



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 AnyConnect

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

FY21 Security Priorities



SecureX

Platform Focus
SecOps (AMP, Email, TG)
EAs



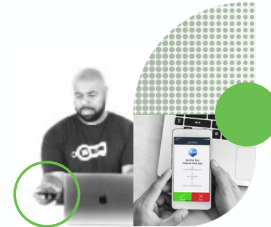
Cloud Transition

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



Cisco Security



Your infrastructure



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

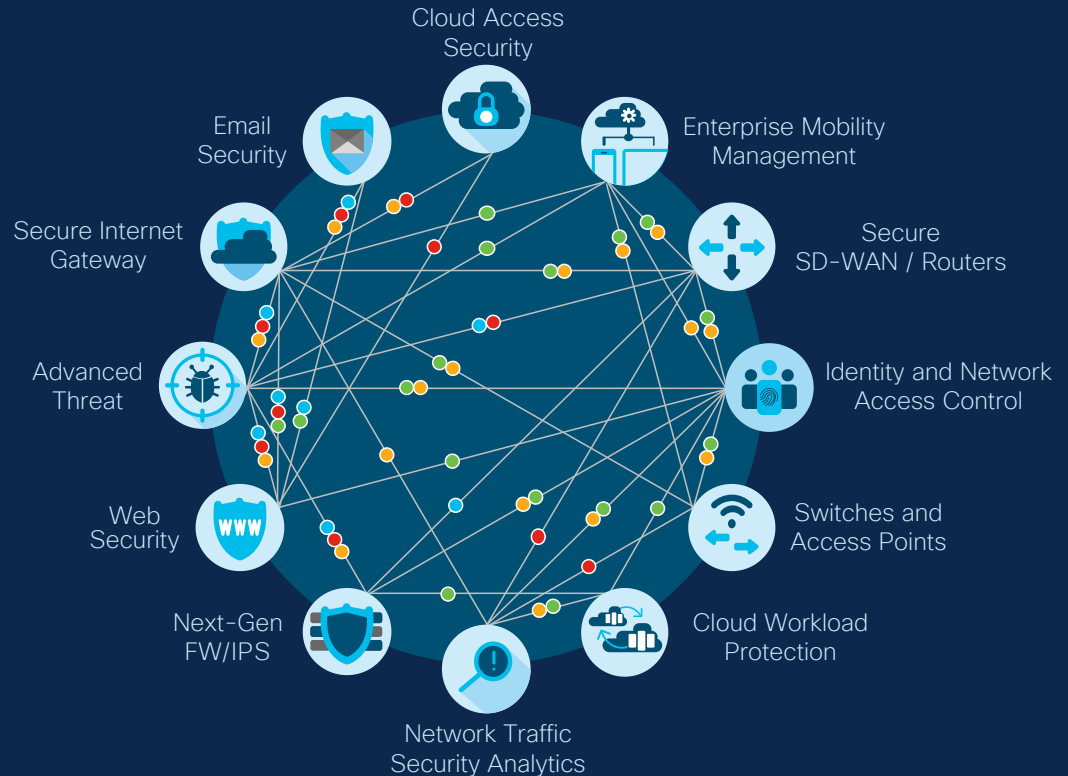
How Cisco Integrates Security

Threat Intel/Enforcement
Increased Threat Prevention

Event Visibility
Decreased Time to Detect

Context Awareness
Decreased Time to Investigate

Automated Policy
Decreased Time to Remediate



Dashboard

Customize

Applications

Integrations

My Applications

Amp AMP for Endpoints

Cdo Cisco Defense Orchestrator

Esa Email Security

Fp Firepower

O Orbital

Swc Stealthwatch Cloud

Tg Threat Grid

Tr Threat Response

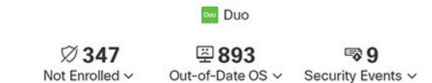
U Umbrella

Free Trials

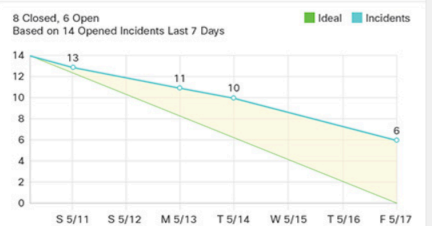
Swc Stealthwatch Enterprise

Wsa Web Security Appliance

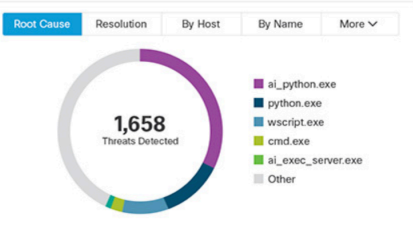
App Metrics Last 24 Hours



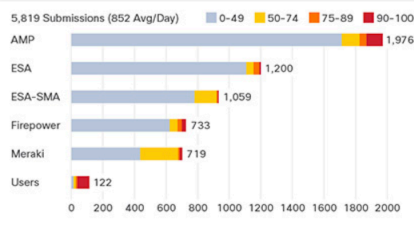
Threat Response Incident Burndown Last 7 Days



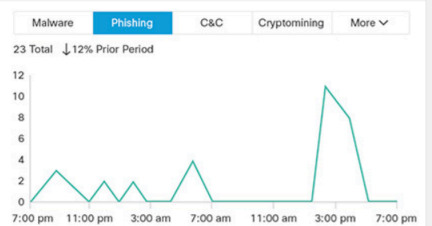
AMP for Endpoints Threats Last 7 Days



Threat Grid Submission Source Last 7 Days



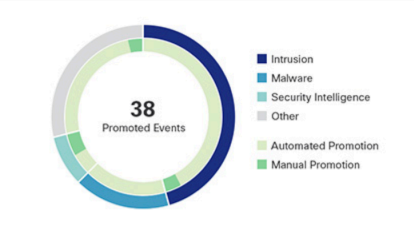
Umbrella Blocks by Security Category Last 24 Hours



Stealthwatch Cloud High Risk Countries Last 7 Days



Firepower Promoted Events Last 24 Hours



Activity

Potential Data Exfil Alert

Threat Hunt Incident

8.8 Talos Vuln Report

New Flagged App

InfoSec Trends

Out of Date Limit Hit

Incident Escalated

Orbital Query Incident

Out of Date Limit Hit

Incident Escalated

Orbital Query Incident

Orbital Query Incident

Orbital Query Incident



Search & Filter

Search

Category

- 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

Rating

- ★★★★★
- ★★★★☆
- ★★★☆☆
- ★★☆☆☆
- ★☆☆☆☆



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 policies 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](#)

Activity




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



Advanced Threat



The bridge to possible

© 2020 Cisco and/or its affiliates. All rights reserved.

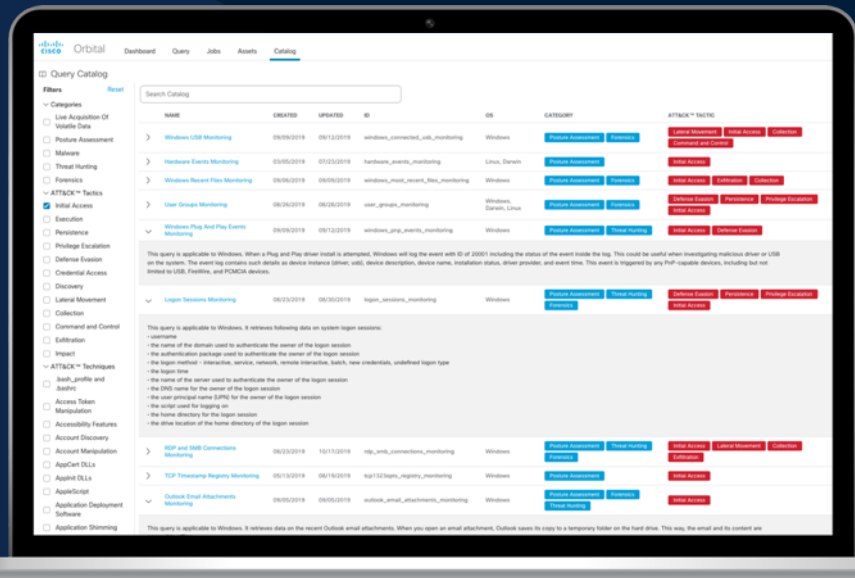




Relentless Breach Defense

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

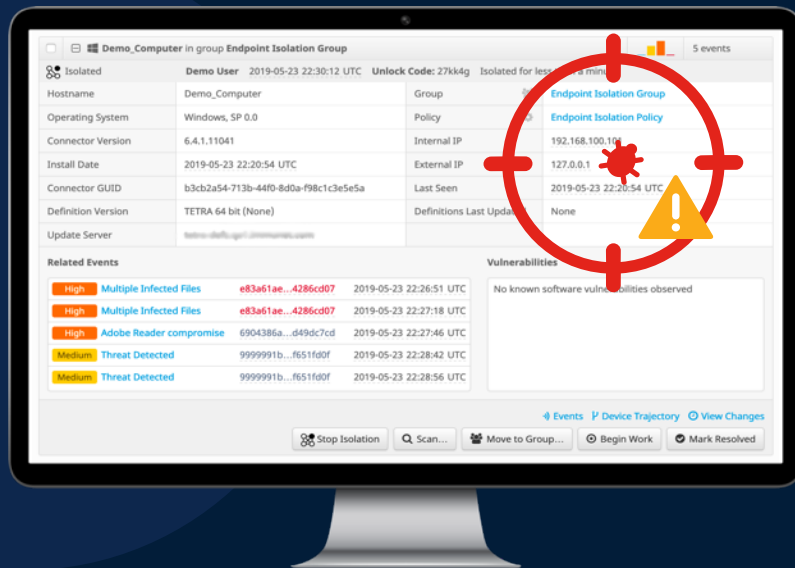




Relentless Breach Defense

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





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**

The screenshot shows a list of indicators on the left and a detailed view of the **OSX.Dok.ioc** indicator on the right. The detailed view includes the following information:

- Indicator Name:** OSX.Dok.ioc
- Category:** Command and Control
- 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
- Impact:** Critical
- Severities:** Medium, High, Low

The screenshot shows the **Indicators** page with a search bar and filters. The list of indicators includes:

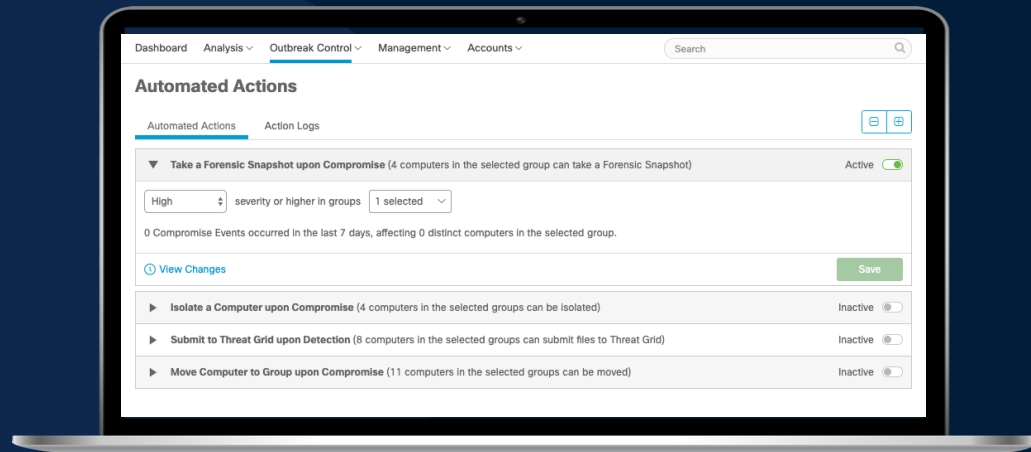
- Crossrider.ioc** (Impact: Medium)
- Dummy.ioc** (Execution Persistence: Medium)
- GateDotPhp.ioc** (Command and Control: High)
- JS.Trojan.Generic_48153.ioc** (Command and Control: Critical)
- Linux.AutostartPersistence.ioc** (Persistence: High)
- Linux.CurlDownloadExecute.ioc** (Defense Evasion: Medium)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



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



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



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

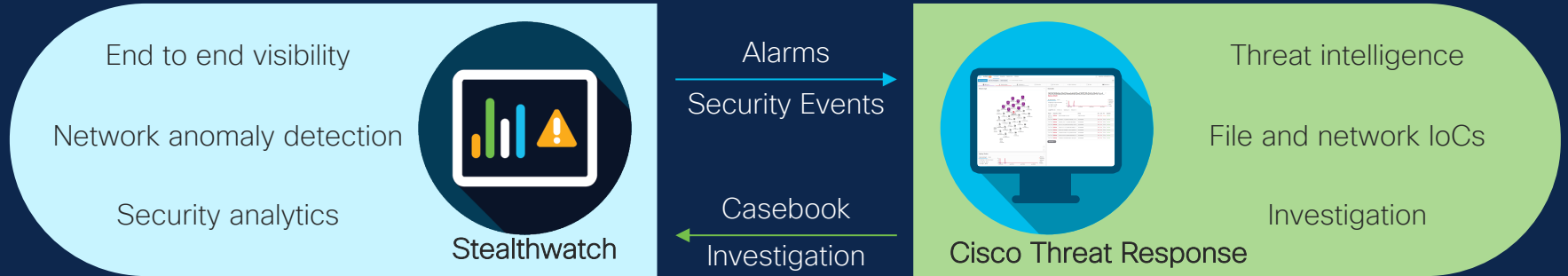


User Management

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

Integration with Cisco Threat Response

For accelerated investigation and remediation



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.

New Investigation Assign to Incident Snapshots ...

Automatic Layout

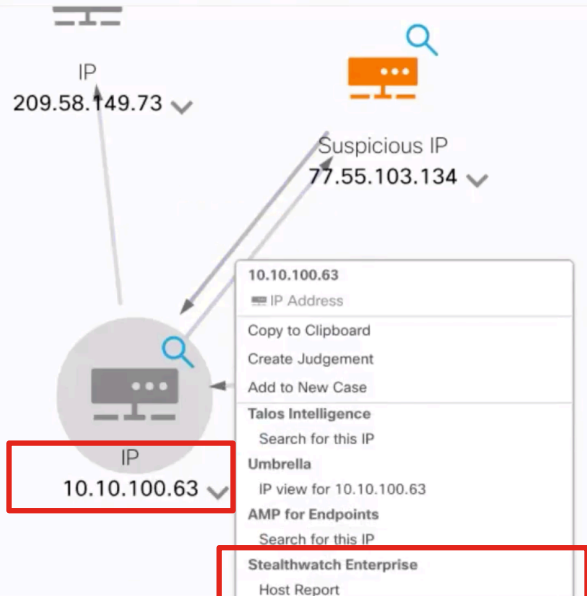
0 Targets 2 Observables 9 Indicators 0 Domains 0 File Hashes 2 IP Addresses 0 URLs 3 Modules

Investigation 2 of 2 enrichments complete with 5 Alerts

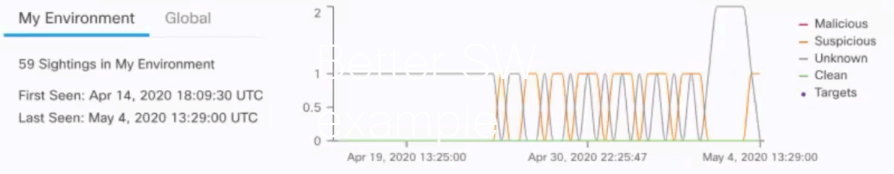
ip:"77.55.103.134"
ip:"10.10.100.63"

Investigate Clear Reset What can I search for?

Relations Graph Filters: Show All, Expanded Showing 4 nodes



Sightings



Observables List View

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

My Environment Global

26 Sightings in My Environment

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

May 4, 2020 13:29:00

— Malicious
— Suspicious
— Unknown
— Clean
• Targets

Judgements (1) Verdicts (1) Sightings (26) Indicators (10)

Observation	Reason	Source	Severity	Confidence
Malicious	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

Flows

History

Status:

Hostname: --

Host Groups: [End User Devices, Desktops, New York](#)

Location: RFC 1918

First Seen: 3/26/20 8:36 PM

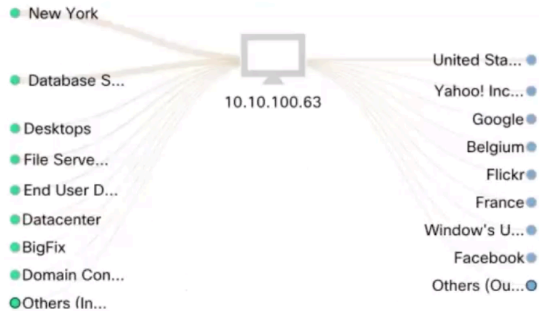
Last Seen: 5/4/20 8:08 PM

Policies: Client IP Policy, Inside

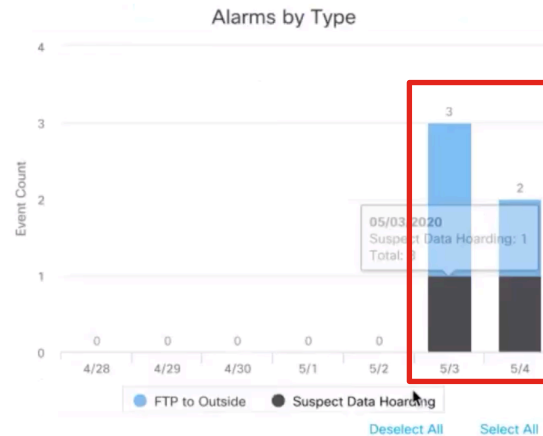
MAC Address: --

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

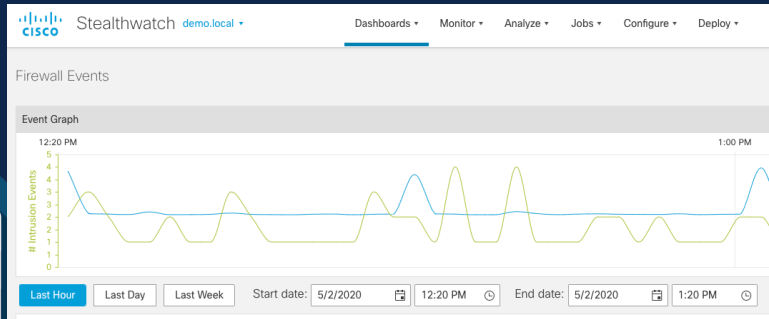
- SAL provides a single logging aggregation point for Cisco's Firewall fleet
- TLS Fingerprinting to improve detections



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

Firepower as a Sensor



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

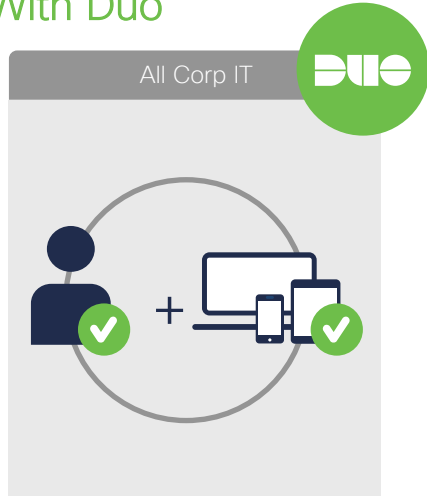
Security Analytics and Logging, SAL On-Prem

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



Cisco Zero Trust

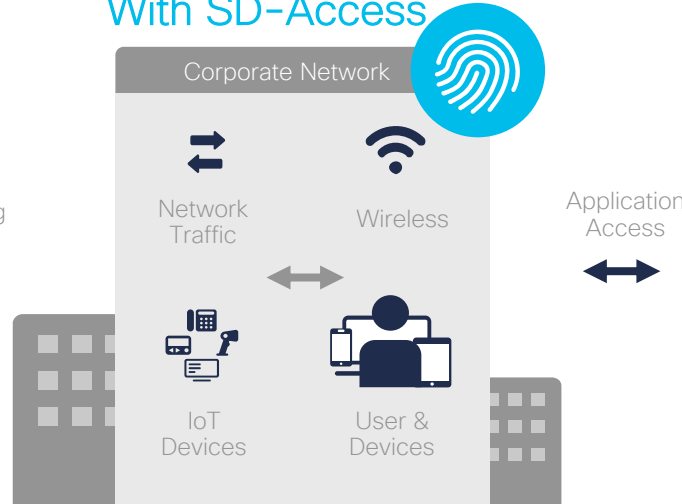
Secure the Workforce
With Duo



User-bound Device Access



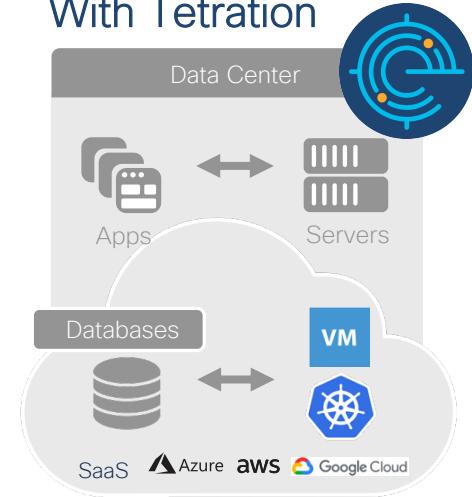
Secure the Workplace
With SD-Access



Network Access

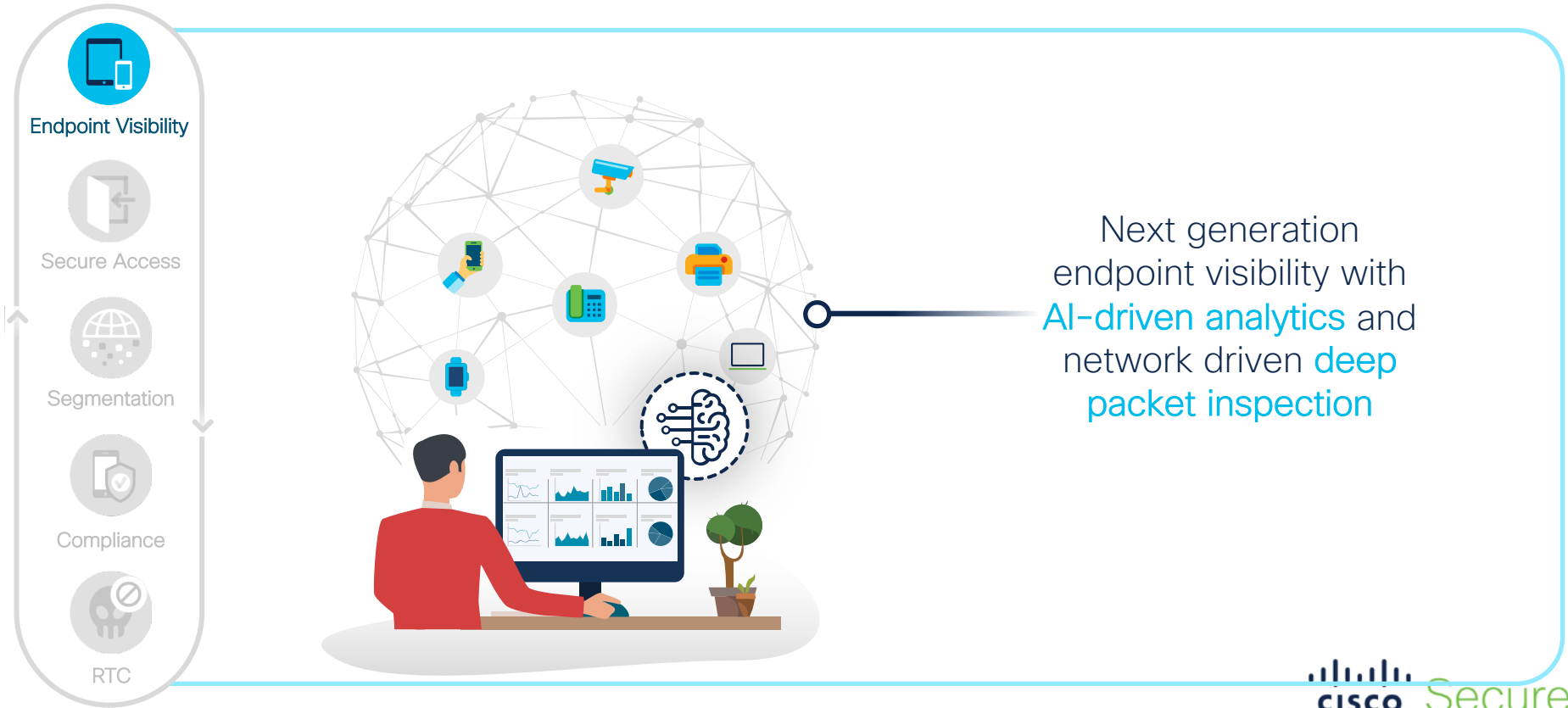


Secure Your Workloads
With Tetration



Workload Access

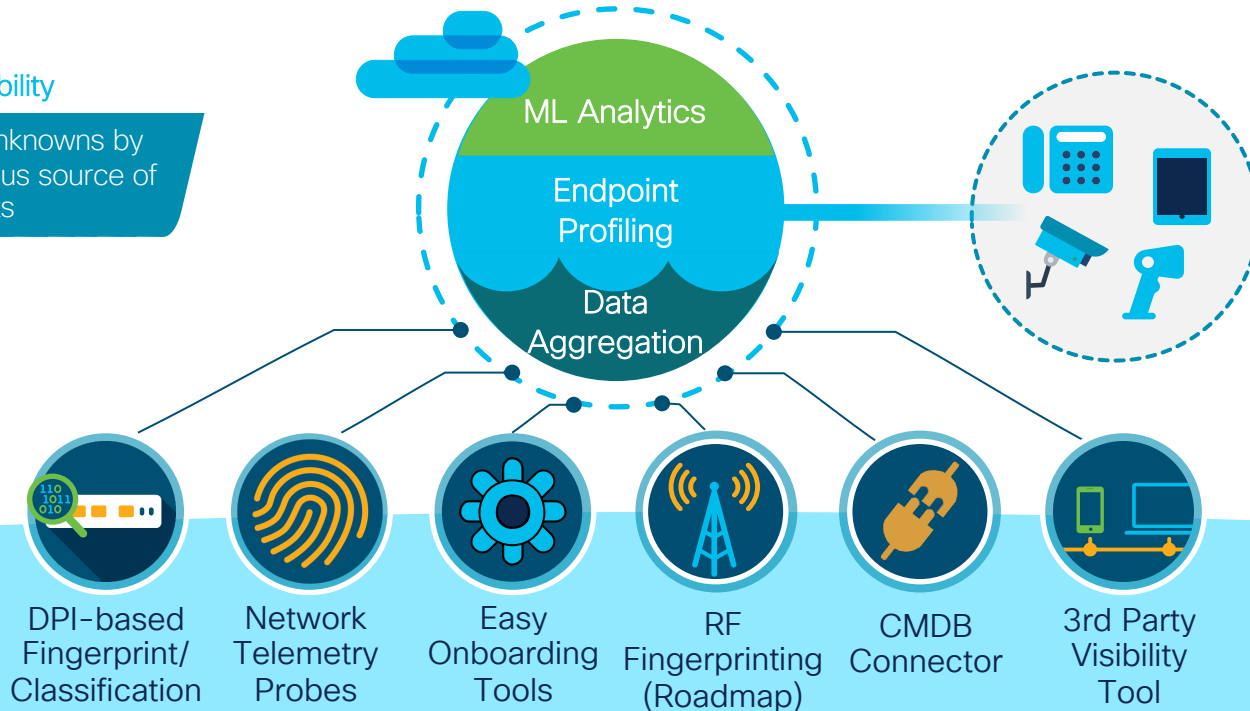
Next phase of Endpoint Visibility



Endpoint Analytics on Cisco DNA Center

High Fidelity Visibility

Rapidly reduce unknowns by aggregating various source of device fingerprints



DPI-based
Fingerprint/
Classification

Network
Telemetry
Probes

Easy
Onboarding
Tools

RF
Fingerprinting
(Roadmap)

CMDB
Connector

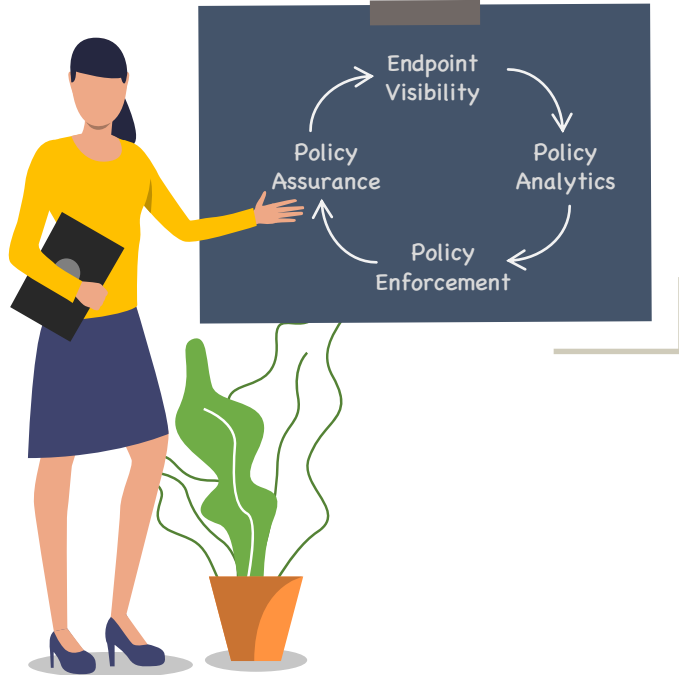
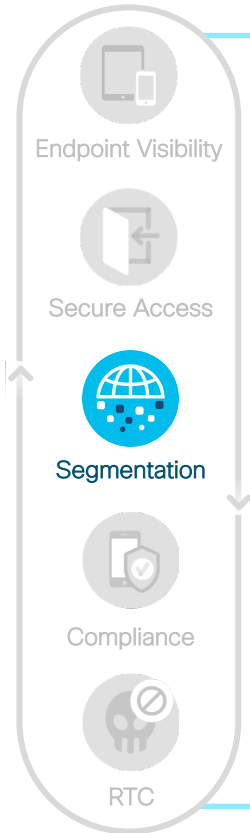
3rd Party
Visibility
Tool

Next phase of Secure Access



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.

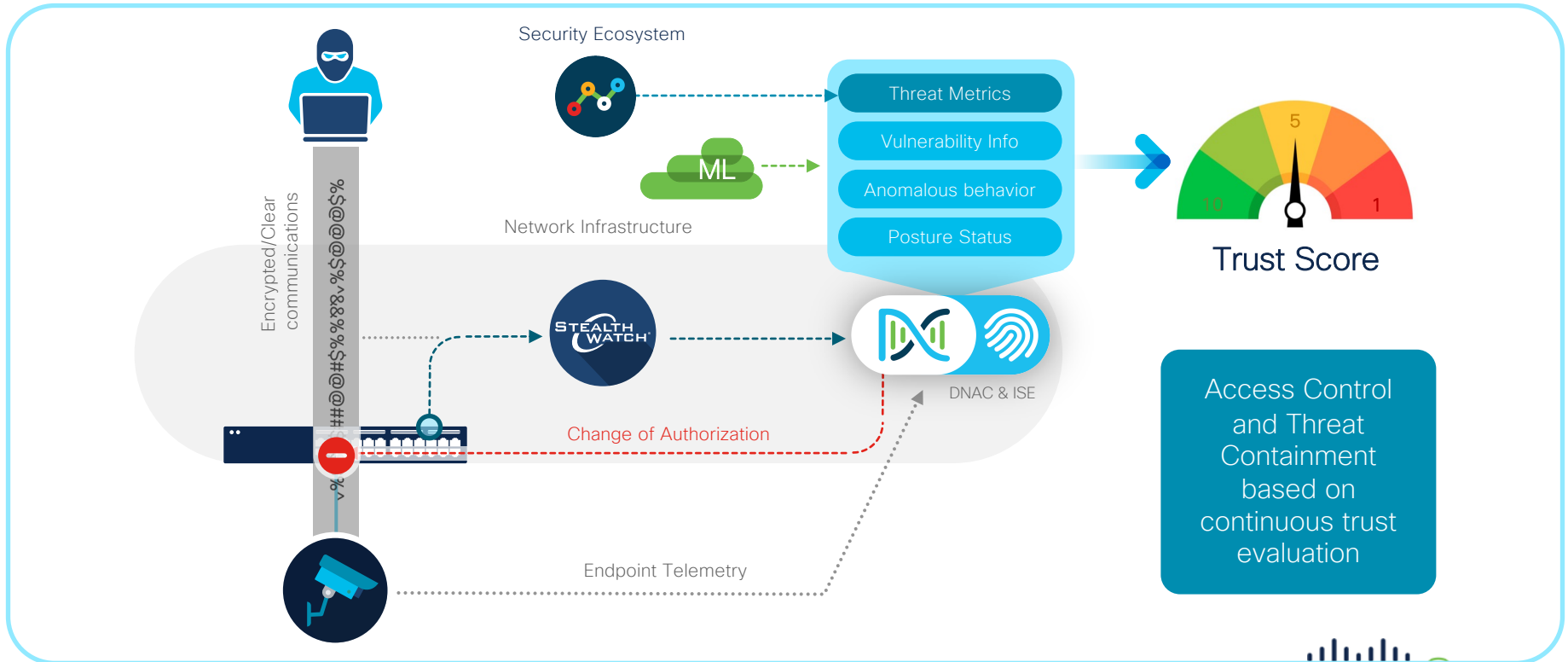
Next Phase of Segmentation



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

“Trust” based network access

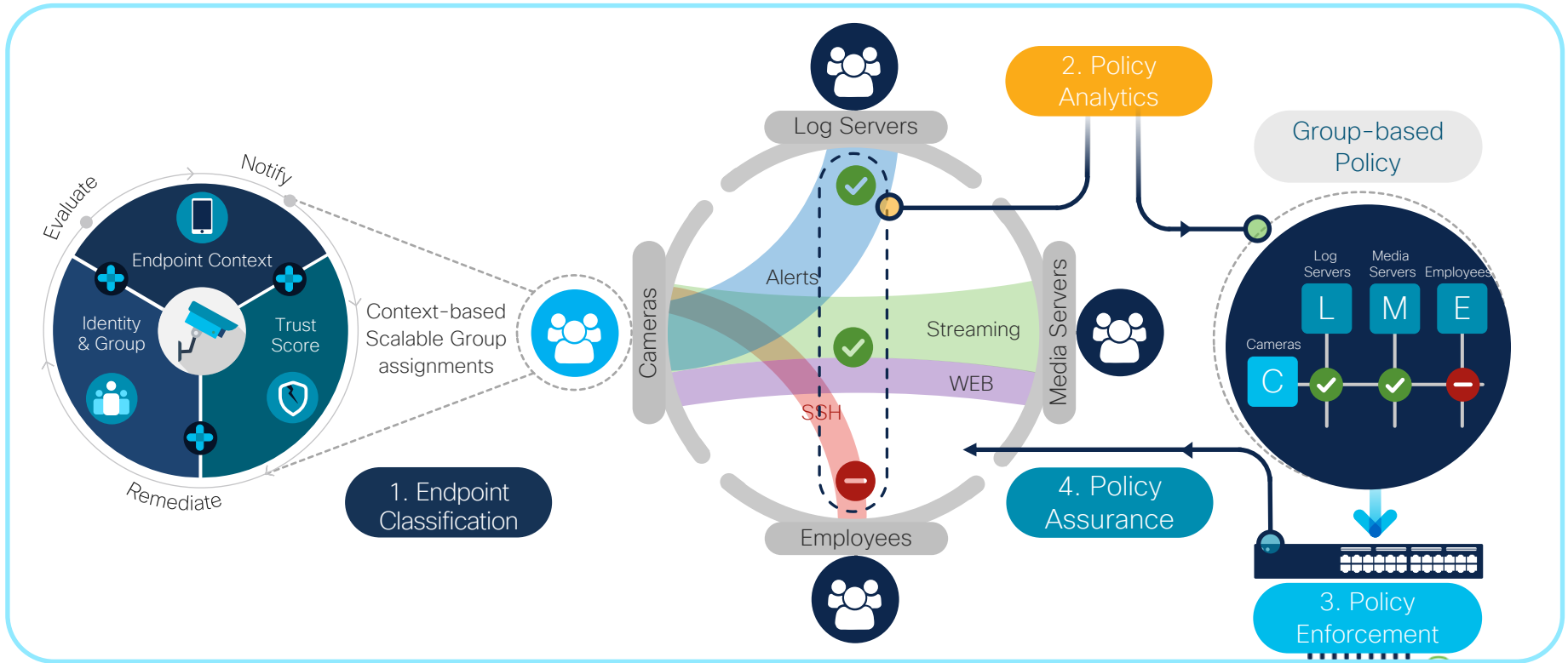
Bringing it all together



Trust Score using ML Anomaly detection for endpoint spoofing

Bring it all together

Visibility Driven Segmentation



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)

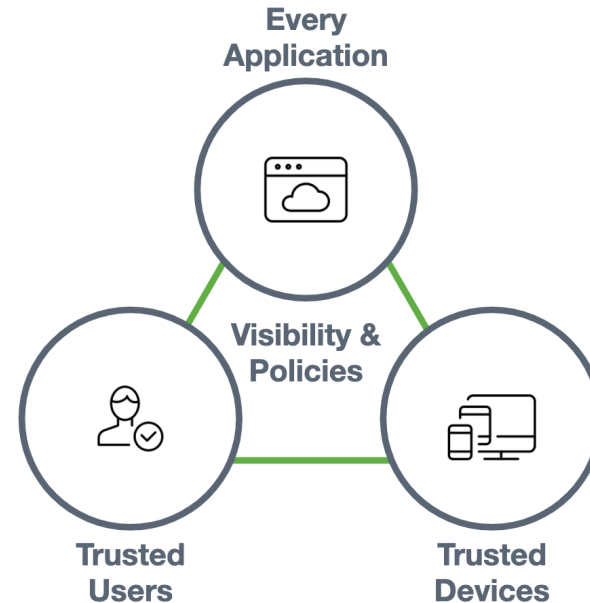


Somewhere you are
(e.g. location)

Worlds Easiest and Most Secure MFA



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



Gain Complete Visibility

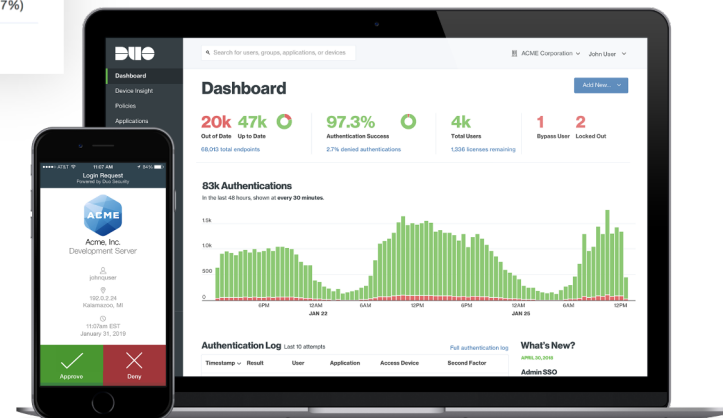
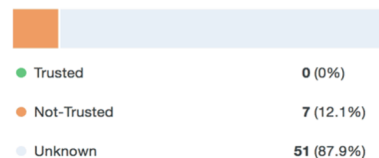
Device Health & Compliance



Operating Systems by Platform



Trusted Endpoints (58)



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



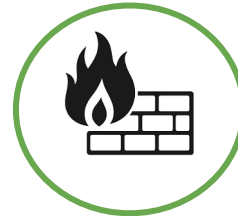
OS patch level



Disk encryption



Device password



Firewall enabled



3rd party agents

New: Integration with AMP4E, Meraki and Microsoft

- AMP4E: Automatically block malware infected Macs and PCs Trust 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



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



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

The screenshot displays the Cisco Security Management Appliance interface for Message Tracking. The top navigation bar includes 'Email', 'Service Status', 'Monitoring', 'Tracking' (selected), and 'Quarantine'. The user 'robshew' is logged in. The main content area shows search criteria for messages received between 03 May 2020, 09:50 and 04 May 2020, 09:50, filtered by 'Cisco Host: All Hosts'. A red box highlights the message status 'Advanced Phishing Protection Forwarding Successful'. Below this, three message details are listed, each with a 'Delivered' status and a 'More Details' link.

Message ID	Time	Policy Match
MID 46725,46726,46727	04 May 2020 08:30:39 (GMT -04:00)	Incoming Policy Match
MID 53491,53492,53493	04 May 2020 08:27:03 (GMT -04:00)	Incoming Policy Match
MID 53488,53489,53490	04 May 2020 08:18:09 (GMT -04:00)	Incoming Policy Match

Superior Intelligence

Learns and authenticates identities and behavioral relationships for enhanced protection

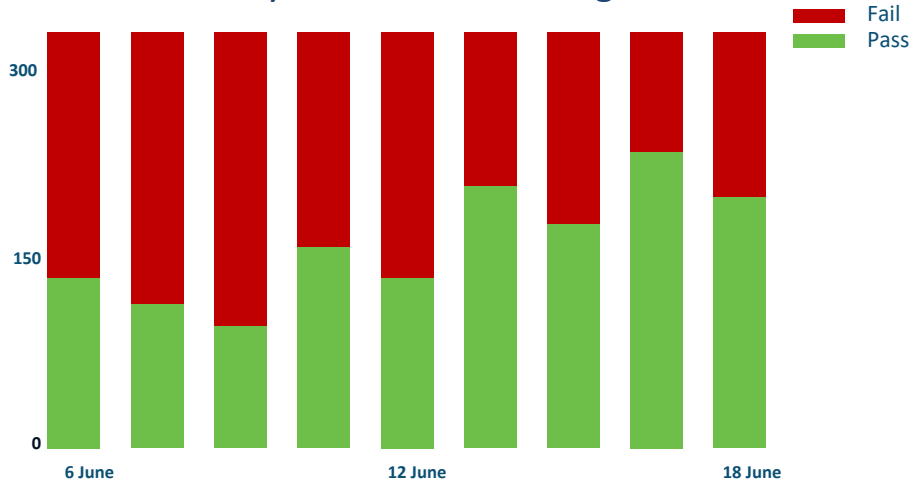
Protects against business email compromise and phishing attacks

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

Cisco Domain Protection

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

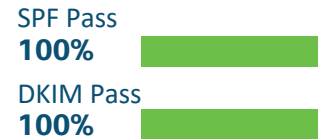
Identify unauthorized usage



Authenticate 3rd party email senders



Volume: **32,078**



Volume: **4,047**



Cisco Domain Protection

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

The screenshot displays the Cisco Security Management Appliance (SMA) interface. The main dashboard shows a 'Mail Flow Summary' for 'Incoming' mail, with a donut chart indicating the status of 291 total messages: 100.00% Attempted, 4.47% Clean, 95.19% Threat, and 0.34% Other. A sidebar lists various reports like 'Email Threat Reports', 'DMARC Verification', and 'Outbreak Filtering'. A modal window titled 'sashimbank.com' is open, showing domain protection details. It includes a summary table and a detailed table of destination domains.

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%
Mall.ru		7	0%	100%
BigCommerce		5	0%	100%
Intermedia		4	0%	100%

The modal window also shows summary statistics for sashimbank.com: Approved Senders (285488), Unapproved Senders (5966), SPF Record (Published), DKIM Keys (Messages Pass), and DMARC Policy (Monitor). A secondary table shows: Approved Senders Pass (100%), Unapproved Senders Pass (100%), SPF Pass (96.27%), DKIM Pass (97.52%), and BIM Record.

Web Security Protection and Work from Home



Workforce

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

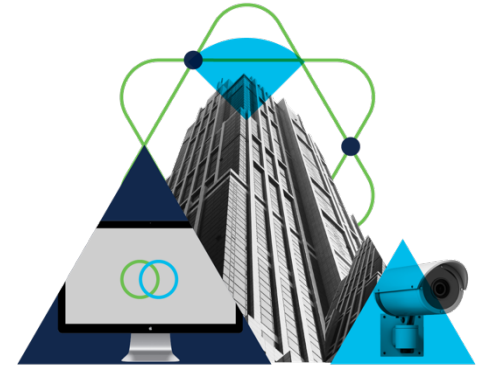
Cisco ISE + WSA + DLP



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

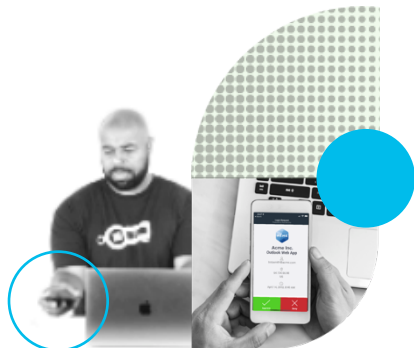
12.5



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



Defending 100% of Fortune 100
companies every day

Thank you

