, batch, new credentials, undefined logon type
- the logon time
- the name of the server used to authenticate the owner of the logon session
- the DNS name for the owner of the logon session
- the user principal name (UPN) for the owner of the logon session
- the script used for logging on
- the home directory for the logon session
- the drive location of the home directory of the logon session

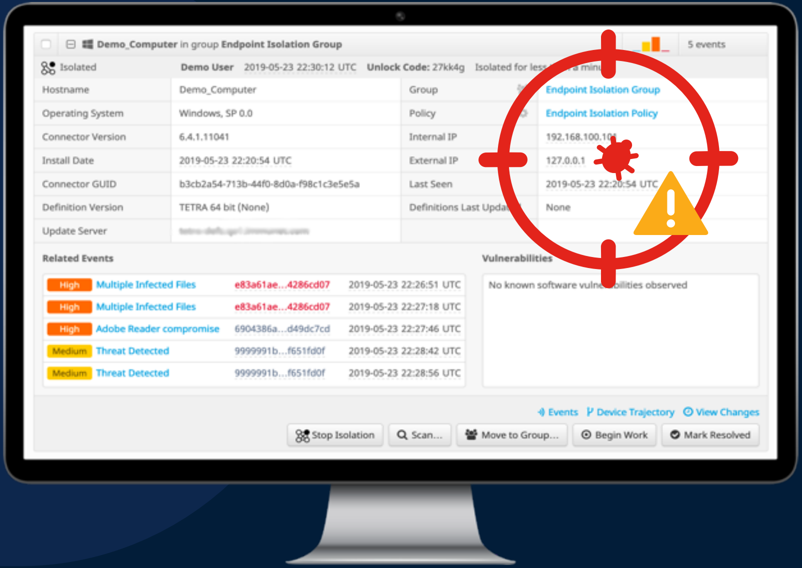
NAME	CREATED	UPDATED	ID	OS	CATEGORY	ATT&CK™ TACTIC
RDP and SMB Connections Monitoring	08/23/2019	10/17/2019	rdp_smb_connections_monitoring	Windows	Posture Assessment Threat Hunting Forensics	Initial Access Lateral Movement Collection Exfiltration
TCP Timestamp Registry Monitoring	05/13/2019	08/19/2019	tcp1323opts_registry_monitoring	Windows	Posture Assessment	Initial Access
Outlook Email Attachments Monitoring	09/05/2019	09/05/2019	outlook_email_attachments_monitoring	Windows	Posture Assessment Forensics Threat Hunting	Initial Access

This query is applicable to Windows. It retrieves data on the recent Outlook email attachments. When you open an email attachment, Outlook saves its copy to a temporary folder on the hard drive. This way, the email and its content are

Relentless Breach Defense

Contain the attack fast with **Endpoint Isolation**

- Isolate infected hosts from the rest of the network
- Contain the threat without losing forensics data
- Shrink remediation cost by limiting the scale of attack
- Fast endpoint reactivation once remediation is complete
- Take action directly from the AMP Console, Cisco Threat Response or API scripting



Demo_Computer in group **Endpoint Isolation Group** 5 events

Isolated **Demo User** 2019-05-23 22:30:12 UTC **Unlock Code:** 27kk4g Isolated for less a minu

Hostname	Demo_Computer	Group	Endpoint Isolation Group
Operating System	Windows, SP 0.0	Policy	Endpoint Isolation Policy
Connector Version	6.4.1.11041	Internal IP	192.168.100.10
Install Date	2019-05-23 22:20:54 UTC	External IP	127.0.0.1
Connector GUID	b3cb2a54-713b-44f0-8d0a-f98c1c3e5e5a	Last Seen	2019-05-23 22:20:54 UTC
Definition Version	TETRA 64 bit (None)	Definitions Last Upda	None
Update Server	[redacted]		

Related Events

High	Multiple Infected Files	e83a61ae...4286cd07	2019-05-23 22:26:51 UTC
High	Multiple Infected Files	e83a61ae...4286cd07	2019-05-23 22:27:18 UTC
High	Adobe Reader compromise	6904386a...d49dc7cd	2019-05-23 22:27:46 UTC
Medium	Threat Detected	9999991b...f651fd0f	2019-05-23 22:28:42 UTC
Medium	Threat Detected	9999991b...f651fd0f	2019-05-23 22:28:56 UTC

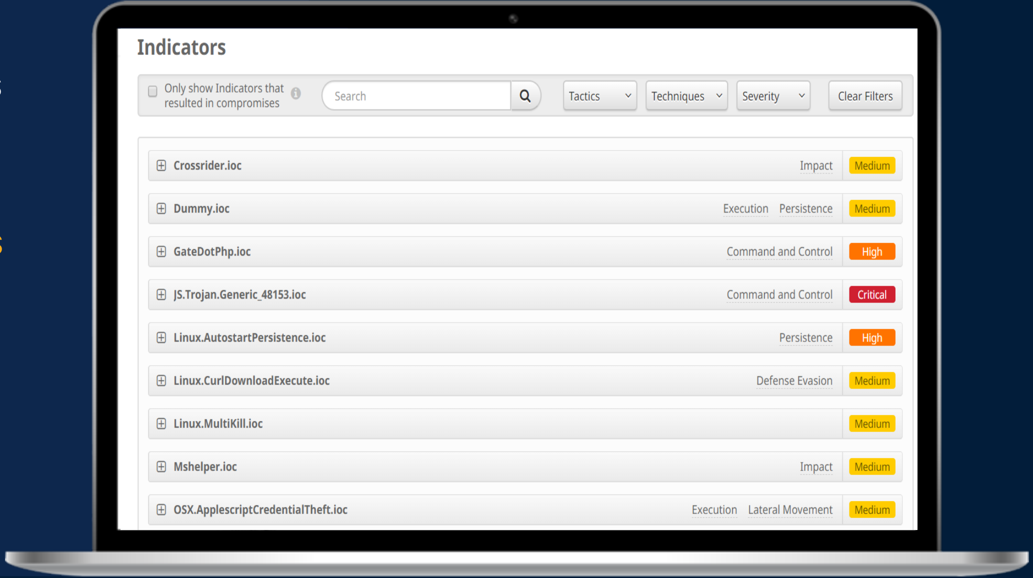
Vulnerabilities

No known software vulne bilities observed

Relentless Breach Defense

Gain deeper insight on Cisco's Coverage
Indicators of Compromise

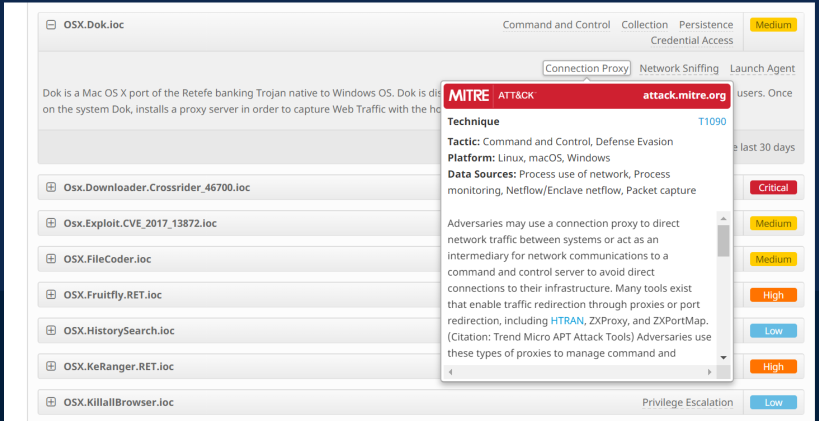
- A new Indicators page maps Cloud Indications of Compromise (IOCs) to the MITRE ATT&CK knowledge base of tactics and techniques
- You can search/filter the knowledge base by indicator name, tactics, and techniques



Indicators

☐ Only show Indicators that resulted in compromises | Search | Tactics | Techniques | Severity | Clear Filters

⊞ Crossrider.ioc	Impact	Medium
⊞ Dummy.ioc	Execution Persistence	Medium
⊞ GateDotPhp.ioc	Command and Control	High
⊞ JS.Trojan.Generic_48153.ioc	Command and Control	Critical
⊞ Linux.AutostartPersistence.ioc	Persistence	High
⊞ Linux.CurlDownloadExecute.ioc	Defense Evasion	Medium
⊞ Linux.MultiKill.ioc		Medium
⊞ Mshelper.ioc	Impact	Medium
⊞ OSX.ApplescriptCredentialTheft.ioc	Execution Lateral Movement	Medium



⊟ OSX.Dok.ioc — Command and Control Collection Persistence Credential Access — Medium

Connection Proxy Network Sniffing Launch Agent

Dok is a Mac OS X port of the Retefe banking Trojan native to Windows OS. Dok is dis users. Once on the system Dok, installs a proxy server in order to capture Web Traffic with the ho

e last 30 days

MITRE ATT&CK attack.mitre.org

Technique T1090

Tactic: Command and Control, Defense Evasion
Platform: Linux, macOS, Windows
Data Sources: Process use of network, Process monitoring, Netflow/Enclave netflow, Packet capture

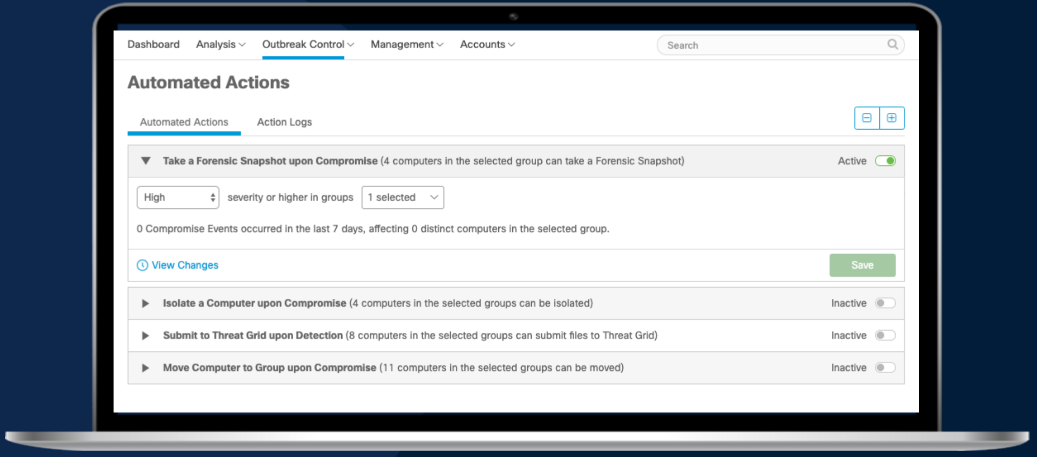
Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and

⊞ Osx.Downloader.Crossrider_46700.ioc		Critical
⊞ Osx.Exploit.CVE_2017_13872.ioc		Medium
⊞ OSX.FileCoder.ioc		Medium
⊞ OSX.Fruitfly.RET.ioc		High
⊞ OSX.HistorySearch.ioc		Low
⊞ OSX.KeRanger.RET.ioc		High
⊞ OSX.KillallBrowser.ioc	Privilege Escalation	Low

Relentless Breach Defense

Drive more automation for incident response with **Automated Actions**

- A new feature which allows actions to be driven by events to automate common tasks when a threat is detected
- Capture a forensic snapshot when an endpoint is compromised
- Isolate a computer upon compromise
- Submit a file to Threat Grid for dynamic analysis upon detection
- Move a computer a computer to an audit group upon compromise



Automated Actions

Take a Forensic Snapshot upon Compromise (4 computers in the selected group can take a Forensic Snapshot) Active

High severity or higher in groups 1 selected

0 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected group.

Isolate a Computer upon Compromise (4 computers in the selected groups can be isolated) Inactive

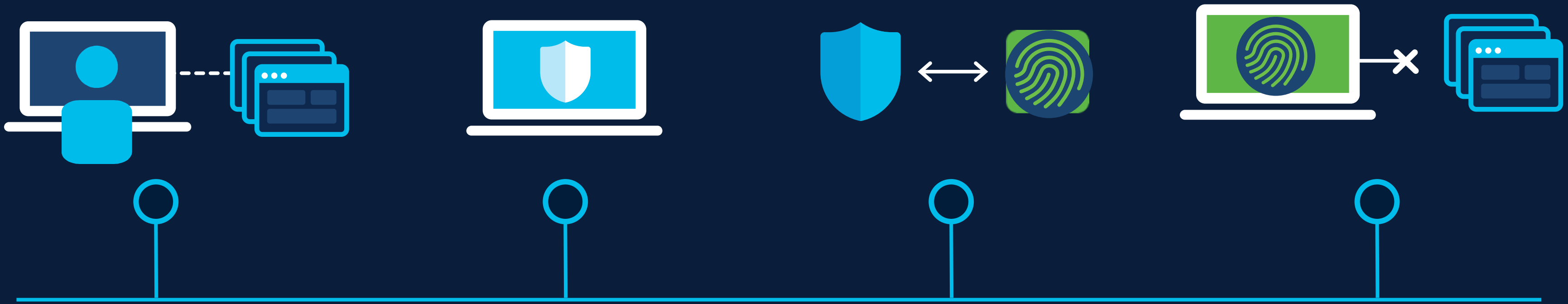
Submit to Threat Grid upon Detection (8 computers in the selected groups can submit files to Threat Grid) Inactive

Move Computer to Group upon Compromise (11 computers in the selected groups can be moved) Inactive

Protect applications from infected devices

A4E + Duo

Block malicious devices from accessing applications.



Users use their devices to access application.

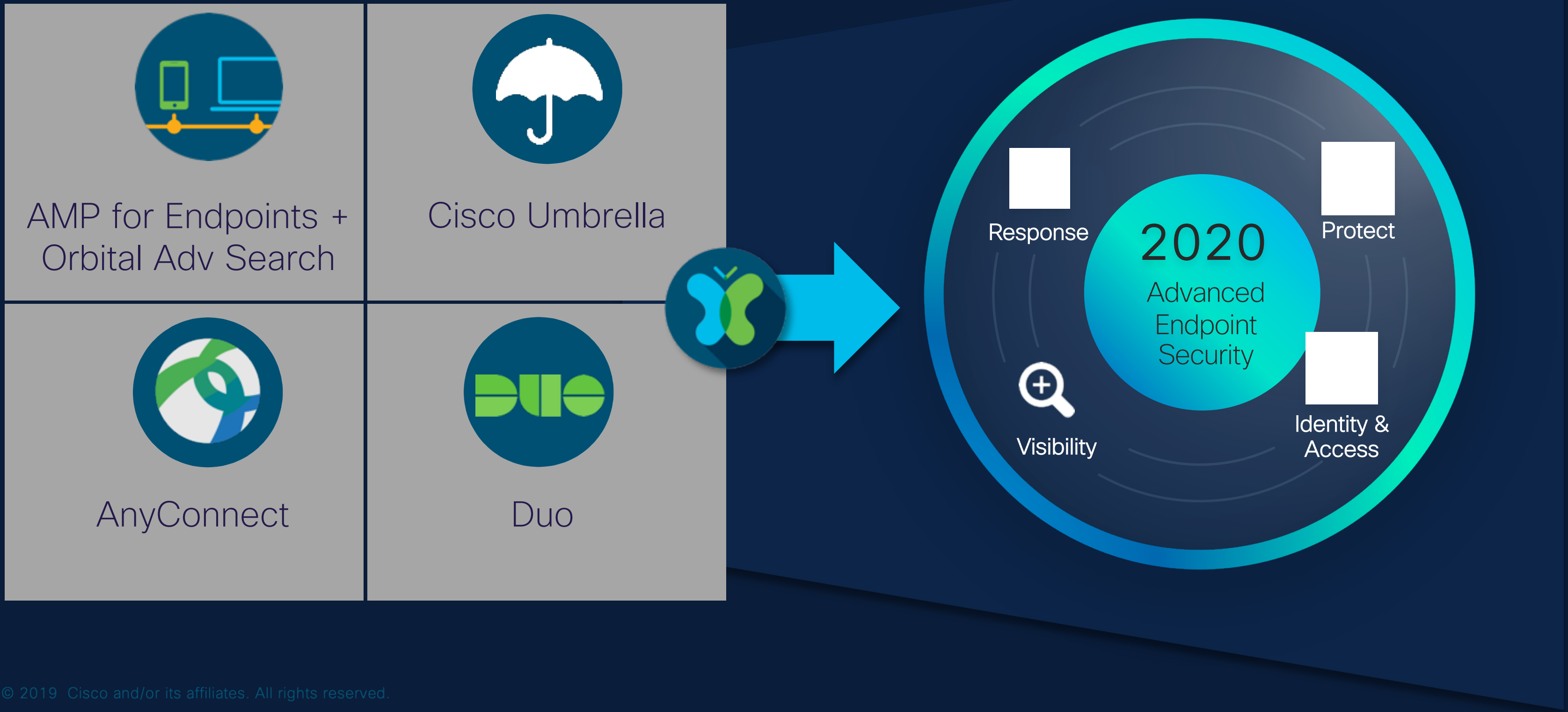
Endpoint security from Cisco running on the device detects malware.

It notifies the MFA about the infected device.

MFA blocks that device from accessing apps.

Unified Endpoints Agent

A true market differentiator



AMP for Endpoints + Orbital Adv Search

Cisco Umbrella

AnyConnect

Duo

Network Visibility And Segmentation (SW, ISE)

Stealthwatch Enterprise Releases 7.1.2 & 7.2.0

Enhanced Security Analytics

- Unified Threat Hunting with Cisco Threat Response (CTR)

Increased Performance

- Flow Sensor 4240
- 80G throughput
- 2x 40G QSFP or 4x 10G SFP fiber interfaces

Improved Usability

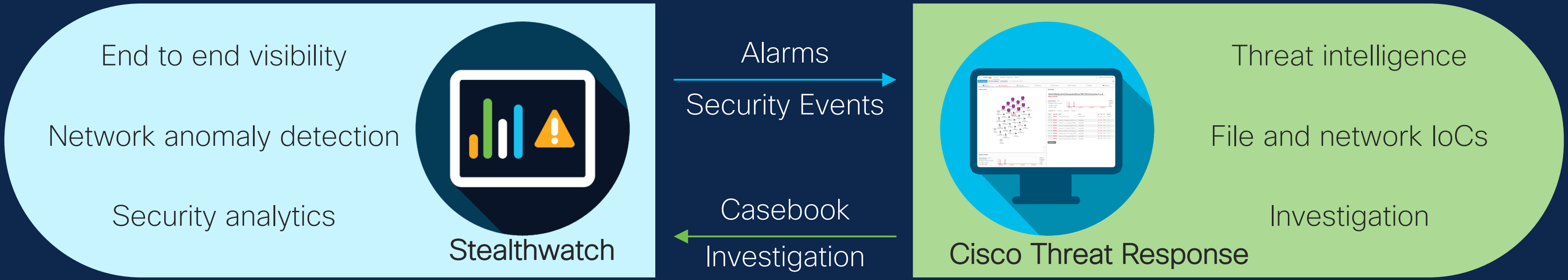
- TACACS+ Authorization
- Smart Licensing Support
- Migration of configuration from Swing to Web UI

User Management

- Personal information management
- Improved remote authorization manageability
- Plan of Action and Milestones (POA&M)

Integration with Cisco Threat Response

For accelerated investigation and remediation



End to end visibility

Network anomaly detection

Security analytics

Stealthwatch

Alarms

Security Events

Casebook

Investigation

Threat intelligence

File and network IoCs

Investigation

Cisco Threat Response

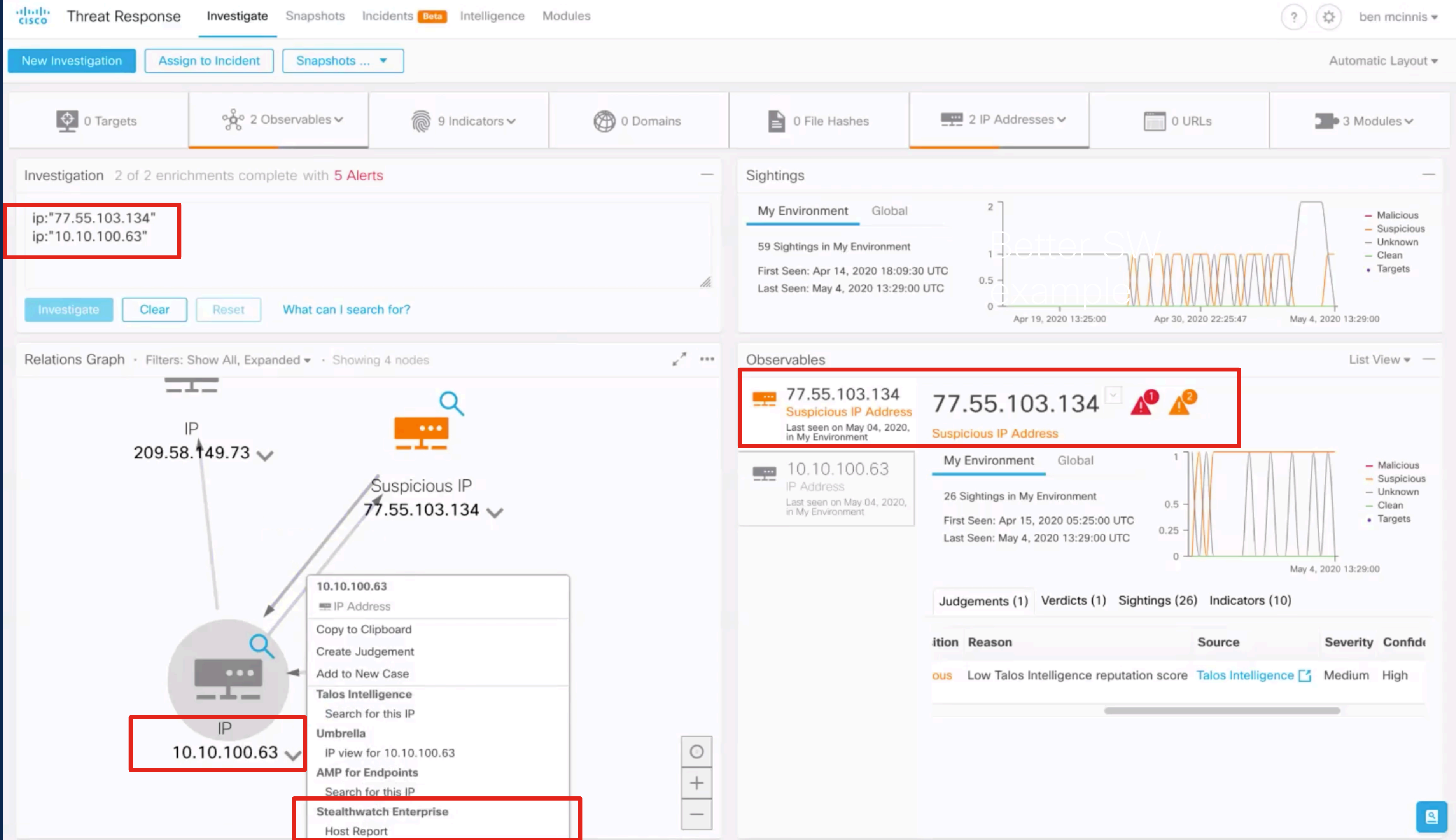
Agentless Detection

Stealthwatch network-based visibility and security analytics will enrich CTR threat detection and response with agentless behavioral and anomaly detection capabilities

Correlate, Enrich, and Resolve

CTR integrations with other sources of global threat intelligence and internal visibility, will affirm and enrich Stealthwatch findings with confirmed threat intel and local sightings. Integrations with Cisco control devices provide two-click mitigation and resolution.

GSO GO-TO-MARKET STRATEGY & OPERATIONS



Investigation 2 of 2 enrichments complete with 5 Alerts

```
ip:"77.55.103.134"
ip:"10.10.100.63"
```

Sightings

59 Sightings in My Environment

First Seen: Apr 14, 2020 18:09:30 UTC
Last Seen: May 4, 2020 13:29:00 UTC

Observables

77.55.103.134
Suspicious IP Address
Last seen on May 04, 2020, in My Environment

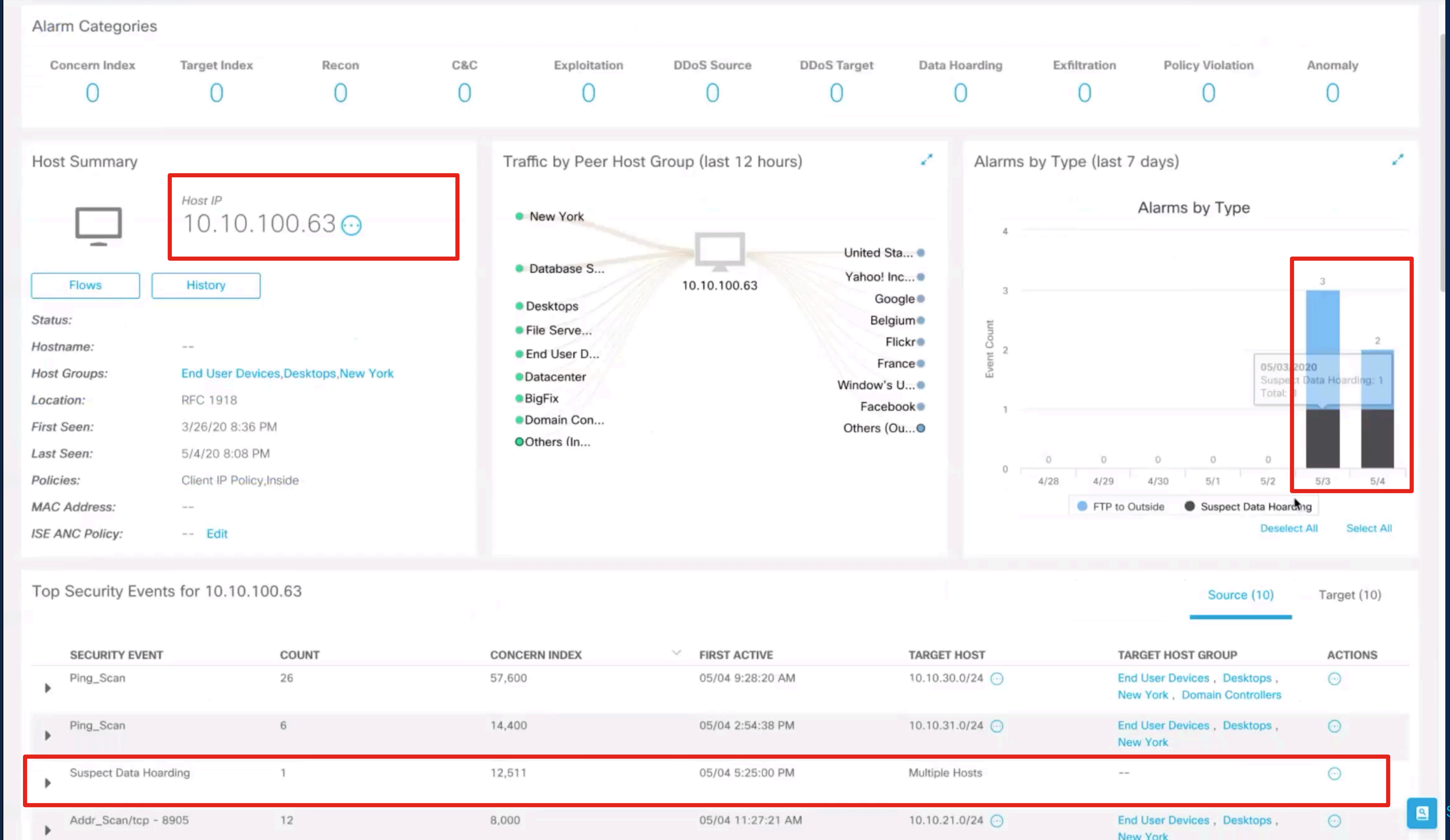
77.55.103.134
Suspicious IP Address

10.10.100.63
IP Address
Last seen on May 04, 2020, in My Environment

26 Sightings in My Environment

First Seen: Apr 15, 2020 05:25:00 UTC
Last Seen: May 4, 2020 13:29:00 UTC

ition	Reason	Source	Severity	Confid
ous	Low Talos Intelligence reputation score	Talos Intelligence	Medium	High



Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	0	0	0	0

Host Summary

Host IP

10.10.100.63

Status:	
Hostname:	--
Host Groups:	End User Devices,Desktops,New York
Location:	RFC 1918
First Seen:	3/26/20 8:36 PM
Last Seen:	5/4/20 8:08 PM
Policies:	Client IP Policy,Inside
MAC Address:	--
ISE ANC Policy:	-- Edit

Traffic by Peer Host Group (last 12 hours)

Alarms by Type (last 7 days)

Top Security Events for 10.10.100.63

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TARGET HOST GROUP	ACTIONS
▸ Ping_Scan	26	57,600	05/04 9:28:20 AM	10.10.30.0/24	End User Devices , Desktops , New York , Domain Controllers	
▸ Ping_Scan	6	14,400	05/04 2:54:38 PM	10.10.31.0/24	End User Devices , Desktops , New York	
▸ Suspect Data Hoarding	1	12,511	05/04 5:25:00 PM	Multiple Hosts	--	
▸ Addr_Scan/tcp - 8905	12	8,000	05/04 11:27:21 AM	10.10.21.0/24	End User Devices , Desktops , New York	

Stealthwatch Enterprise Releases 7.3.0

Increased Performance

- Centralised datastore provides increased query performance

Easier management

- Full configuration in the WebUI
- Report Builder allows for key netops and secops reporting in the WebUI

Enhanced security analytics

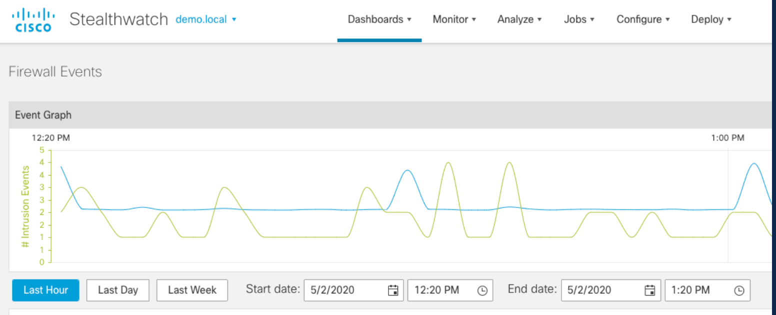
- SAL provides a single logging aggregation point for Cisco's Firewall fleet
- TLS Fingerprinting to improve detections

Context-aware response

- Modernized response management module in WebUI
- Configurable rules and actions such as automated response with ISE & ANC policies
- Additional enhancements related to CTR integration

ANC: Adaptive Network Control

Firepower as a Sensor



Firewall Events

Start date: 5/2/2020 12:20 PM

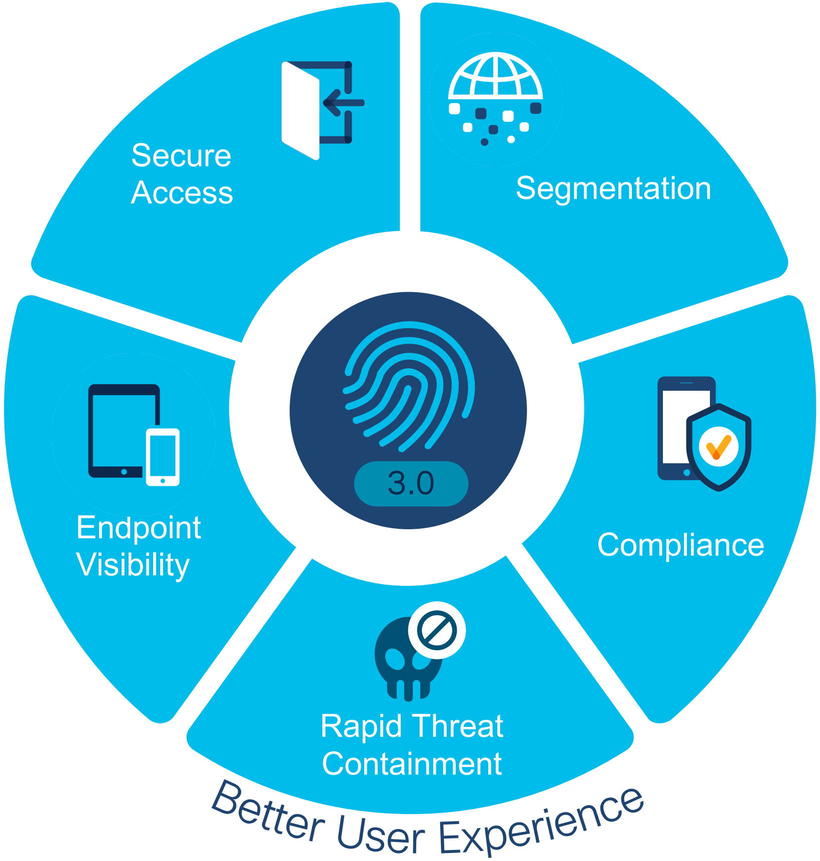
End date: 5/2/2020 1:20 PM

Stealthwatch can now claim all Firepower detections

- Firepower Integration App will be made available to Stealthwatch Customers
- Collection of Firepower events on SMC:
  - Connection
  - Intrusion
  - File
  - Malware

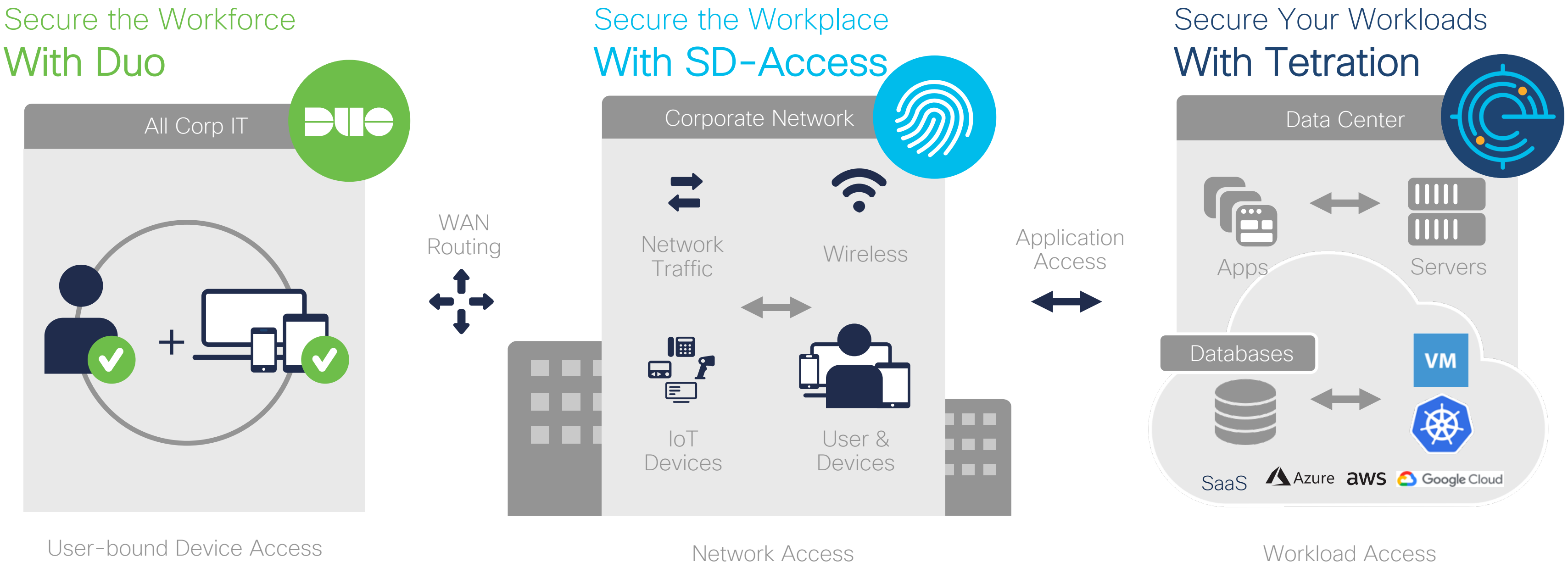
Security Analytics and Logging, SAL
On-Prem

ISE is at the heart of Cisco's Zero Trust Solution



cisco Secure

Cisco Zero Trust



cisco Secure

Next phase of Endpoint Visibility

Endpoint Visibility

Secure Access

Segmentation

Compliance

RTC

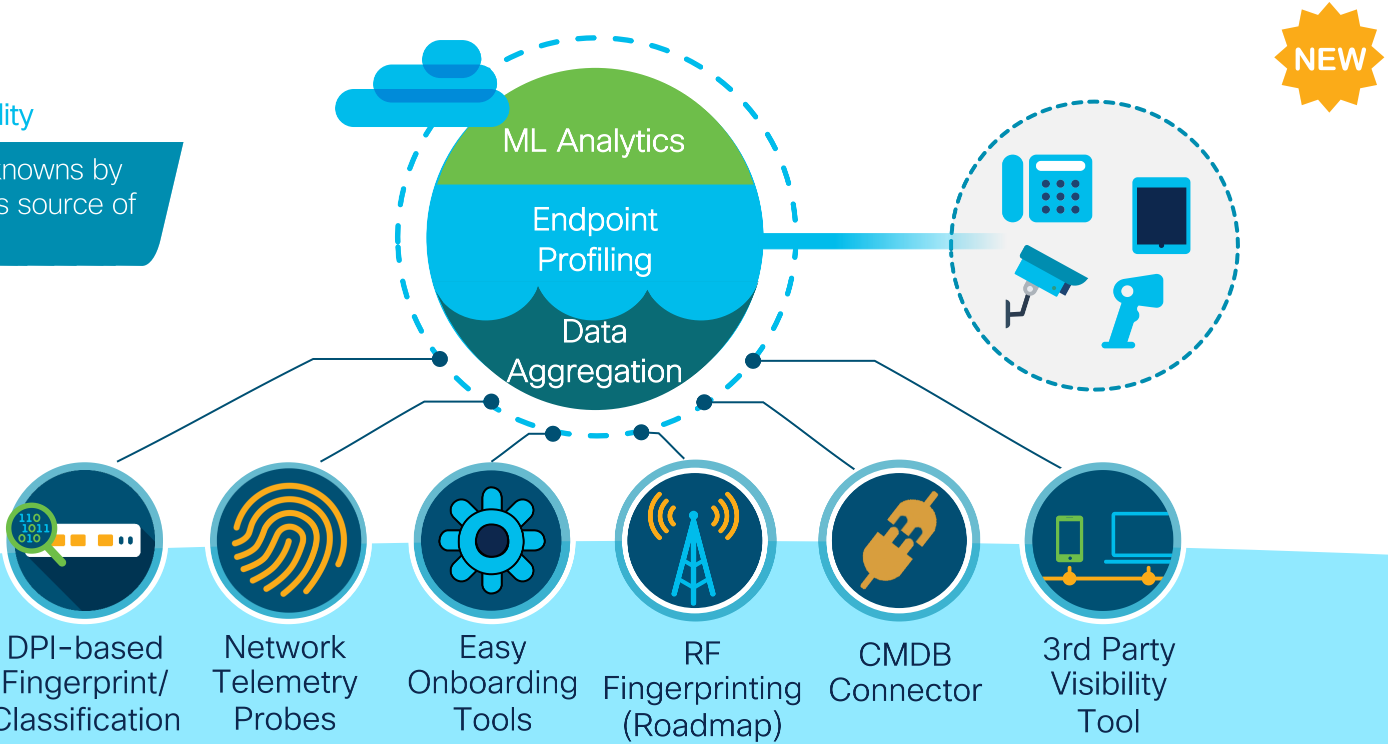
Next generation endpoint visibility with AI-driven analytics and network driven deep packet inspection

cisco Secure

Endpoint Analytics on Cisco DNA Center

High Fidelity Visibility

Rapidly reduce unknowns by aggregating various source of device fingerprints



Next phase of Secure Access

Endpoint Visibility

Secure Access

Segmentation

Compliance

RTC

1. Enabling customer journey to the cloud.

2. Securing access in a MAC (Address) less / randomized MAC world.

3. DevOps friendly platform for managing access policies.

cisco Secure

Next Phase of Segmentation

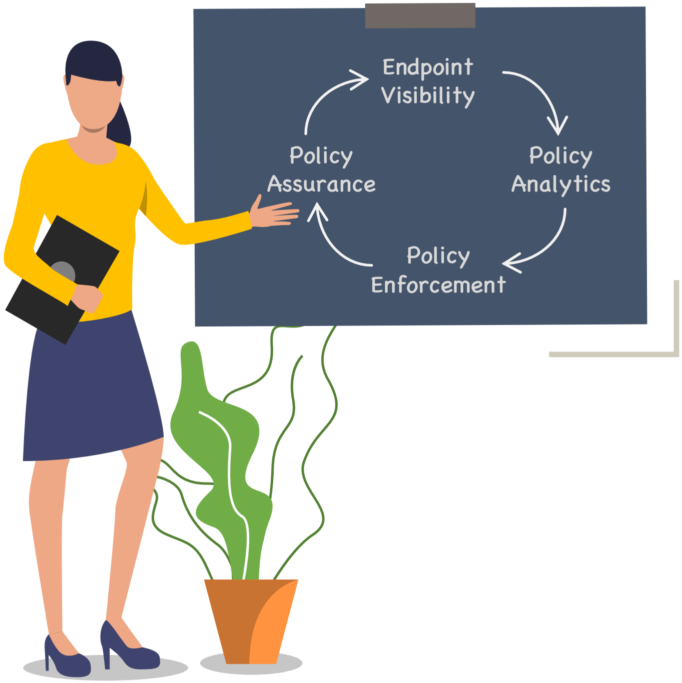
Endpoint Visibility

Secure Access

Segmentation

Compliance

RTC

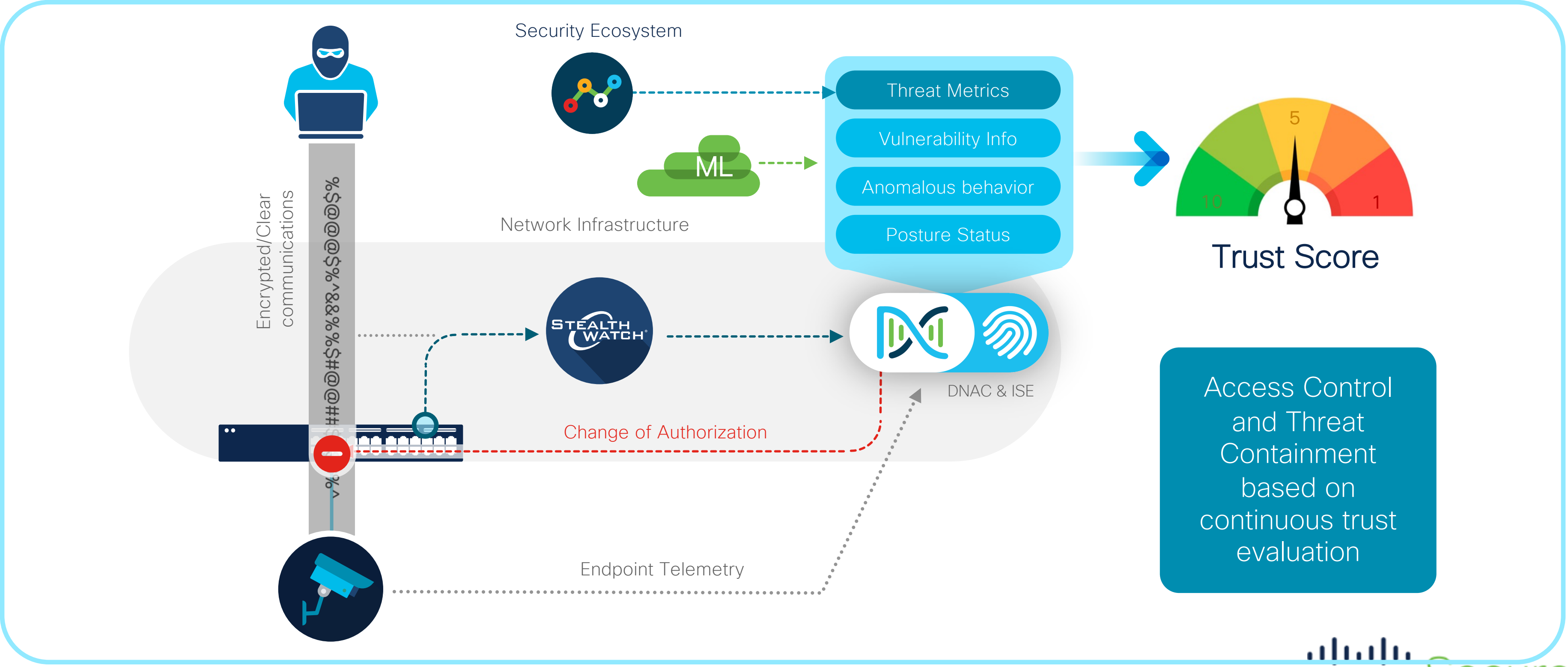


1. Simplified segmentation rollouts with new tools.
2. Best-in-class segmentation solution for brownfield environments
3. Accelerating on Cisco’s multi-domain architecture.

cisco Secure

“Trust” based network access

Bringing it all together



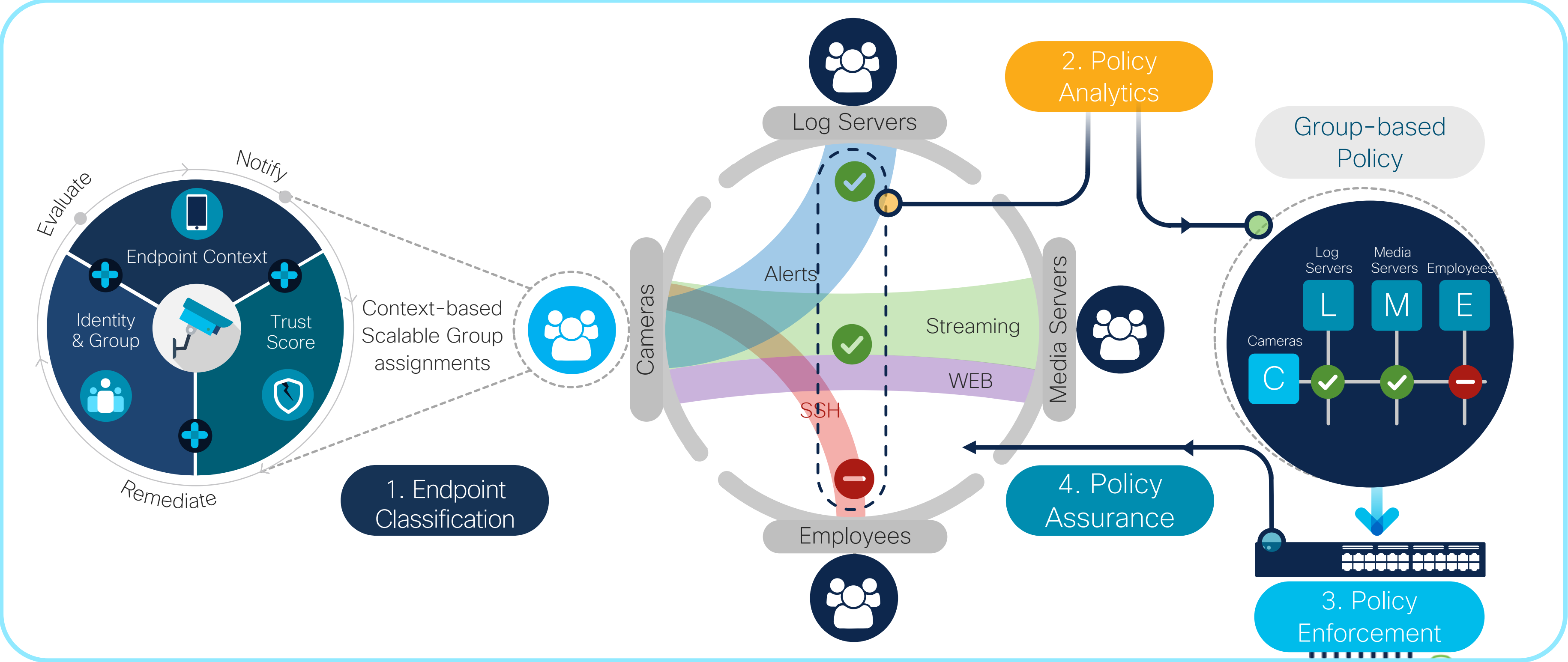
Access Control and Threat Containment based on continuous trust evaluation

→ Trust Score using ML Anomaly detection for endpoint spoofing

Cisco DNAC and ISE

Bring it all together

Visibility Driven Segmentation



cisco Secure

Duo Multifactor Authentication

passwords are not enough

Something you know
(e.g. password)

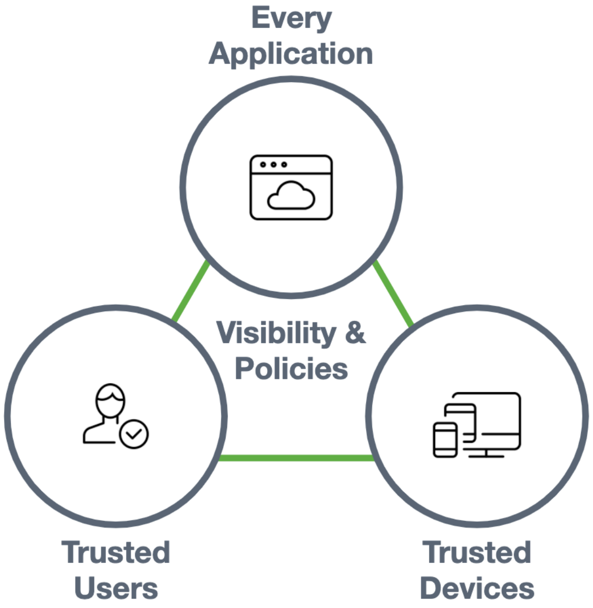
Something you have
(e.g. phone, key..)

Something you are
(e.g. biometrics)

Somewhere you are
(e.g. location)

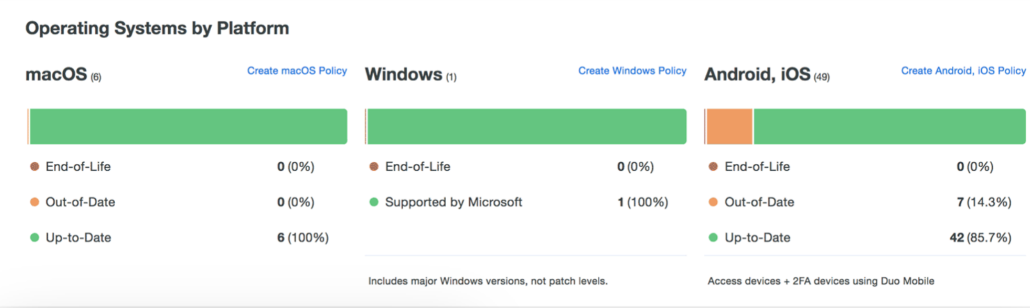
Worlds Easiest and Most Secure MFA

1. Verify Users Identity
2. Verify Device Health
3. Control Access



Gain Complete Visibility

Device Health & Compliance



Operating Systems by Platform

macOS (6) — Create macOS Policy

● End-of-Life	**0** (0%)
● Out-of-Date	**0** (0%)
● Up-to-Date	**6** (100%)

Windows (1) — Create Windows Policy

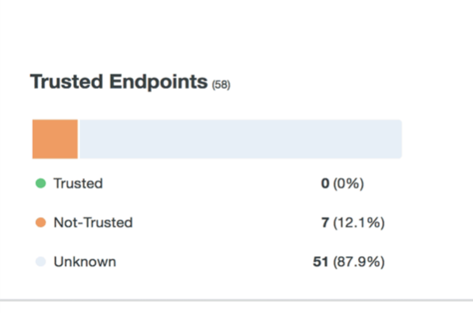
● End-of-Life	**0** (0%)
● Supported by Microsoft	**1** (100%)

Includes major Windows versions, not patch levels.

Android, iOS (49) — Create Android, iOS Policy

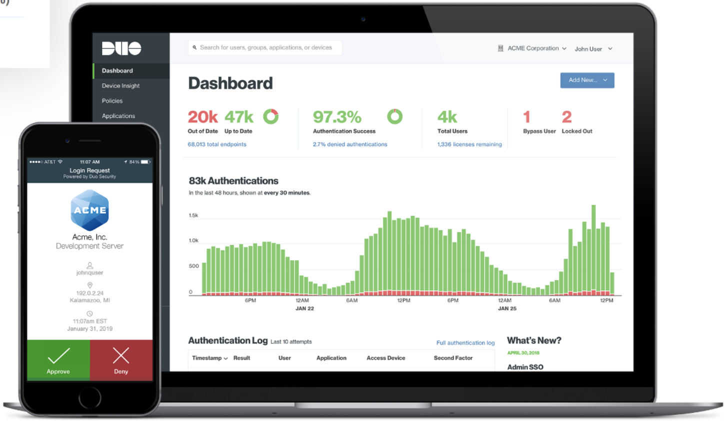
● End-of-Life	**0** (0%)
● Out-of-Date	**7** (14.3%)
● Up-to-Date	**42** (85.7%)

Access devices + 2FA devices using Duo Mobile



Trusted Endpoints (58)

● Trusted	**0** (0%)
● Not-Trusted	**7** (12.1%)
○ Unknown	**51** (87.9%)



Cisco Secure

New: Device Health Application [DHA]

Simple and Easy

Expanding on iOS/Android functionality

New: A light app for Mac and Win devices that checks the posture of the device at the time of access

10.1.2

OS patch level

Disk encryption

Device password

Firewall enabled

3rd party agents

New: Integration with AMP4E, Meraki and Microsoft

- AMP4E: Automatically block malware infected Macs and PCsTrust a device if it's managed

- New MDM Integrations:
  - Meraki and MS Intune
  - Expanding on current integrations with MobileIron, Vmware, JAMF, Landesk, Sophos, etc.
  - Radically easy for customers

AMP4E

CISCO Meraki

Microsoft Intune

Content Security
New refreshed solution and new members of the family

Cisco Email Security

Email Security

- Email Security Appliance (ESA)
- Cloud Email Security (CES)
- Security Management Appliance (SMA)

Cisco Registered Envelope Service (CRES)

- Email Security Plug-in & Add-in

Advanced Phishing Protection (APP)

Domain Protection (DMP)

New - Available Now

Cisco Security Awareness (CSA)

Coming Soon

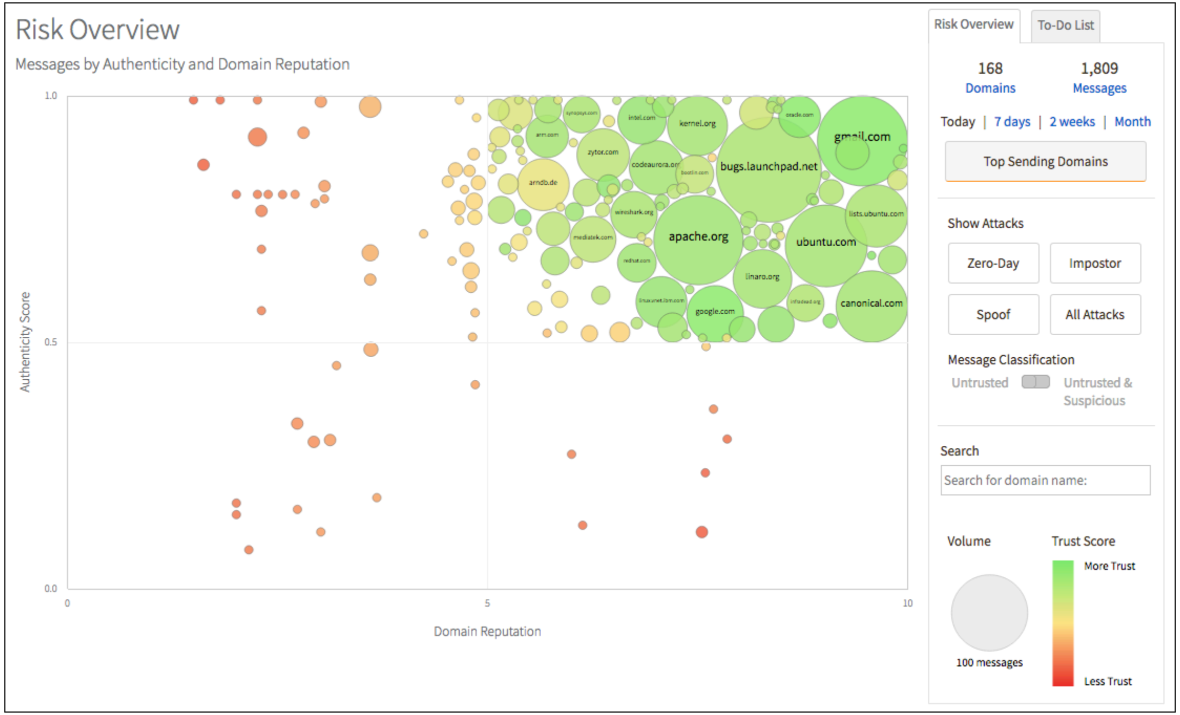
Cisco Mailbox Defense (Codename Raptor)

What’s new with Email Security

- Leverage Talos Cloud URL Analysis
  - adds more internal information and analysis techniques as well as 3rd part intelligence
- Updated Advanced Phishing & Domain Protection Integration
  - ESA is able to act as sensor and collects metadata for the APP cloud service
  - Reporting on SMA
- Search and Remediate
  - ESA admin can now remediate direct in O365 & on-prem Exchange
- SMA proxy support for CTR registrations
- SMA scalability supports now 40+ ESAs connecting to a single SMA

Advanced Phishing Protection

Analyze and manage untrusted, suspicious messages



Risk Overview

Messages by Authenticity and Domain Reputation

168 Domains

1,809 Messages

Show Attacks

Message Classification

Search

Superior Intelligence

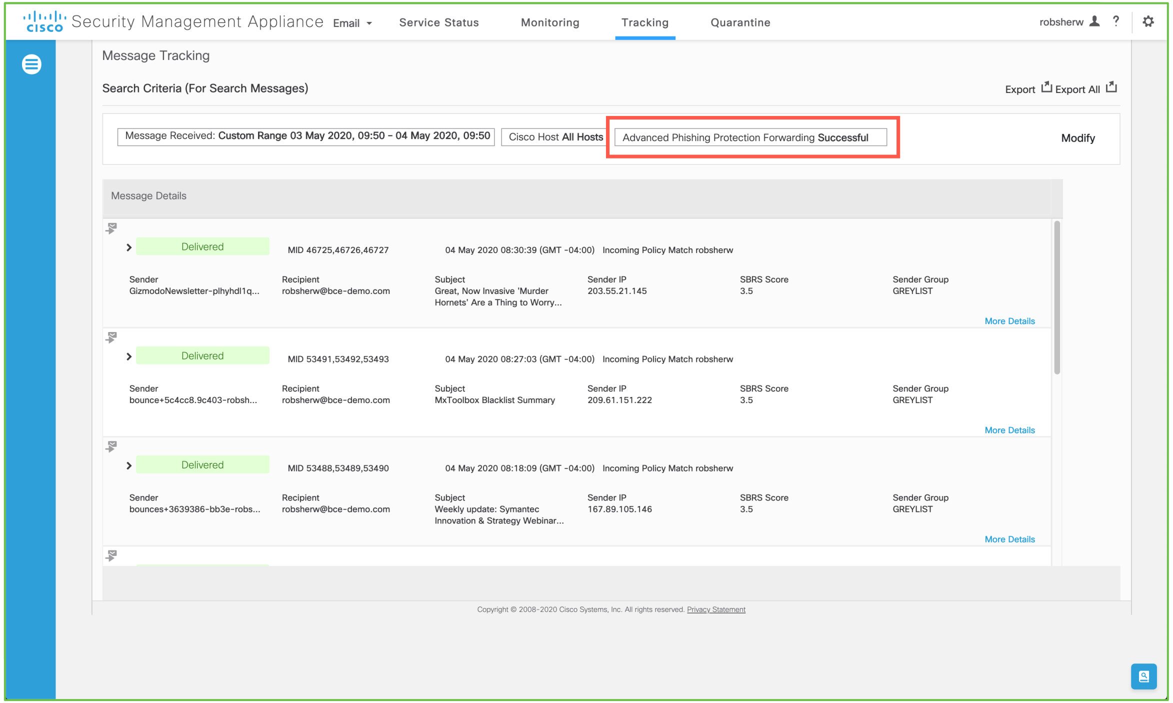
Learns and authenticates identities and behavioral relationships for enhanced protection

Protects against business email compromise and phishing attacks

Discerns which emails carry targeted phishing attacks and only legitimate emails get delivered

Advanced Phishing Protection

Analyze and manage untrusted, suspicious messages



Message Tracking

Search Criteria (For Search Messages)

Message Received: **Custom Range 03 May 2020, 09:50 – 04 May 2020, 09:50** | Cisco Host **All Hosts** | Advanced Phishing Protection Forwarding **Successful**

Message Details

Delivered MID 46725,46726,46727 04 May 2020 08:30:39 (GMT -04:00) Incoming Policy Match robsherw

Sender	Recipient	Subject	Sender IP	SBRS Score	Sender Group
GizmodoNewsletter-plhyhdl1q...	robsherw@bce-demo.com	Great, Now Invasive 'Murder Hornets' Are a Thing to Worry...	203.55.21.145	3.5	GREYLIST

More Details

Delivered MID 53491,53492,53493 04 May 2020 08:27:03 (GMT -04:00) Incoming Policy Match robsherw

Sender	Recipient	Subject	Sender IP	SBRS Score	Sender Group
bounce+5c4cc8.9c403-robsh...	robsherw@bce-demo.com	MxToolbox Blacklist Summary	209.61.151.222	3.5	GREYLIST

More Details

Delivered MID 53488,53489,53490 04 May 2020 08:18:09 (GMT -04:00) Incoming Policy Match robsherw

Sender	Recipient	Subject	Sender IP	SBRS Score	Sender Group
bounces+3639386-bb3e-robs...	robsherw@bce-demo.com	Weekly update: Symantec Innovation & Strategy Webinar...	167.89.105.146	3.5	GREYLIST

More Details

Copyright © 2008-2020 Cisco Systems, Inc. All rights reserved. Privacy Statement

Superior Intelligence

Learns and authenticates identities and behavioral relationships for enhanced protection

Protects against business email compromise and phishing attacks

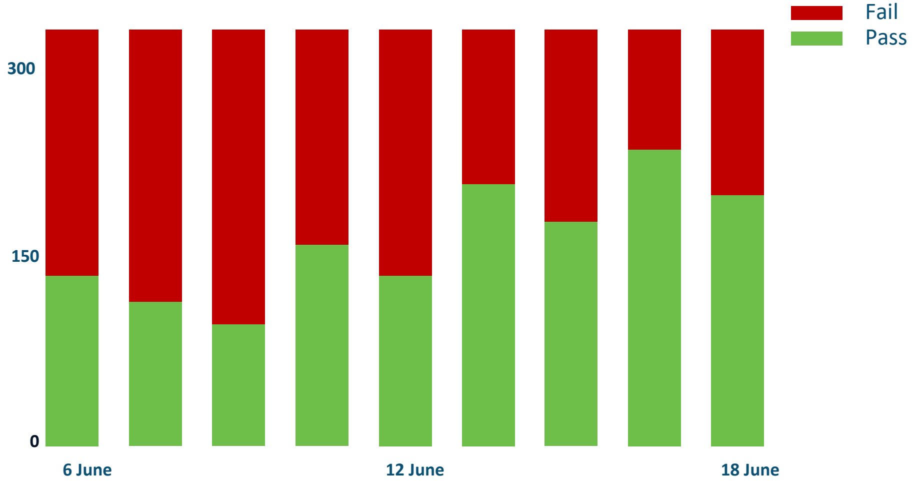
Discerns which emails carry targeted phishing attacks and only legitimate emails get delivered

cisco Secure

Cisco Domain Protection

- Protect Your Email Domain and Brand
- Manage your Email Authentication and internal and external Email senders

Identify unauthorized usage



Authenticate 3rd party email senders

Marketo

Volume: **32,078**

SPF Pass
100%

DKIM Pass
100%

salesforce

Volume: **4,047**

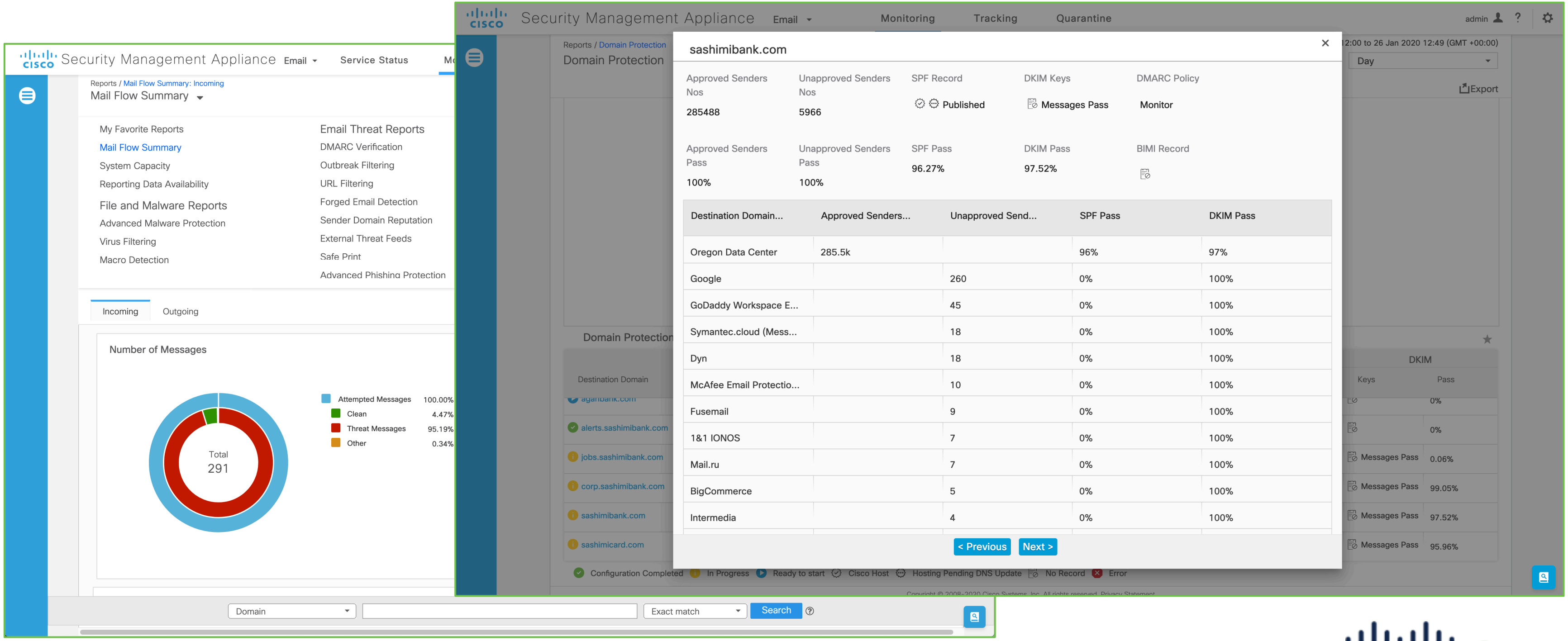
SPF Pass
100%

DKIM Pass
0.4%

cisco Secure

Cisco Domain Protection

- Protect Your Email Domain and Brand
- Manage your Email Authentication and internal and external Email senders



Attempted Messages	100.00%
Clean	4.47%
Threat Messages	95.19%
Other	0.34%

Destination Domain	DKIM Keys	DKIM Pass
aganbank.com		0%
alerts.sashimibank.com		0%
jobs.sashimibank.com	Messages Pass	0.06%
corp.sashimibank.com	Messages Pass	99.05%
sashimibank.com	Messages Pass	97.52%
sashimicard.com	Messages Pass	95.96%

Configuration Completed · In Progress · Ready to start · Cisco Host · Hosting Pending DNS Update · No Record · Error

sashimibank.com

Approved Senders Nos	Unapproved Senders Nos	SPF Record	DKIM Keys	DMARC Policy
285488	5966	Published	Messages Pass	Monitor

Approved Senders Pass	Unapproved Senders Pass	SPF Pass	DKIM Pass	BIMI Record
100%	100%	96.27%	97.52%	

Destination Domain...	Approved Senders...	Unapproved Send...	SPF Pass	DKIM Pass
Oregon Data Center	285.5k		96%	97%
Google		260	0%	100%
GoDaddy Workspace E...		45	0%	100%
Symantec.cloud (Mess...		18	0%	100%
Dyn		18	0%	100%
McAfee Email Protectio...		10	0%	100%
Fusemail		9	0%	100%
1&1 IONOS		7	0%	100%
Mail.ru		7	0%	100%
BigCommerce		5	0%	100%
Intermedia		4	0%	100%

< Previous · Next >

cisco Secure

Web Security Protection and Work from Home

Workforce

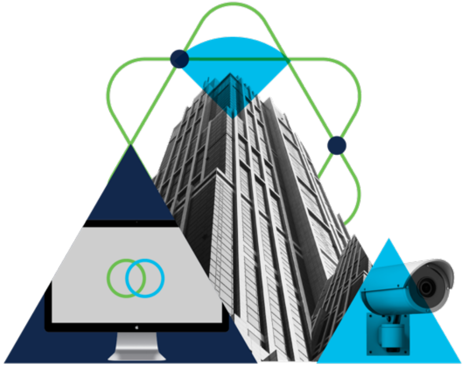
Ensure only the right users and secure devices can access right websites , Applications and protect data

Cisco ISE + WSA + DLP

Workloads

Secure all transactions with WSAv in AWS while using the same corporate IT security policies.

WSAv in AWS (Public Cloud)



Workplace

Secure all user and device connections across your network, with the help of AC,Cisco ISE and WSA.

Anyconnect + WSA + Cisco ISE

High Performance WSA – Phase 2

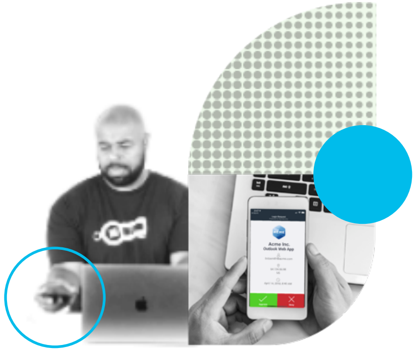
12.5

1.8x – 2x

Increase in performance

All Features supported

WTT, Time/Volume/ bandwidth-based quota now supported



Higher Connections

More Connections supported

Secured Ciphers

ECDSA Cipher used

cisco Secure

Defending 100% of Fortune 100 companies every day

Thank you