

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

SSE, XDR, ZTNA, Hybrid Cloud:

How Cisco Secure Firewall continues to play a pivotal role

Anshul Kaushik - Technical Solutions Architect

Dinesh Moudgil - Technical Leader, Cloud and Network Security TME

BRKSEC-2706

CISCO *Live!*

#CiscoLiveAPJC

Abstract

Modern day application and network architectures have resulted in the need to re-invent how security is architected to protect the critical assets. Some of the examples of novel security approaches include SSE and XDR. All the same, the network remains the backbone connecting all the assets and hence, Cisco Secure Firewall (CSF) continues to be a key piece of the puzzle in securing the network and integrating with the other solutions.

This talk will outline the most common network and security architectures in detail and demonstrate the key capabilities and integrations with CSF. Basic knowledge of next generation firewall capabilities is preferred but not mandatory.

Agenda

- Customer Challenges
- Cisco Security Overview
- Addressing Challenges via
 - XDR
 - SSE
 - ZTNA
 - Hybrid Cloud
- Key Takeaways

Cisco Webex App

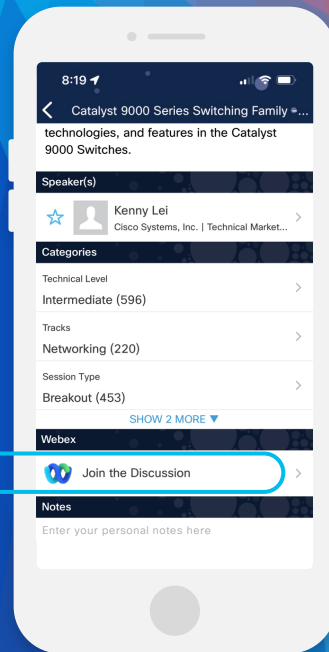
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2706>

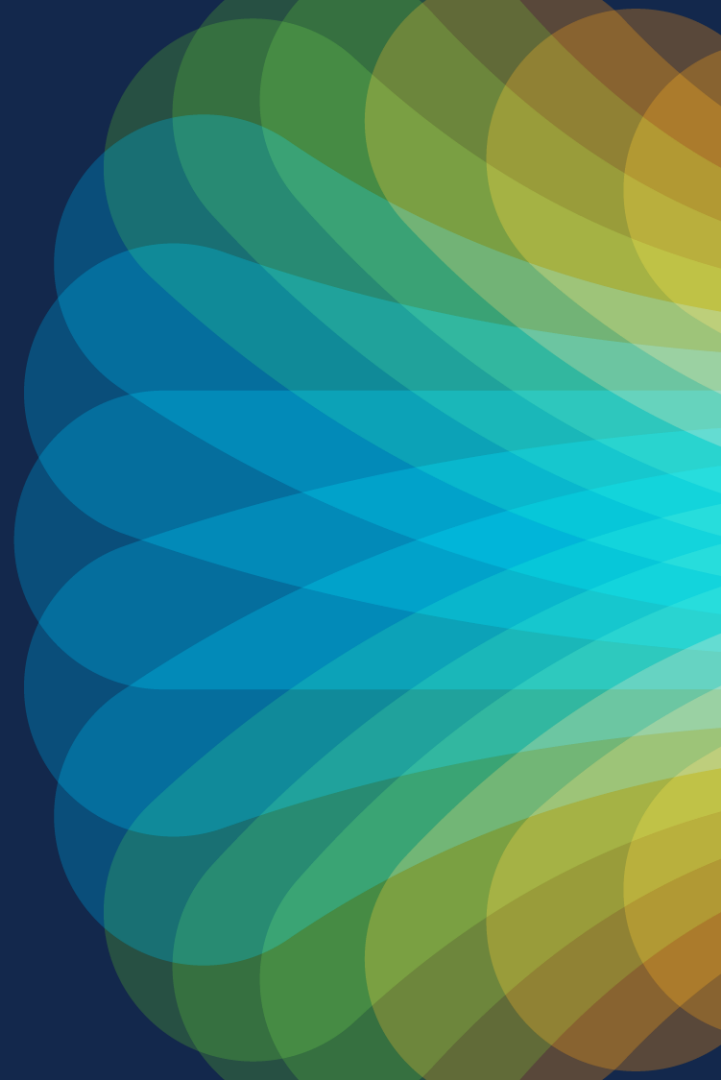
Your Speaker

Anshul Kaushik

- ankaushi@cisco.com
- CCIE Security #23790
- 20 Years in Industry, 18 with Cisco
- TAC – Presales – Channels
- Drive end to end Security Enablement
- Lives in Melbourne and like outdoors



Customer Challenges



Secure connectivity challenges are risky

Hybrid work is the norm

Transition to multi-cloud and SaaS



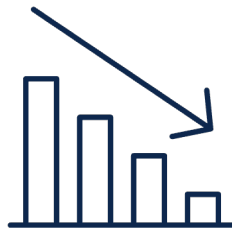


Customer Top Priorities



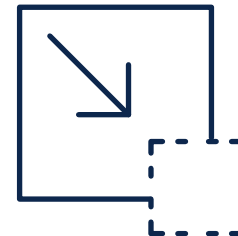
Boost Productivity

Empower users to
do their best work



Optimize Costs

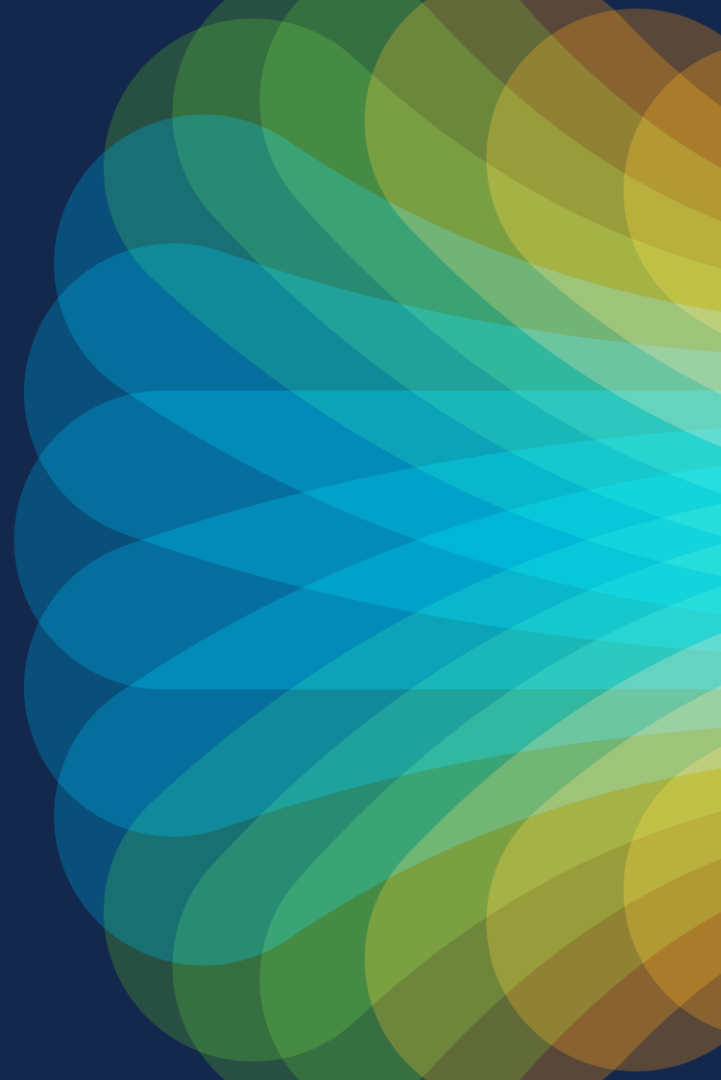
Address inefficiencies



Minimize Risk

Secure your organization

Cisco Security Overview



Security Ecosystem



Threat Centric
DNA & Cloud Security



Hybrid Security
+ Identity



SIG & AppSec



Cisco Secure

2014-16

2016-18

2018-20

2021-22

Next

M&A +
Organic

SOURCEfire
OpenDNS
Lancopé

observable
networks
Cisco Tetration
DUO
SECURITY

Secure Internet Gateway
Sentryo
SecureX

portshift **KENNA**
Security
PAN OPTICA **VALTIX**

OORT
Armorblox

Invest.

esentire **elastic** **VERODIN**
OpenDNS **FLASHPOINT** **SKYPORT**
HYTRUST **illusive** **SYSTEMS**

SKYPORT **exabeam**
SYSTEMS **THREATQ**
illusive **panaseer** **BehavioSec**

NS1
SECURE CODE **ISOVALENT**
WARRIOR

RANGEFORCE **securiti**
SAFEGUARD **styra**
CYBER **JupiterOne**

CISCO Live!

Cisco Security Cloud

Cisco Breach Protection

Extended Detection & Response

Ransomware Recovery

Cisco User Protection

Posture & Auth Management

Endpoint Security

Email Security

Experience Insights

Remote Browser Isolation

Security Service Edge

Cisco Cloud Protection

Workload Security

Application Security

Vulnerability Management

Attack Surface Management

Multicloud Defense

← FIREWALL PROTECTION →

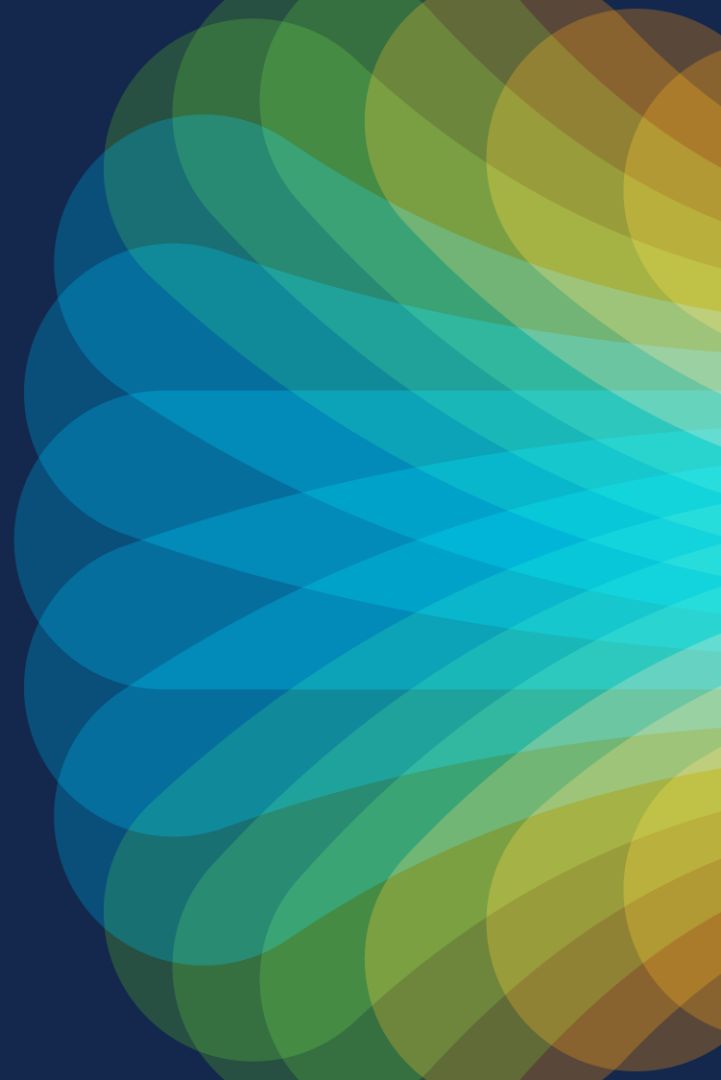
Challenges in Secure Connectivity

- Nature of changing Threat and limited visibility and context
- Significant challenges in dealing with policy complexity and multicloud infrastructure.
- Limited flexibility and efficiency of secure connectivity to private applications
- Need high throughput connectivity between users and applications
- Inadequate security while accessing cloud and on-prem applications

Addressing the challenges

- XDR
- SSE
- ZTNA
- Hybrid Cloud

Extended detection and response (XDR)



Definition of Extended Detection and Response (XDR)

Collection of telemetry from multiple security tools

Application of analytics to the collected and homogenized data to arrive at a detection of maliciousness

Response and remediation of that maliciousness

IDC #US49731922 (September 2022)
Source: Future Enterprise Resiliency & Spending Survey - Wave 7, IDC, August 2022, n = 241; December 2021, n = 361

An XDR is as good as its outcomes

Cisco XDR Outcomes

Where are we **most exposed** to risk? How good are we at detecting attacks **early**?

1 Detect Sooner

How quickly are we able to understand the **full scope** and **entry vectors** of attacks?

Prioritize by Impact

2

Are we **prioritizing the attacks** that represent the largest **material impacts** to our business? How fast can we **confidently respond**?

3 Reduce Investigation Time

Do we have **full visibility** into all our devices? Can we **reliably identify** a device and who uses it?

Accelerate Response

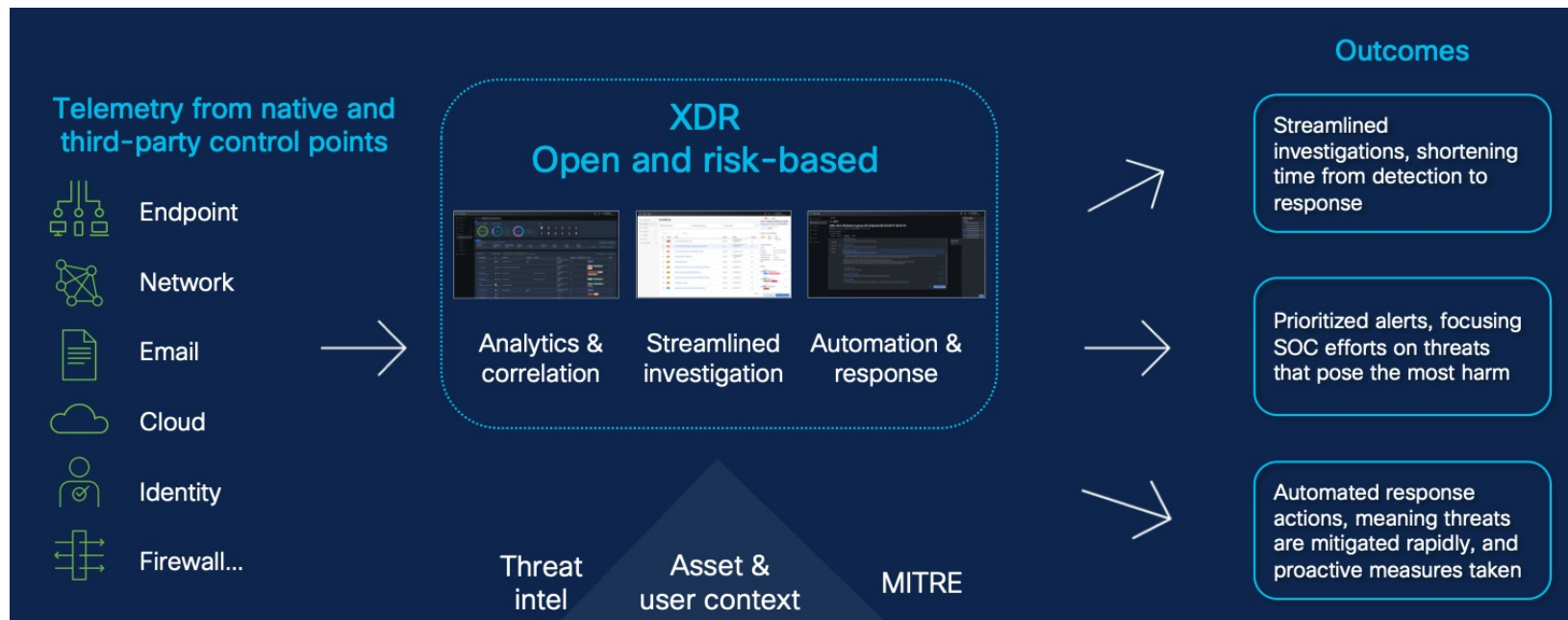
4

How much can SecOps **automate**?

5 Extend Device Context

Are we **improving** our time to respond?

What does an effective XDR looks like



Simplify security operations to elevate productivity and stay resilient against the most sophisticated threats

Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure

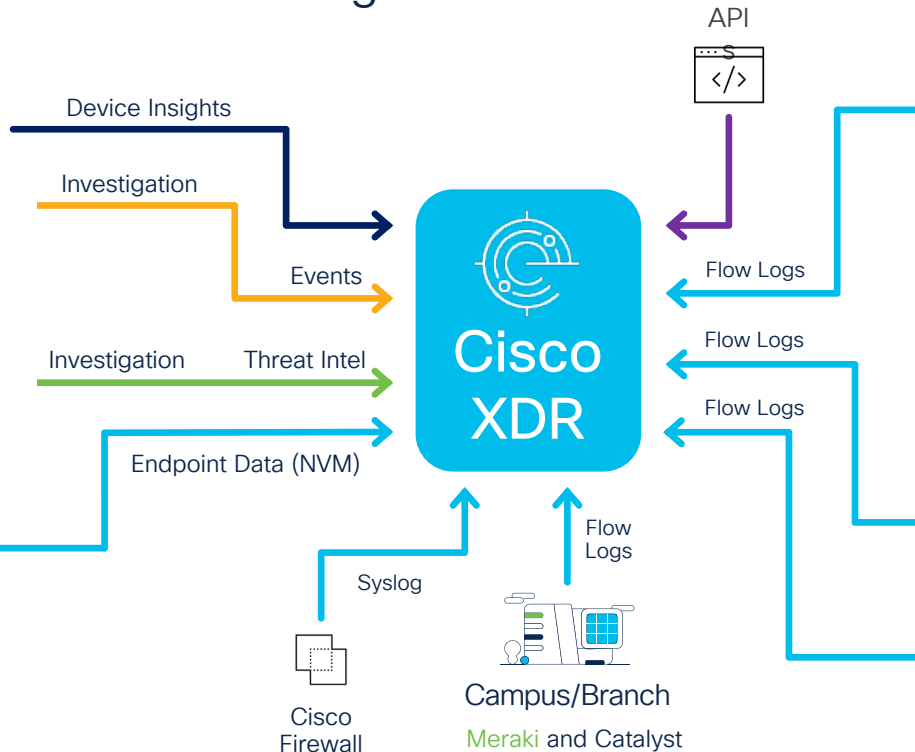
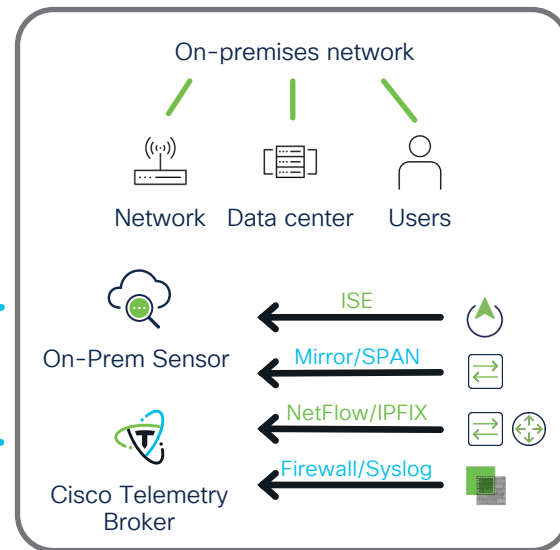
Integrations



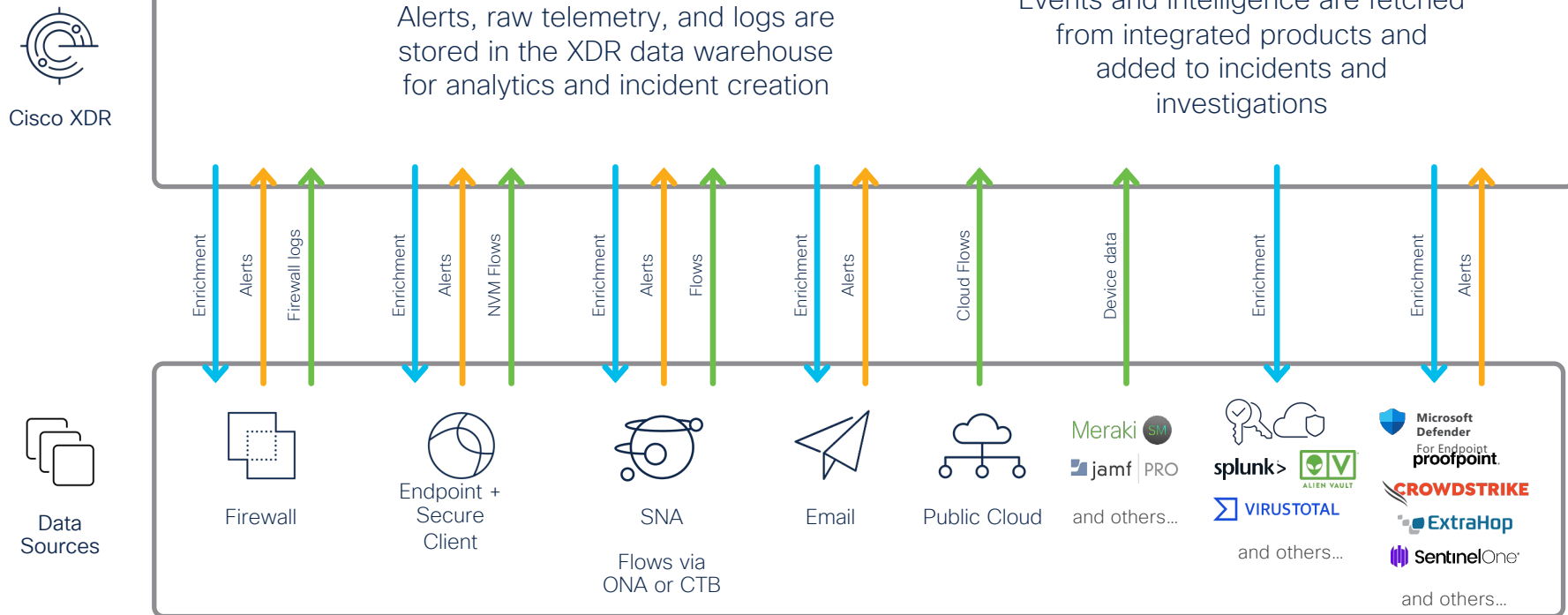
Intelligence



Remote Workers



Telemetry and enrichment



Telemetry and enrichment

Native Cisco

User / Endpoint:

- Secure Endpoint
- Secure Client
- Email Threat Defense
- Cisco Orbital

Network:

- Secure Network Analytics
- Secure Firewall
- Meraki
- Identity Services Engine
- Defense Orchestrator

Cloud:

- Umbrella
- Secure Cloud Insights

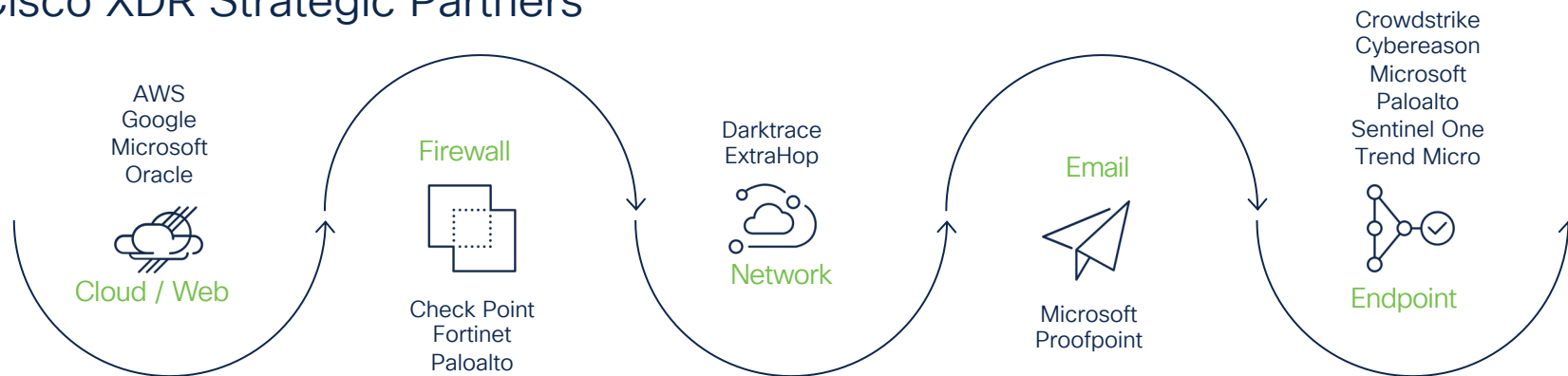
Application and Identity:

- Duo Security

Malware Analysis:

- Secure Malware Analytics

Cisco XDR Strategic Partners

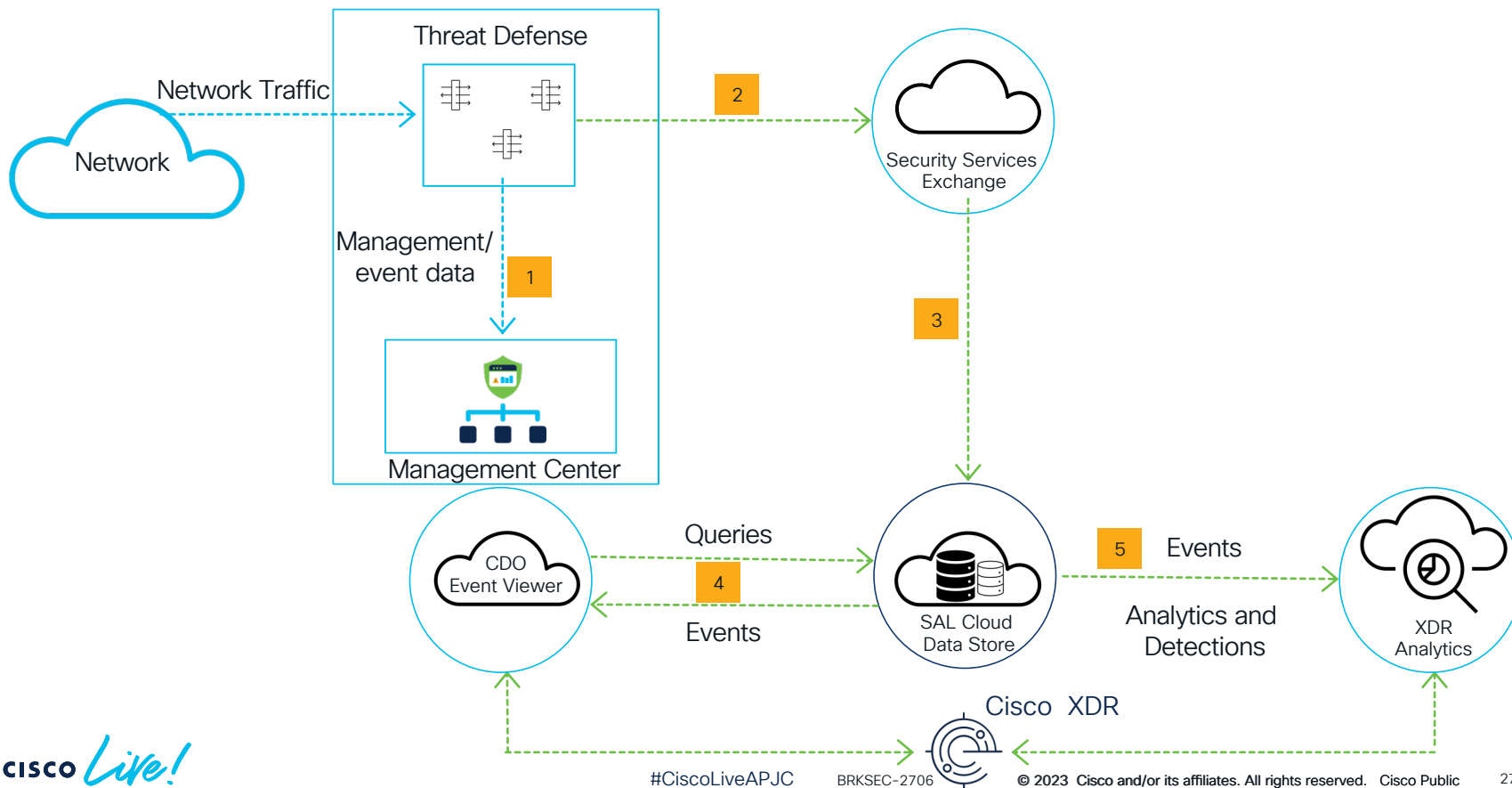


XDR Analytics detection and incident creation path



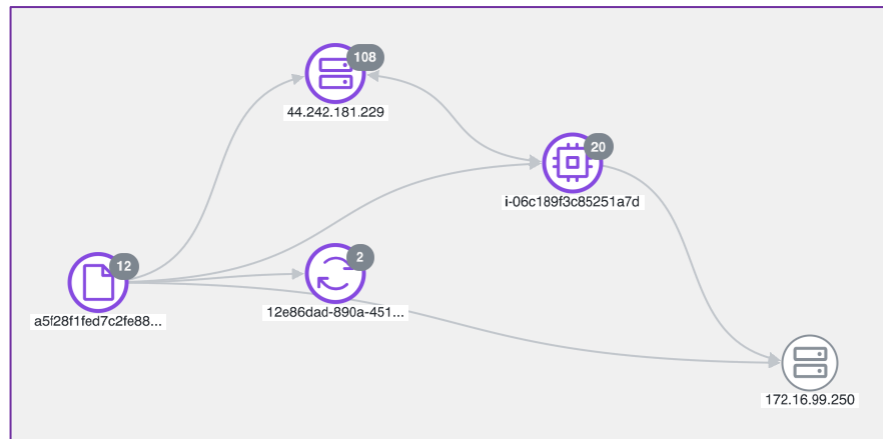
XDR Analytics covers end-to-end from raw telemetry to correlated, prioritized incidents which are enriched with context

Eventing High Level Flow



Reduce investigation time

- Interactive, visual representations of incidents
- Event correlation and incident chaining to group related intelligence
- Automated enrichment for the most critical incidents, ensuring intelligence is gathered immediately



Distinct Alert Types / MITRE Tactic		Zoom	1d	3d	8m	YTD	1y	All	15-May-2023	→	24-May-2023
										2023	
										May	
Internal Port Scanner	#11916	Discovery	Created: 2023-05-15 11:19 EDT								
Potential Data Exfiltration	#11917	Exfiltration	Created: 2023-05-16 08:31 EDT								
Outbound SMB Connection Spike	#11920	Reconnaissance	Created: 2023-05-17 16:50 EDT								
DNS Abuse	#11918	Exfiltration	Created: 2023-05-17 17:02 EDT								
New Unusual DNS Resolver	#11919	Command And Control	Created: 2023-05-18 12:48 EDT								
Outbound Traffic Spike	#11921	Exfiltration	Created: 2023-05-19 17:37 EDT								
Country Set Deviation	#11922	Initial Access	Created: 2023-05-22 09:55 EDT								
Malicious Process Detected	#11924	Execution	Created: 2023-05-22 17:55 EDT								
Suspicious Process Path	#11925	Defense Evasion	Created: 2023-05-22 18:01 EDT								
LDAP Connection from Suspicious Process	#11926	Credential Access	Created: 2023-05-22 18:32 EDT								
Suspected Malicious URL	#11923	Initial Access	Created: 2023-05-23 12:34 EDT								
Suspected Cryptocurrency Activity	#11927	Impact	Created: 2023-05-24 23:25 EDT								

Configure the integration

- 1 Enable XDR
- 2 Enable XDR Automate
- 3 Select a user role for XDR workflows
- 4 Save the configuration

The screenshot shows the 'SecureX Setup' page in the Firewall Management Center. The page has a navigation bar with 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Integration' tab is selected, and the 'SecureX' sub-tab is active. The page title is 'SecureX Setup'. Below the title, a description states: 'This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon. [Learn more](#)'. The setup is divided into four numbered steps:

- 1 Cloud Region**: This setting determines where events are sent, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools. The 'Current Region' is set to 'us-east-1 (US Region)'.
- 2 SecureX Enablement**: After completing this configuration, the SecureX ribbon will show up at the bottom of each page. [Learn more](#). A green box indicates 'SecureX is enabled for US Region.' A blue button labeled 'Disable SecureX' is visible.
- 3 Event Configuration**: This section has checkboxes for 'Send events to the cloud' (checked), 'Intrusion events' (checked), 'File and malware events' (checked), and 'Connection Events' (checked). Below these are radio buttons for 'Security' and 'All' (selected). A tooltip for the 'All' option says: 'View your [Cisco Cloud configuration](#). View your [Events in SecureX](#)'.
- 4 Orchestration**: Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#). A checkbox for 'Enable SecureX Orchestration' is checked. Below this, a text field 'Assigned Role' has 'Administrator' selected from a dropdown menu.

At the bottom right, there is a blue 'Save' button. Green arrows and numbers 1, 2, 3, and 4 are overlaid on the screenshot to correspond with the steps in the list on the left.

Configure the integration

ADD INTEGRATION

**Secure Email Threat Defense**
Formerly Secure Email Cloud Mailbox

Cisco Secure Email Threat Defense (formerly Secure Email Cloud Mailbox) provides the most comprehensive protection against damaging and...

 **+ Enable**

**Secure Email and Web Manager**
Formerly SMA Email

Cisco Secure Email and Web Manager (formerly SMA Email) centralizes management and reporting functions across multiple Cisco email and web...

 **+**

**Secure Firewall**
Formerly Firepower

Secure Firewall (formerly Firepower) provides complete and unified management for firewall application control, intrusion prevention, URL filtering...

 **+**

**Secure Malware Analytics**
Formerly Threat Grid

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect...

 **+**

Module Name

/all

Manage Devices **Check for New Devices**

	Version	Status	Description	IP Address
	7.2.0	Registered	10.90.12.219 atl-tme-fmc	10.90.12.219
	7.2.3	Registered	10.90.12.236 atl-tme-fmc-log.cisco.com	10.90.12.236
100-1	7.2.0	Registered	10.90.12.210 atl-tme-fp4100-1 (FMC managed)	10.90.12.210
100-2	7.2.0	Registered	10.90.12.220 atl-tme-fp4100-2 (FMC managed)	10.90.12.220
-log	7.2.3	Registered	10.90.12.237 atl-tme-ftd-log (FMC managed)	10.90.12.237

5 per page 1-5 of 5 << < 1 / 1 > >>

Dashboard

Dashboard of the tiles associated with this integration module, which can be shared by members of your organization.

Save

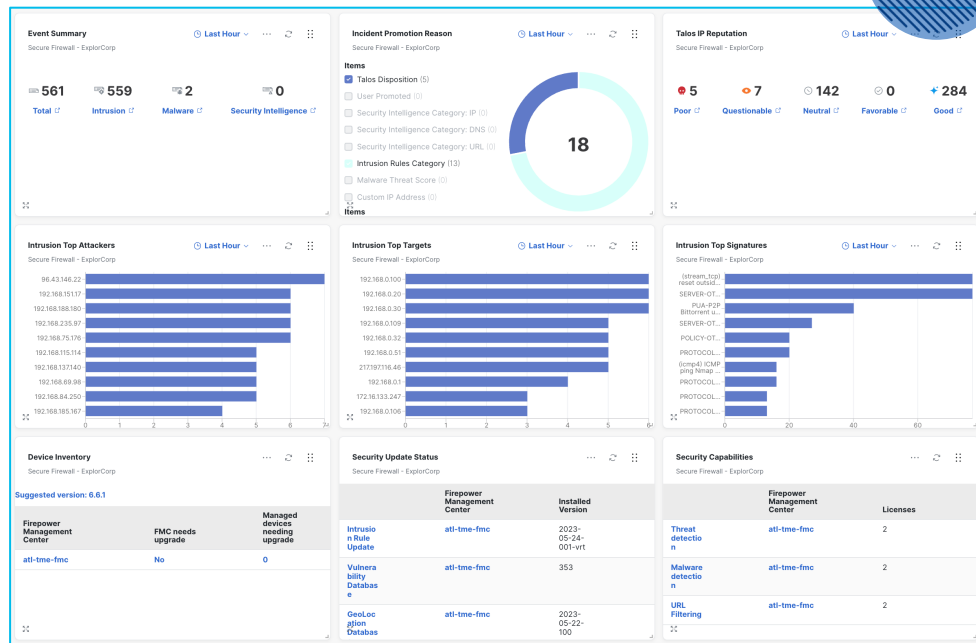
1 Add Firewall module

2 Save the module

Secure Firewall

Dashboard tiles

- Raw event summary
- Incident promotion reason
- Talos IP reputation
- Intrusion top attackers
- Intrusion top targets
- Intrusion top signatures
- Security Capabilities (FMC)
- Security Update Status (FMC)
- Device Inventory(FMC)



Secure Firewall

Enrichment

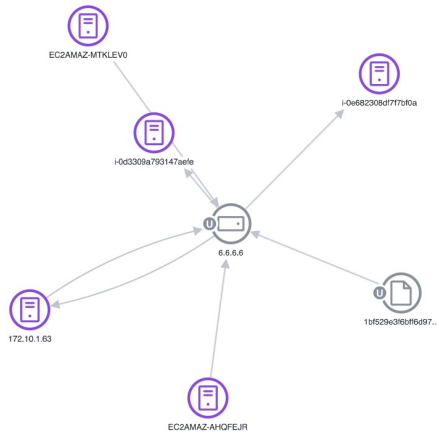
- Local IP sightings

Reference

- Pivot point to raw event

Promote events

- Promote alerts from Analytics to incidents in XDR



```
graph TD; EC2AMAZ-MTKLEVO --> 6.6.6.6; 10c330ba793147a0e --> 6.6.6.6; 10c682308d777f30a --> 6.6.6.6; 172.10.1.63 --> 6.6.6.6; 1b529e3f6f697... --> 6.6.6.6; EC2AMAZ-AHQFJR --> 6.6.6.6;
```

Security Intelligence event - IP_ReputationSI_Category:...

First Seen: 2023-04-17T13:10:36.000Z

High

Reported by

Module: Secure Firewall - ExplorCorp
Source: NGFW Event Service

Short description

Security Intelligence event - IP_ReputationSI_Category

Long description

Sighting Title
Security Intelligence event - IP_ReputationSI_Category:ExplorCorp_Malicious_IPs: cd8cce4a-c4c7-4b84-a9a5-5da22fc6f686

Secure Firewall

Incident Response

- See network security events in the prioritized incidents list.

Incident management

- Assign to others, change status, link incidents or add notes

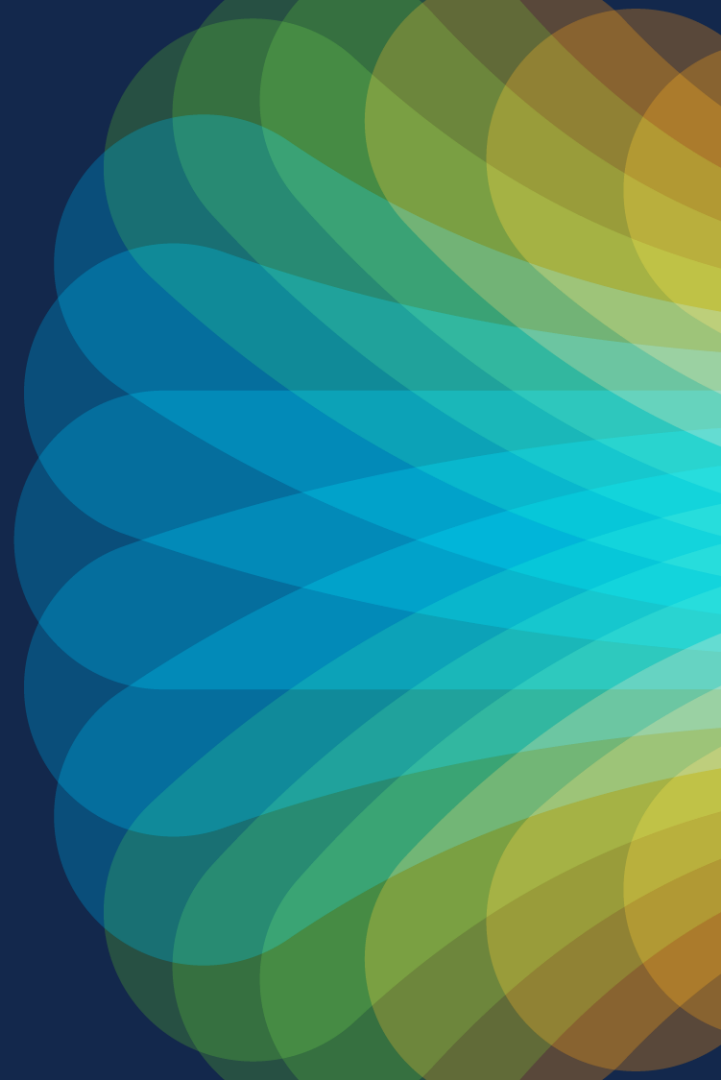
Maintain context

- View incidents in the XDR ribbon or the browser extension

The screenshot displays the Cisco Secure Cloud Analytics (cisco-dcloud-rtp) interface for a specific incident titled "Suspected Malicious URL on ip 192-168-249-115". The interface is divided into several sections:

- Incident Header:** Shows the incident title, status (Unassigned), and a "View Investigation" button. It also includes a timestamp: "Reported by Cisco Secure Cloud Analytics (cisco-dcloud-rtp) on 2023-05-26T13:41:55.000Z - 7 Linked Incidents".
- Overview Tab:** The active tab, showing a network diagram with nodes representing assets, observables, and indicators. The diagram shows a central node (IP Address) connected to several other nodes (URLs, Assets, and Indicators).
- Priority score breakdown:** A section showing the incident's priority score of 765, broken down into 76 Detection Risk and 10 Asset Value at Risk.
- Short description:** A brief summary of the incident: "Suspected Malicious URL for Cisco Demo (RTP)".
- Long description:** A detailed description of the incident, including the alert, tenant (Cisco Demo (RTP)), source (ip-192-168-249-115.us-east-2.compute.internal), and a description of the device communication with a suspected malicious URL.
- Assets, Observables, and Indicators:** Three sections at the bottom, each with a "View all" link. The Assets section lists 13 assets, including "marble", "granite", "slate", "ip-172-16-133-37.us-east-2...", and "441840514". The Observables section lists 4 observables, including "108.62.141.250", "0d5a1c01c2706c8b66ba9...", "drinkfoodapp.com", and "http://drinkfoodapp.com/Ad...". The Indicators section lists 7 indicators, including "Cisco Secure Cloud Analytics (cisco-dcloud-rtp)", "Watchlist Interaction", "User Watchlist Hit", and "Data_Exfiltration".

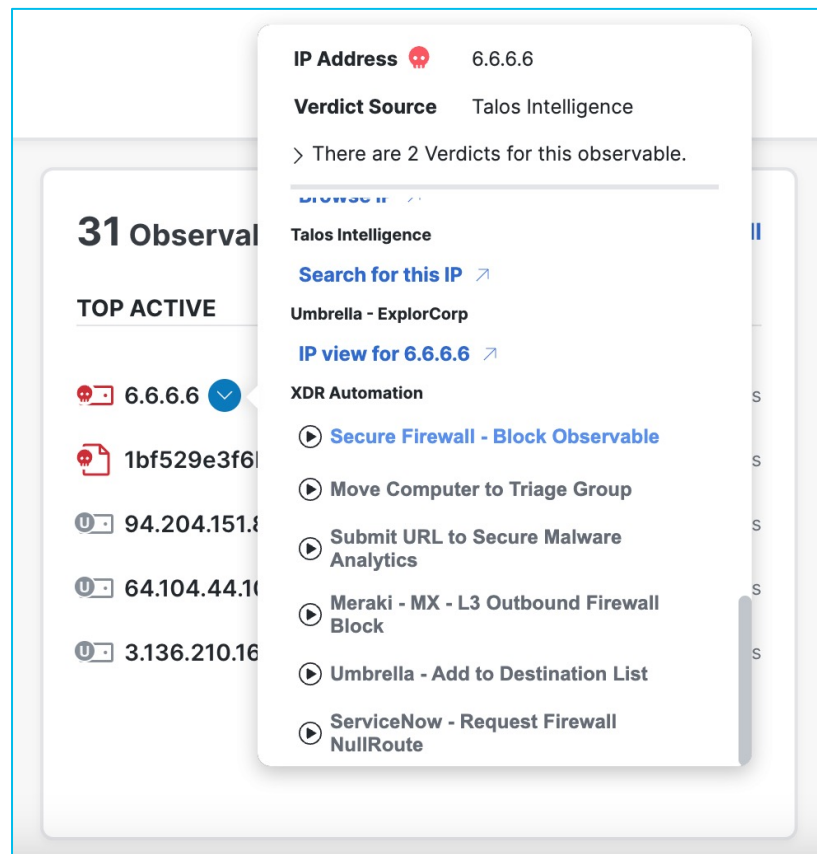
Use Cases



Use Case : Block Observables on Firewall

Problem: Adam the analyst, is reviewing an endpoint alert. He notices an unknown IP address related to a compromise on the endpoint. Adam wants to act by blocking this IP address on the firewall, but he doesn't have access to Firepower Management Center.

Solution: Using the pivot menu Adam can block the IP address at the click of a button from anywhere.



Use Case: PSIRT Impact Monitoring

Problem: A network administrator is continuously monitoring for new PSIRT announcements and checking to see if their devices are vulnerable

Solution: This orchestration workflow will check for new PSIRTs then compare your devices version and notify you if any vulnerable devices were found.

SXO-WF QA 3:05 PM

PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

PSIRT advisory alert

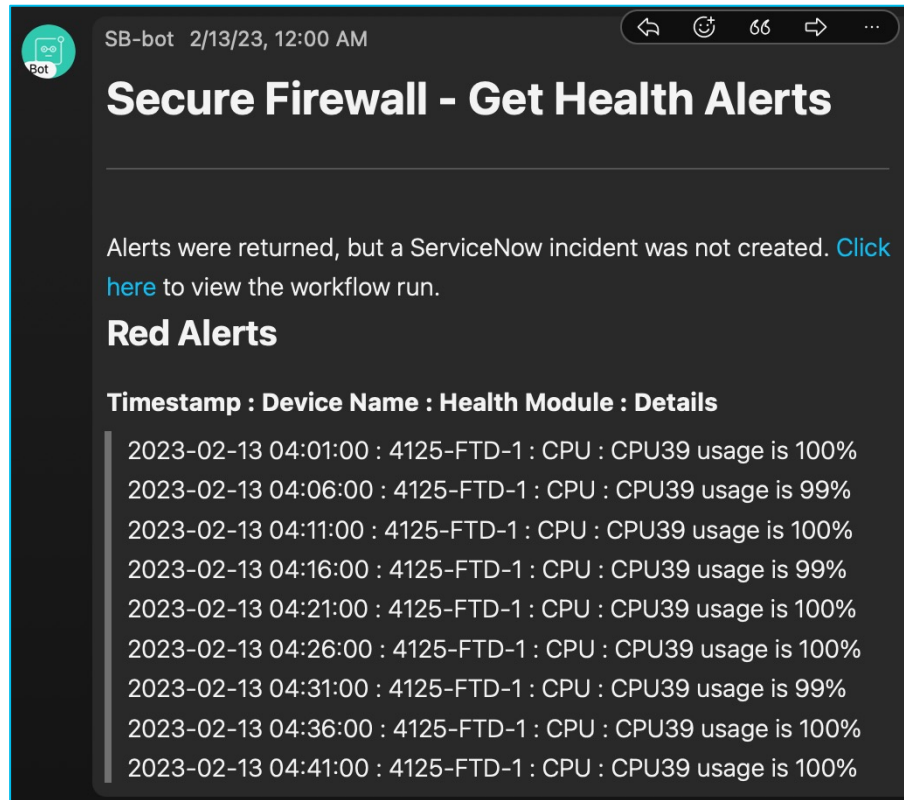
One or more devices managed by Secure Firewall Manager require software updates due to a Medium PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.
2 | FTD-test (ASA) at 127.0.0.1 is running software version 9.14.4 and needs to be upgraded.
3

Use Case: Firewall Health Monitoring

Problem: A network administrator is trying to maintain a healthy network but sometimes a device gets into an unhealthy state. It can take time to react these issue the network administrator is not aware.

Solution: This orchestration workflow will check for health alerts from your devices and proactively notify via Webex teams, Slack, or email.



SB-bot 2/13/23, 12:00 AM

Secure Firewall - Get Health Alerts

Alerts were returned, but a ServiceNow incident was not created. [Click here](#) to view the workflow run.

Red Alerts

Timestamp	Device Name	Health Module	Details
2023-02-13 04:01:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:06:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:11:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:16:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:21:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:26:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:31:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:36:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:41:00	4125-FTD-1	CPU	CPU39 usage is 100%

Use Case: Expiring Time-based Objects

Problem: As a network administrator it is always challenging to manage your policies. Some rules in the policy may not be active due to an expired time range and finding expired rules can be time consuming.

Solution: This orchestration workflow will check rules that have already expired or will expire soon and proactively notify you of which rules to review.

SXO-WF QA 4:10 PM

Time-based rules set to expire

An audit of Secure Firewall has uncovered one or more policies with time-based rules set to expire within the next 30 days

Policy: Block All Traffic

- Allow Apple has a time-based object titled 2-28 which expired -77 days ago

Policy: Default

- Allow Apple has a time-based object titled 2-28 which expired -77 days ago

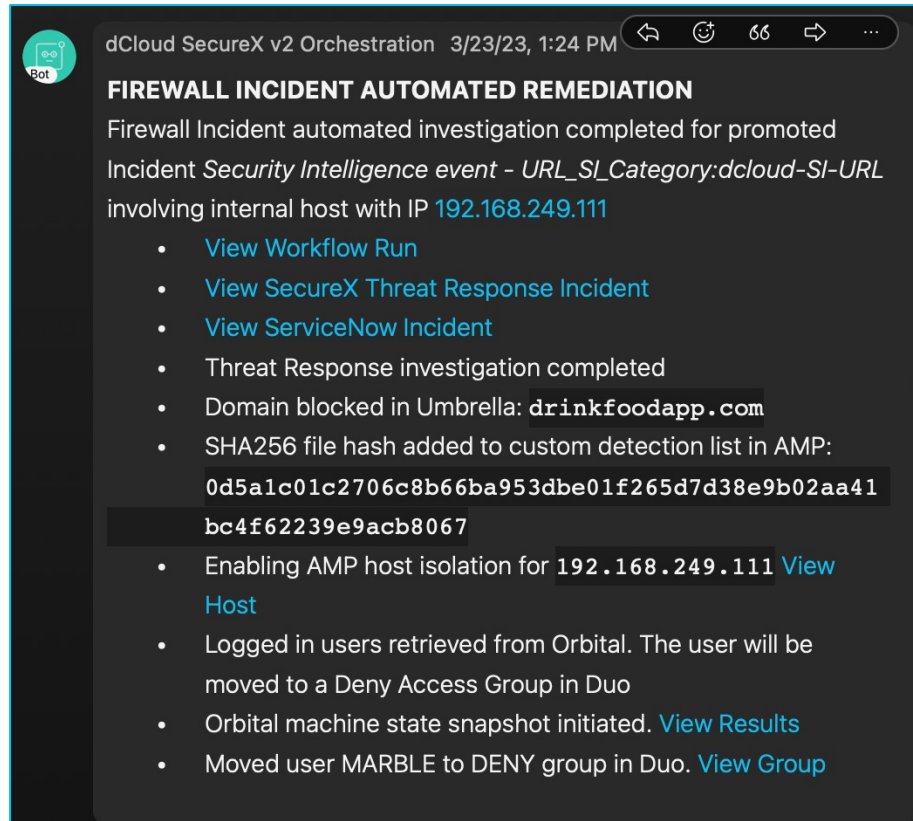
Policy: SecureX Policy

- end_of_april_rule has a time-based object titled end_of_april which expired -16 days ago
- end_of_may_rule has a time-based object titled end_of_may which is set to expire in 14 days
- 5/15 end has a time-based object titled 5-15 which expired -1 days ago

Use Case: Impact RED Remediation

Problem: A high priority intrusion event is detected by the Firewall. Adam, the analyst, needs to remediate quickly across multiple technologies.

Solution: An XDR orchestration workflow investigates the event and waits for approval. Once approval is granted, automated remediation at the DNS, application, and endpoint level are taken.



The screenshot displays the dCloud SecureX v2 Orchestration interface. At the top, it shows the title 'dCloud SecureX v2 Orchestration' and the timestamp '3/23/23, 1:24 PM'. Below the title, the main heading is 'FIREWALL INCIDENT AUTOMATED REMEDIATION'. The text describes the workflow: 'Firewall Incident automated investigation completed for promoted Incident Security Intelligence event - URL_SI_Category:dcloud-SI-URL involving internal host with IP 192.168.249.111'. A list of actions follows, including links to view workflow runs, threat response incidents, and service now incidents, as well as status updates like 'Threat Response investigation completed', 'Domain blocked in Umbrella: drinkfoodapp.com', and 'SHA256 file hash added to custom detection list in AMP: 0d5a1c01c2706c8b66ba953dbe01f265d7d38e9b02aa41bc4f62239e9acb8067'. The final actions listed are 'Enabling AMP host isolation for 192.168.249.111', 'Logged in users retrieved from Orbital', 'Orbital machine state snapshot initiated', and 'Moved user MARBLE to DENY group in Duo'.

dCloud SecureX v2 Orchestration 3/23/23, 1:24 PM

FIREWALL INCIDENT AUTOMATED REMEDIATION

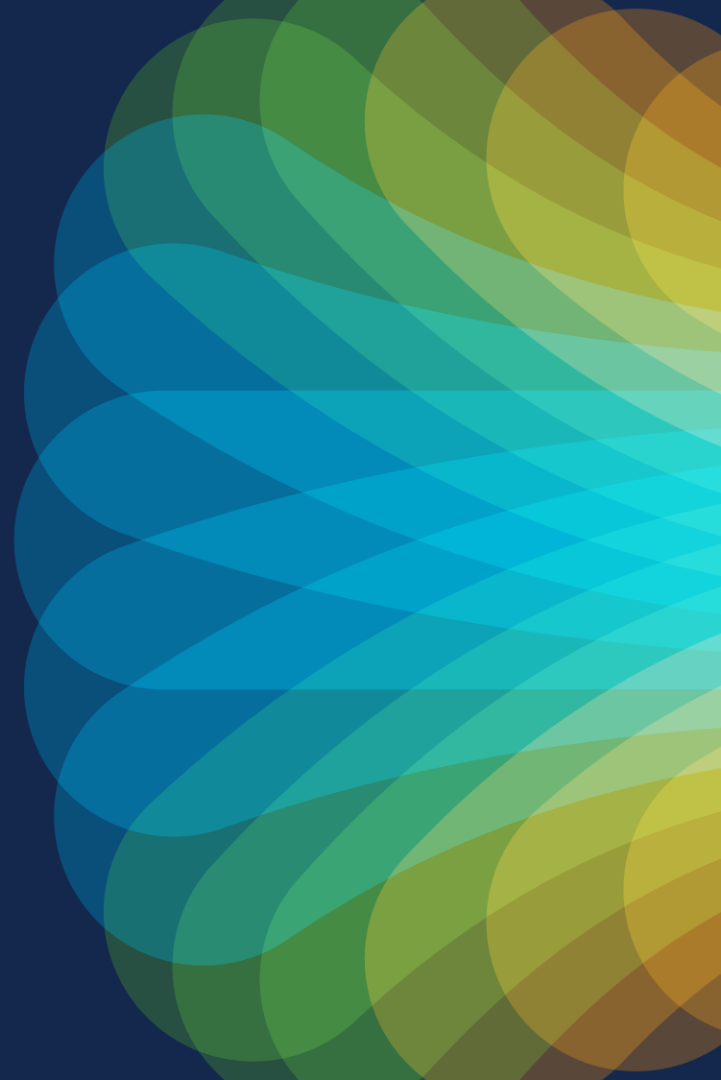
Firewall Incident automated investigation completed for promoted Incident Security Intelligence event - URL_SI_Category:dcloud-SI-URL involving internal host with IP 192.168.249.111

- [View Workflow Run](#)
- [View SecureX Threat Response Incident](#)
- [View ServiceNow Incident](#)
- Threat Response investigation completed
- Domain blocked in Umbrella: drinkfoodapp.com
- SHA256 file hash added to custom detection list in AMP: 0d5a1c01c2706c8b66ba953dbe01f265d7d38e9b02aa41bc4f62239e9acb8067
- Enabling AMP host isolation for 192.168.249.111 [View Host](#)
- Logged in users retrieved from Orbital. The user will be moved to a Deny Access Group in Duo
- Orbital machine state snapshot initiated. [View Results](#)
- Moved user MARBLE to DENY group in Duo. [View Group](#)

Key Takeaways

- Unified Management and Visibility
- Comprehensive Threat Protection
- Automated and Guided Incident Response

Security Service Edge (SSE)



SASE/SSE approach is the technology foundation

Fundamental to your security strategy for a hyper-distributed world

SASE brings networking & security capabilities into a single-service, cloud-native model to address today's challenges.

65% plan on adopting SSE in next 2 years

SASE

Converged set of **cloud networking**



SD-WAN

cloud security



SSE

SSE Product Family

Protecting your investment throughout the SSE journey



Introducing Cisco Secure Access

Modernize your defense with converged cloud security grounded in zero trust



Cisco Secure Access

A comprehensive Security Service Edge (SSE) solution to accelerate your SASE journey

Core SSE Capabilities



Firewall as a
Service
(FWaaS)



Secure Web
Gateway (SWG)



Cloud Access
Security
Broker (CASB)



Zero Trust
Network
Access (ZTNA)

and so much more in one subscription...

Cisco Secure Access

Go beyond core Secure Service Edge (SSE) to better connect and protect your business

Core SSE



Secure Web Gateway (SWG)



Cloud Access Security Broker (CASB) and DLP



Zero Trust Network Access (ZTNA)



Firewall as a Service (FWaaS) and IPS

Cisco delivers the core and more in a single subscription...



DNS Security



Multimode DLP



Advanced Malware protection



Sandbox



Talos Threat Intelligence



VPN as a Service



Digital Experience Monitoring*



Remote Browser Isolation*

Add-on solutions



SD-WAN



XDR

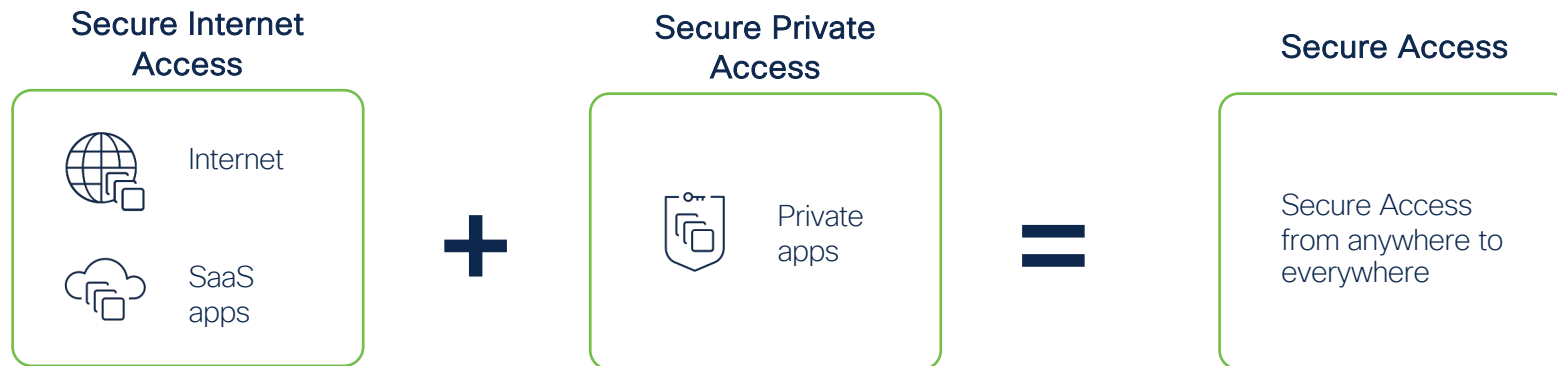


DUO MFA/SSO



CSPM

Use Cases



Cisco Secure Access – User Anywhere

STEP 1
Authenticate

STEP 2
Go to Work



ZTNA



VPN



SaaS



Direct

Secure
Access

Private apps

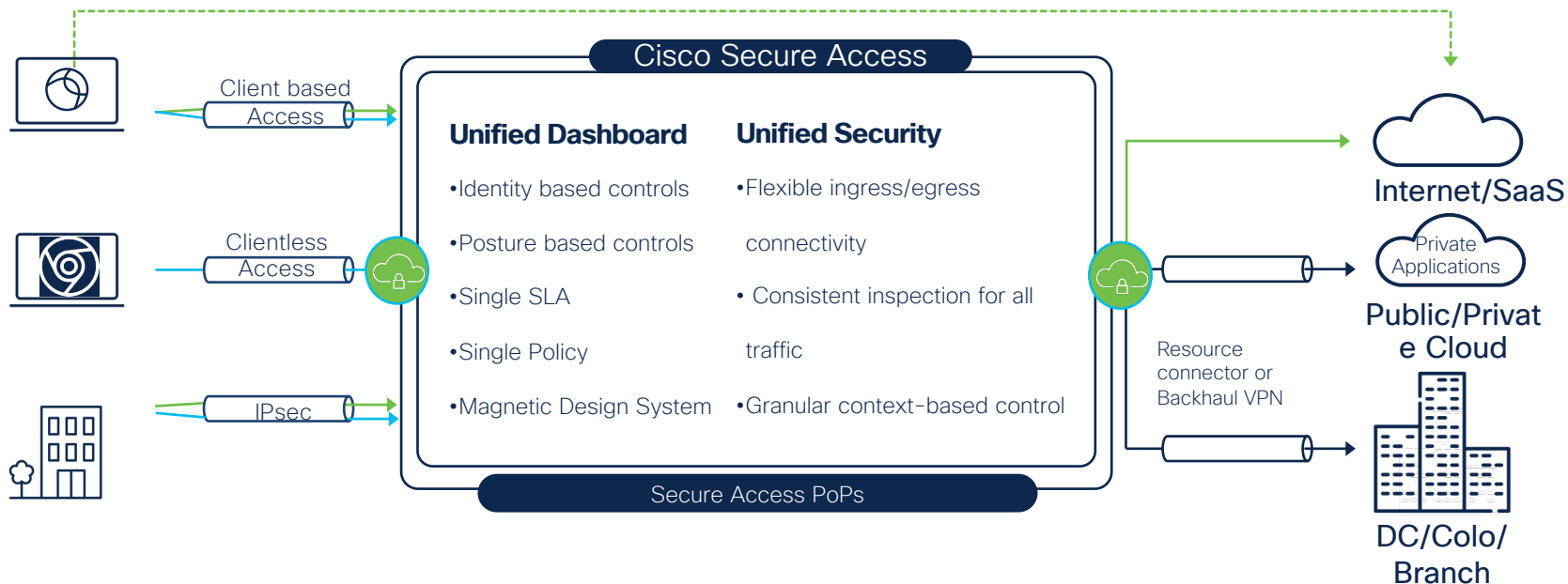
Traditional apps

SaaS apps

Internet apps

We handle the
connectivity, access
control and security

Architecture Overview

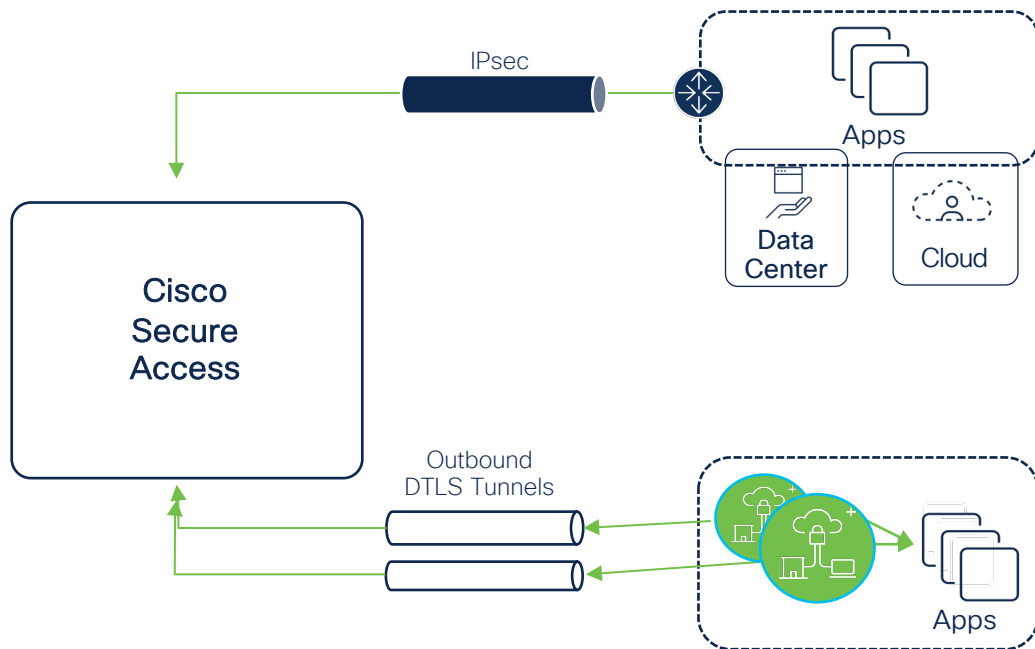


Users

How

Apps

Apps: Private Applications



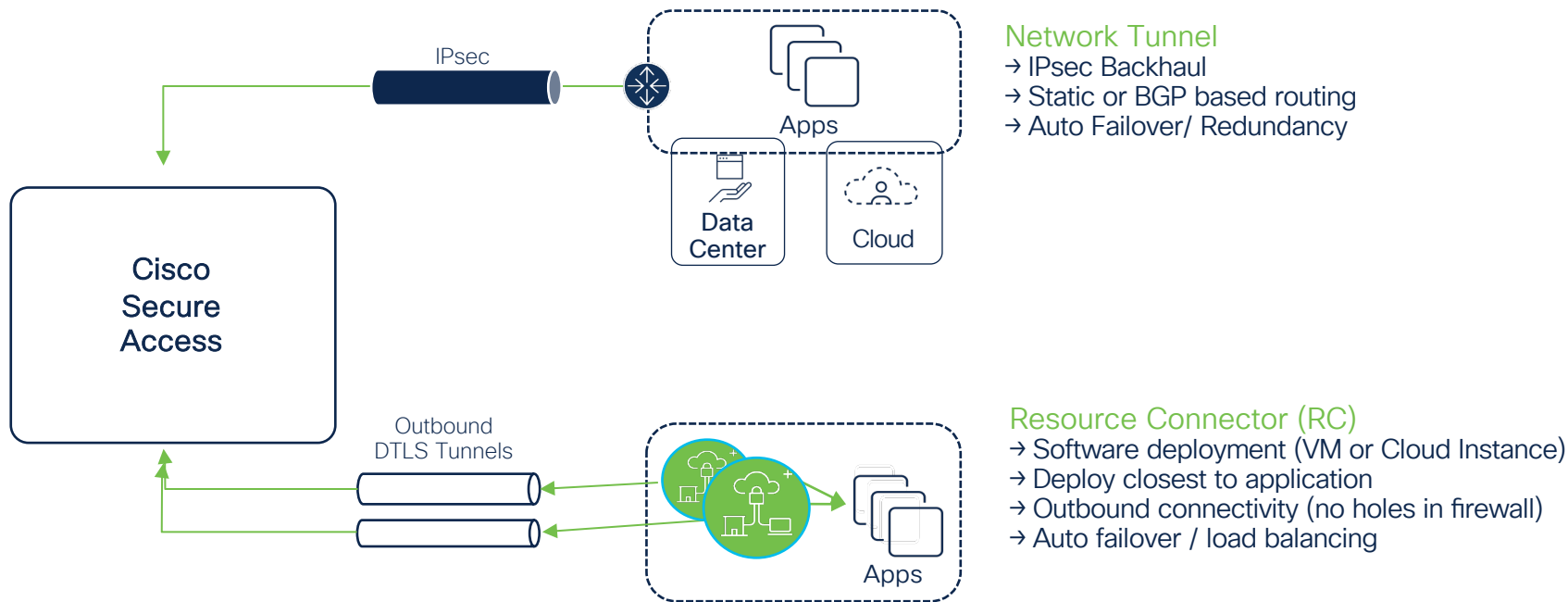
Network Tunnel

- IPsec Backhaul
- Static or BGP based routing
- Auto Failover/ Redundancy

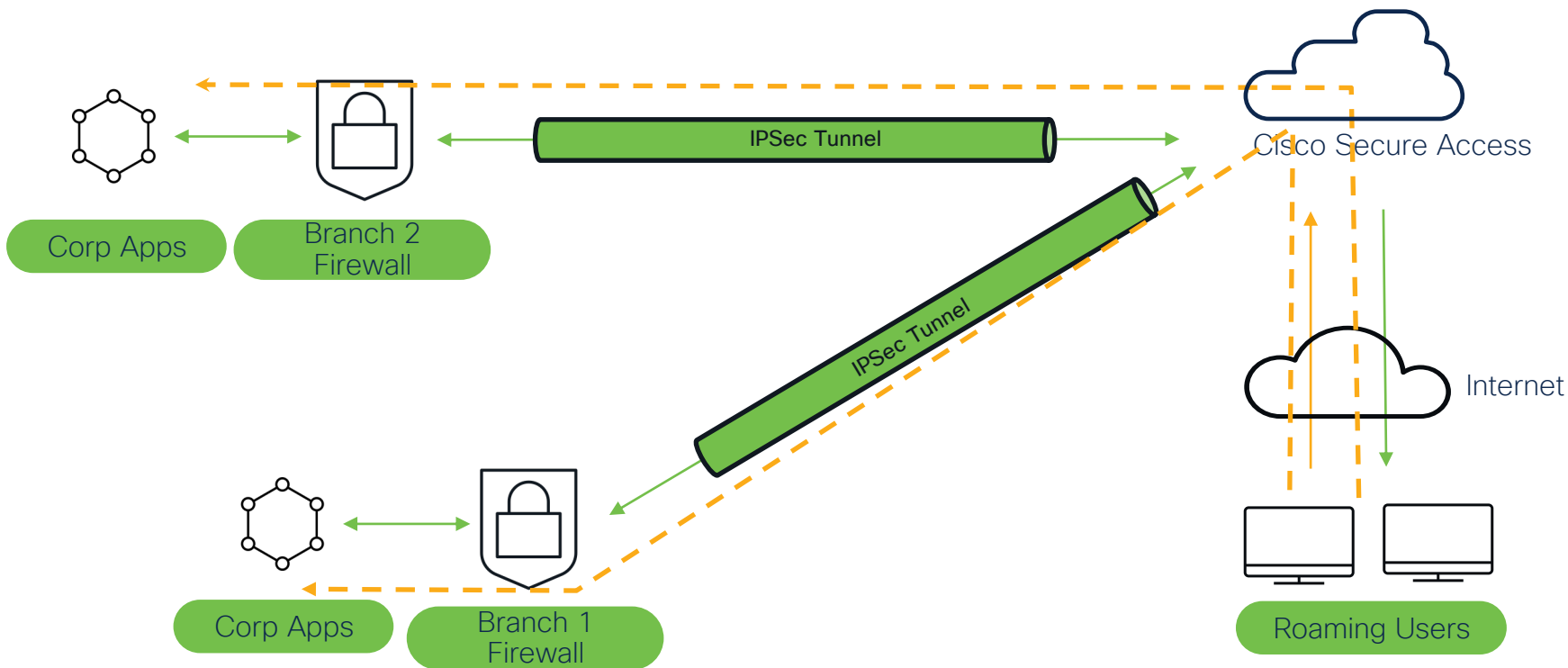
Resource Connector (RC)

- Software deployment (VM or Cloud Instance)
- Deploy closest to application
- Outbound connectivity (no holes in firewall)
- Auto failover / load balancing

Apps: Internet/SaaS Applications

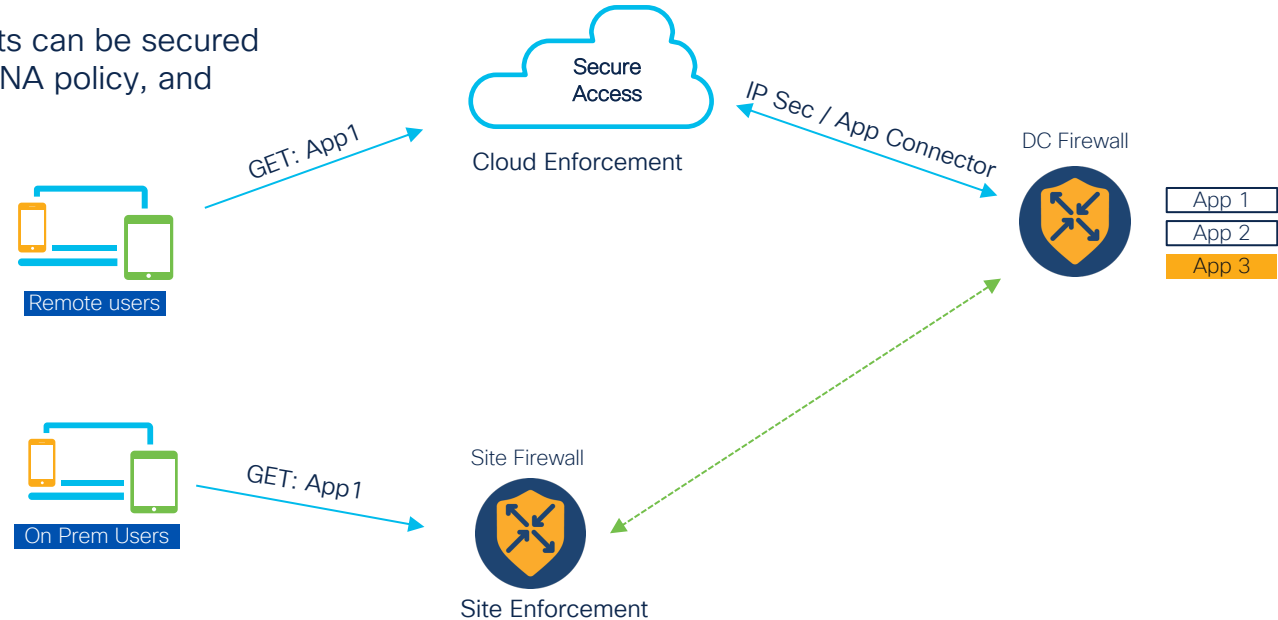


Secure Firewall Integration



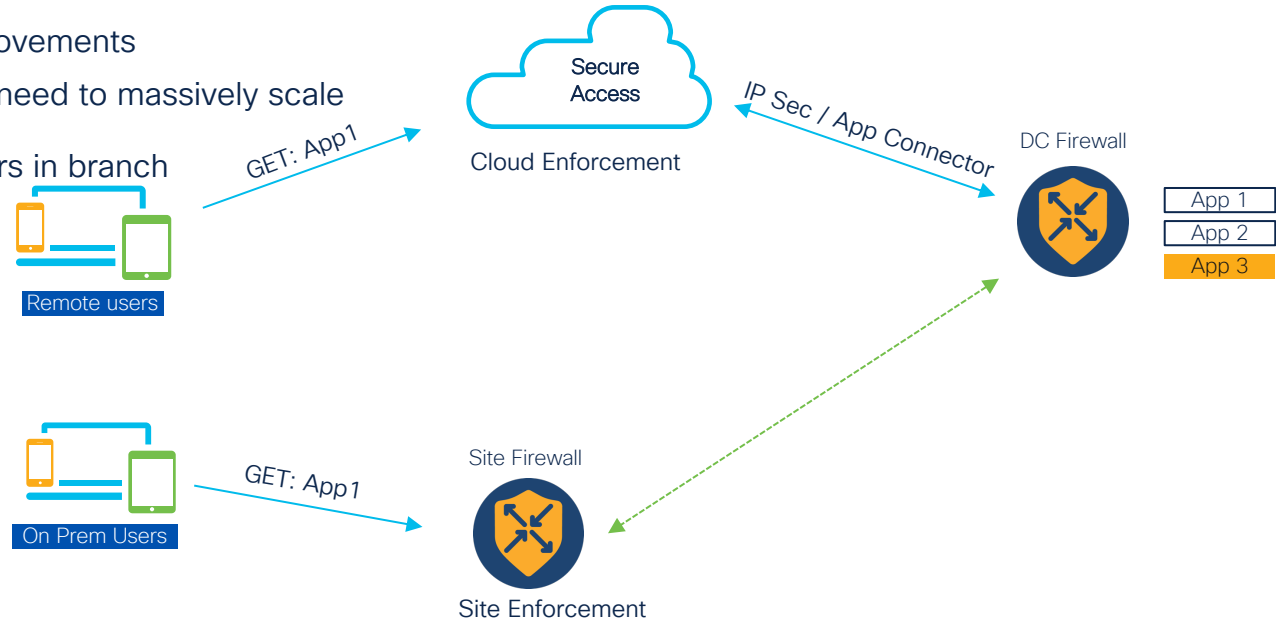
Secure Firewall + SSE = Future

- Admin has Central Policy Configuration – Secure Access
- Users On network clients can be secured in branch with same ZTNA policy, and identity



Secure Firewall + SSE = Future

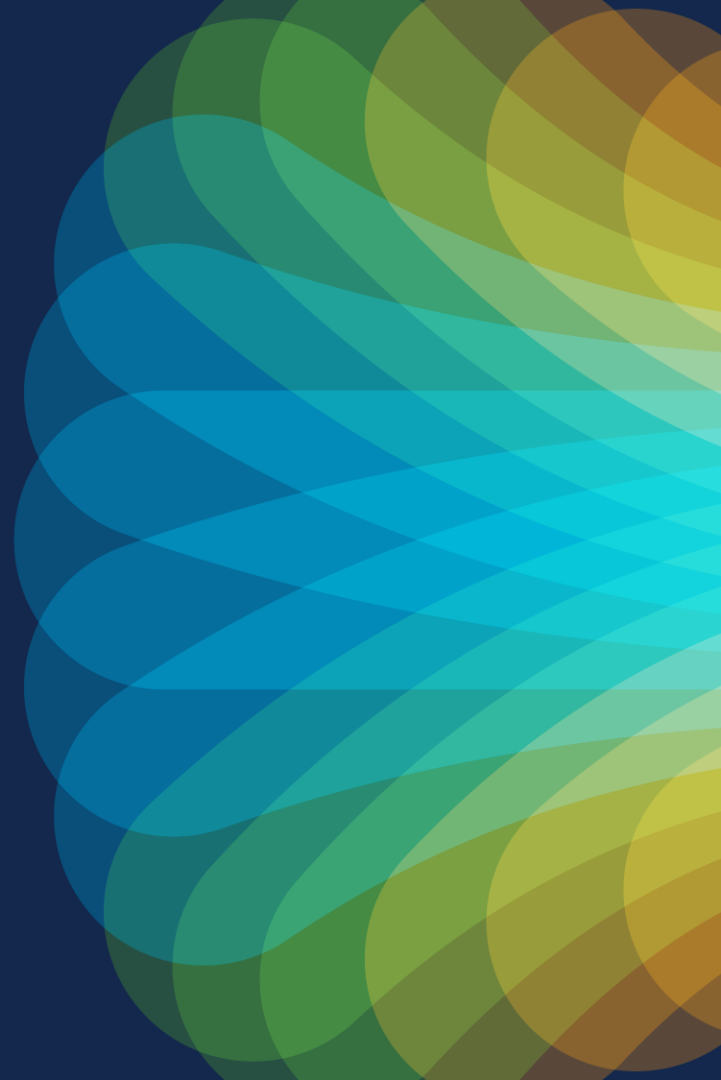
- User network has no direct routes to application network
- User Performance improvements
- Cost optimization – No need to massively scale internet pipe for large number of users in branch



Key Takeaways

- Protect users, applications, and resources anywhere
- Expand visibility into cloud applications and shadow IT
- Unified and consistent applications policies

Zero Trust Network Access (ZTNA)



Your Speaker

Dinesh Moudgil



- dmoudgil@cisco.com
- From Chandigarh, India
- CCIE Security #58881
- 12 Years in Industry, 9 with Cisco
- TAC - HTTS - TME Leader
- Lead VPN & SD-WAN
- Likes outdoors and guitar



What is Zero Trust Network Access?

- Zero Trust Network Access (ZTNA) means different things to different organisations.
- Primarily, it's about granting USERS access to APPLICATIONS and doing so only after the relevant criteria are met.
- The “Network Access” part of ZTNA is not Network Access as we typically understand it.
- Users should not need access at the network level to access a specific application.
- ZTNA does not just apply to remote access, access from inside the network should also be covered by the same protections.

Zero Trust Application Access

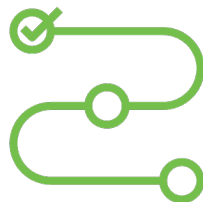
Securely and Simply Connect Users to Private Applications

Zero trust application access (ZTAA) moves beyond traditional “authorize then ignore” ZTNA models by adding complete threat inspection and policy for each individual application



Limit who is allowed

Per application access with clientless SAML, Azure AD, ISE, and Duo



Limit where they can go

Reduce access to specific apps to limit attack surface and lateral spread of threats

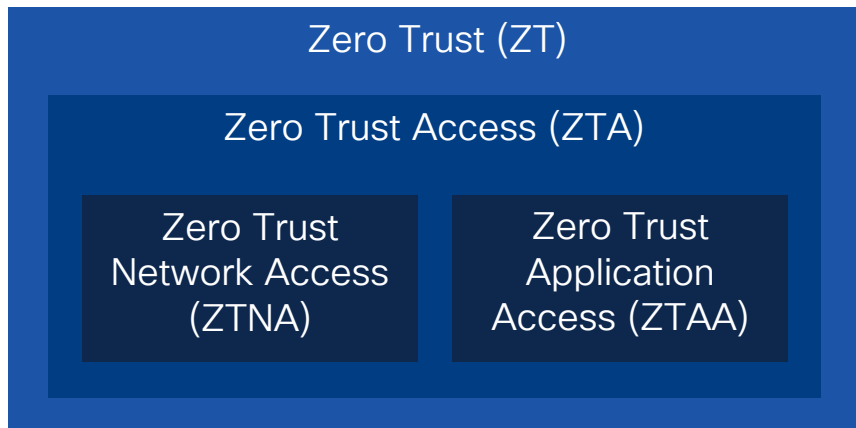


Limit threats they may bring

Go beyond traditional ZTNA by continuously inspecting allowed traffic/behaviors with IPS/malware protection

ZT vs. ZTA vs. ZTNA vs. ZTAA

- Zero Trust
 - A comprehensive security framework that prioritizes least privilege, strict access controls, and continuous monitoring to mitigate risks and protect resources.
- Zero Trust **Access**
 - A specific aspect of Zero Trust that **focuses on managing and enforcing access** to resources
- Zero Trust **Network Access** (ZTNA)
 - A subset of Zero Trust Access that focuses on secure **access to networks**.
- Zero Trust **Application Access** (ZTAA)
 - A subset of Zero Trust Access that focuses on secure **access to individual applications**.



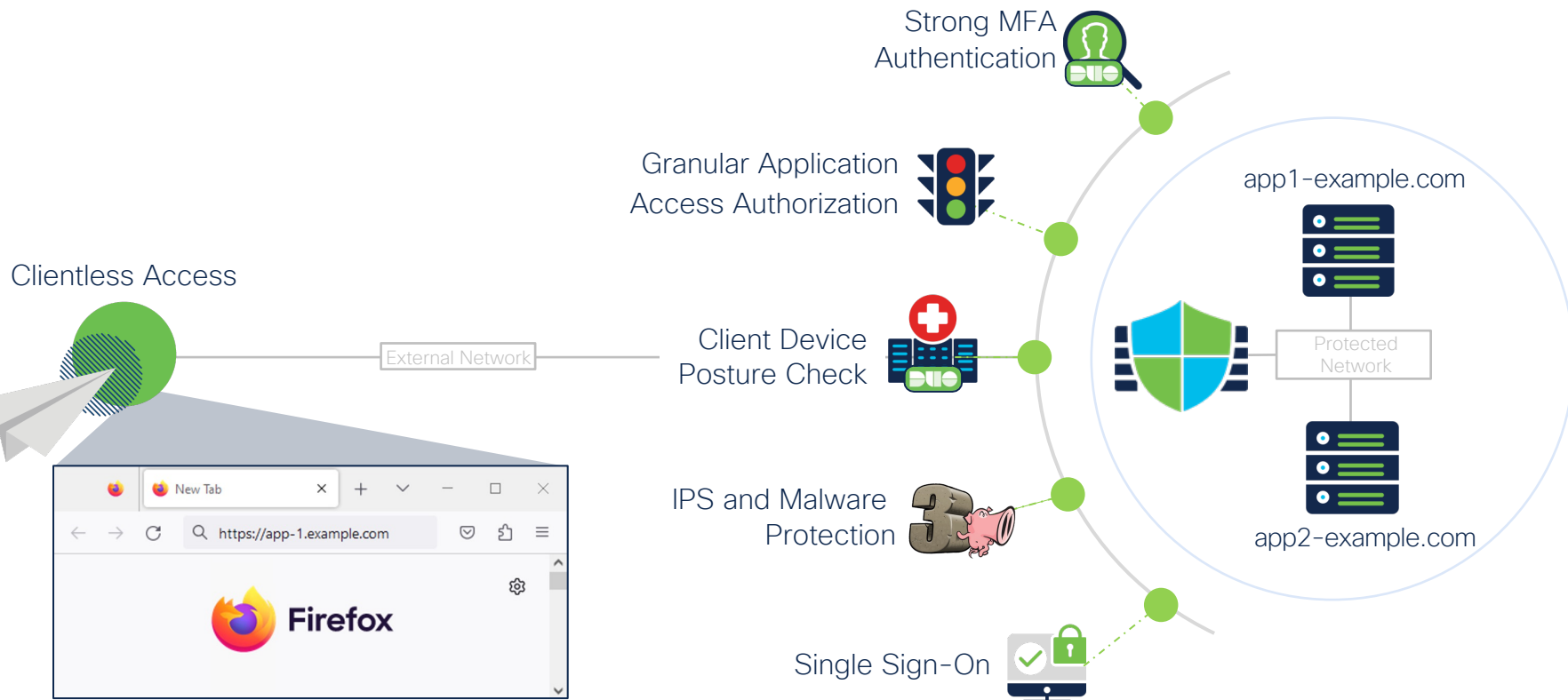
RAVPN vs ZTNA

	Remote Access VPN	Zero Trust Network Access
Access Granted	Access to full network or network segment	Access to specific resource/application
Network	Client gets IP address on the network	No specific IP address assigned to the client for access
Posture	Posture assessed once at VPN Authentication	Posture assessed at each application access with Continuous Trusted Access
Headend	1:1 Client-to-Headend relationship	Client can connect to different headends per application

Clientless and Client-Based ZTNA

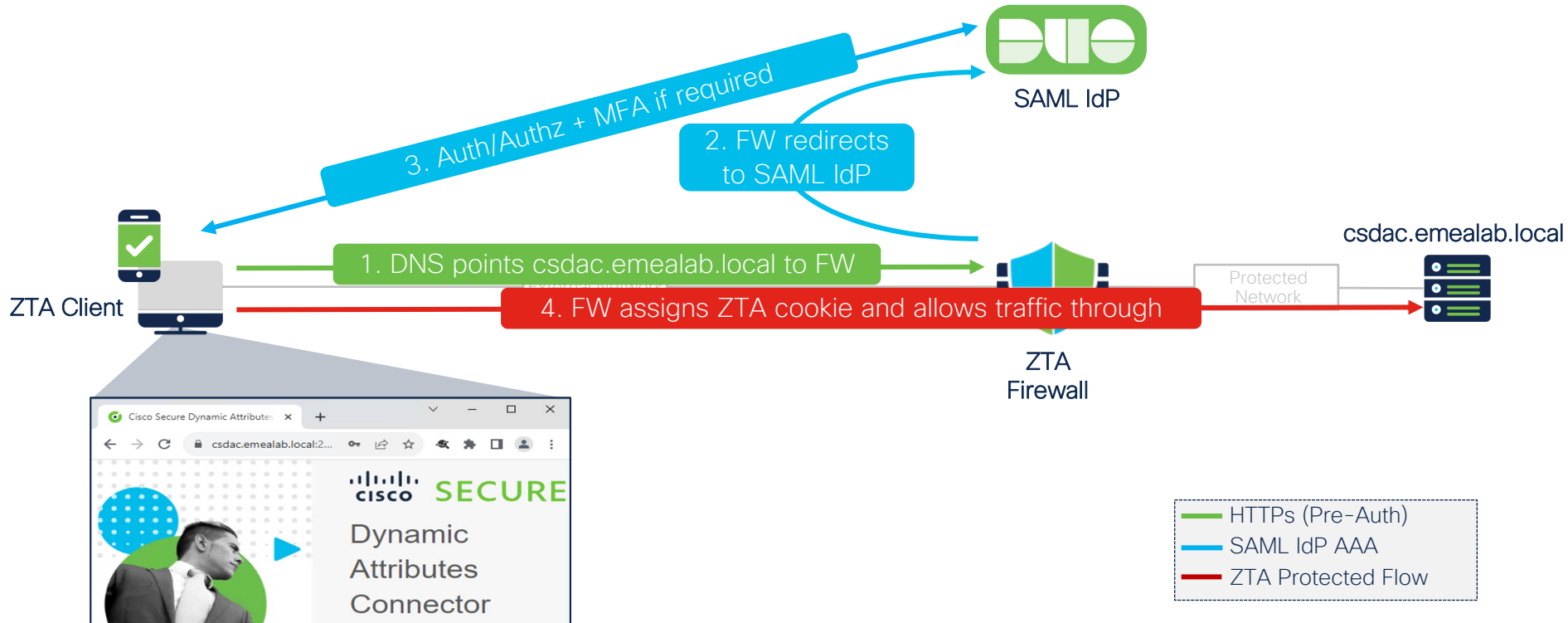
	Clientless ZTNA	Client-Based ZTNA
Endpoint Presence	No client application required on endpoint device	Client software required to be installed on endpoint device
Access Type	Can only be accessed through a web browser	Client software handles traffic transparent to the user
Application Type	Only browser-based web applications	Supports all applications on different ports and protocols
Posture Type	Posture only available through authentication flow (e.g. Duo Health or Intune)	Client software handles posture based on policy (similar to HostScan or ISE Posture)
User Types	Can be used for Contractor/3 rd Party clients as well as internal users on personal devices	Generally restricted to customers owned and managed devices due to client requirement.

Zero Trust Access - Overview



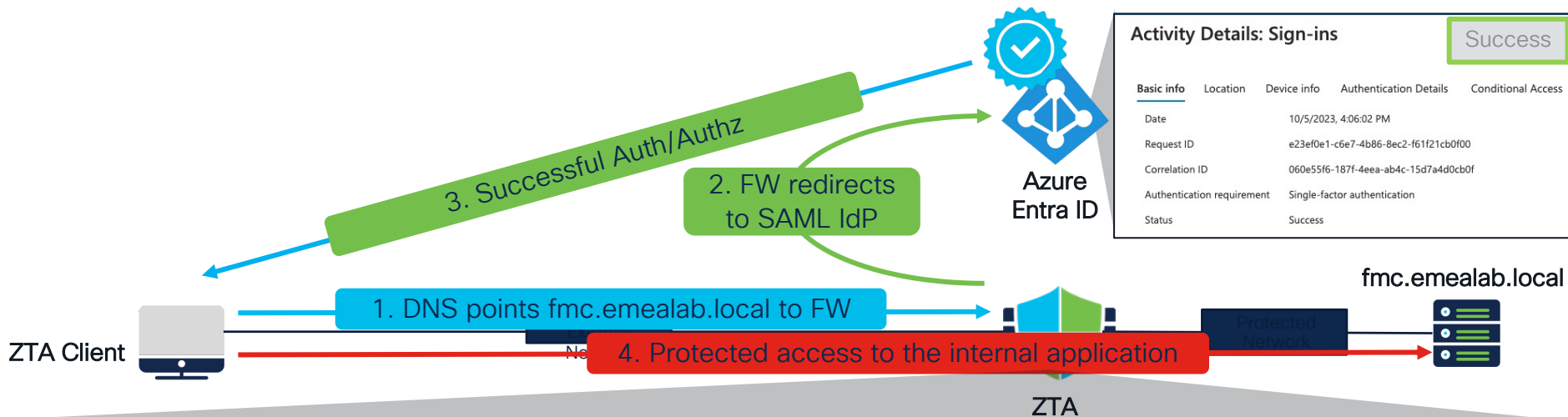


Zero Trust Access – Basic Flow





Zero Trust Access – Successful Auth/Authz



Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ? admin ✓ Cisco SECURE

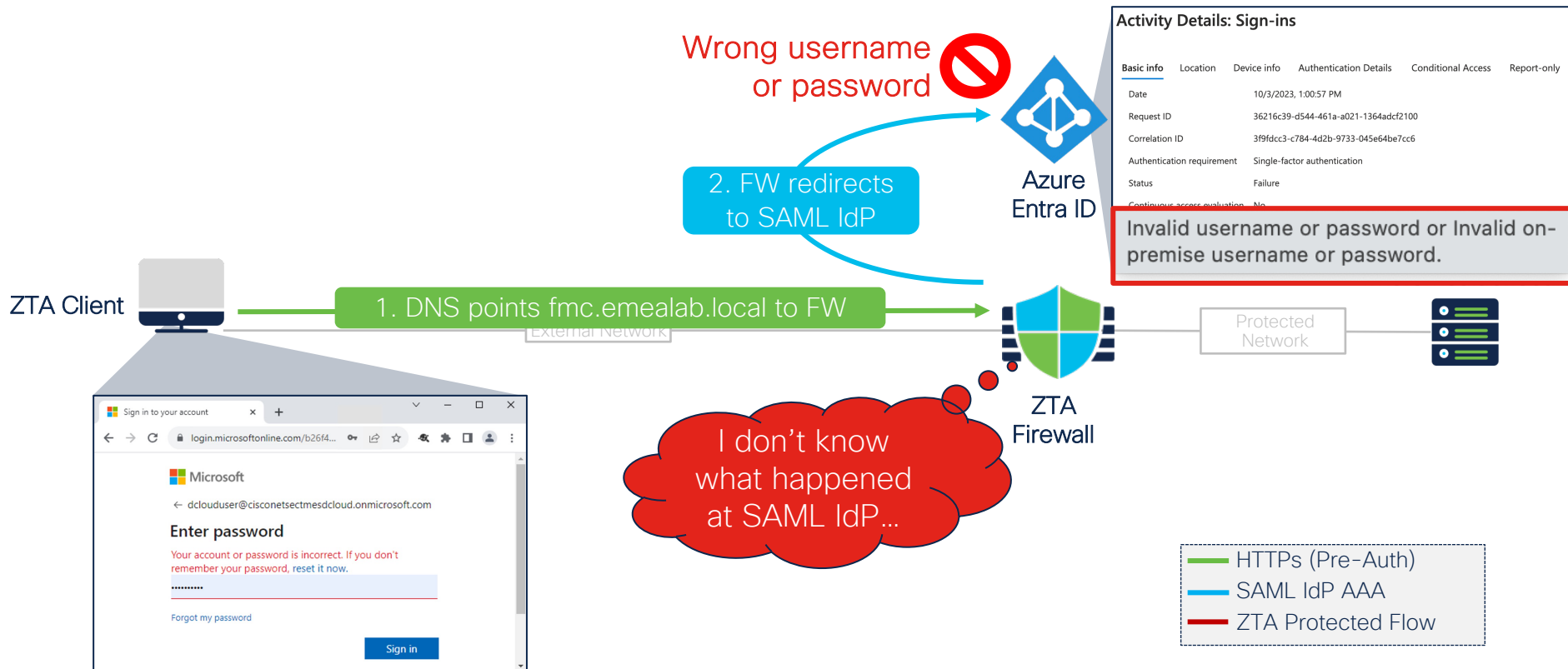
Zero Trust Application /N/A x +

Showing all 4 events (4) Last 30 minutes Go Live

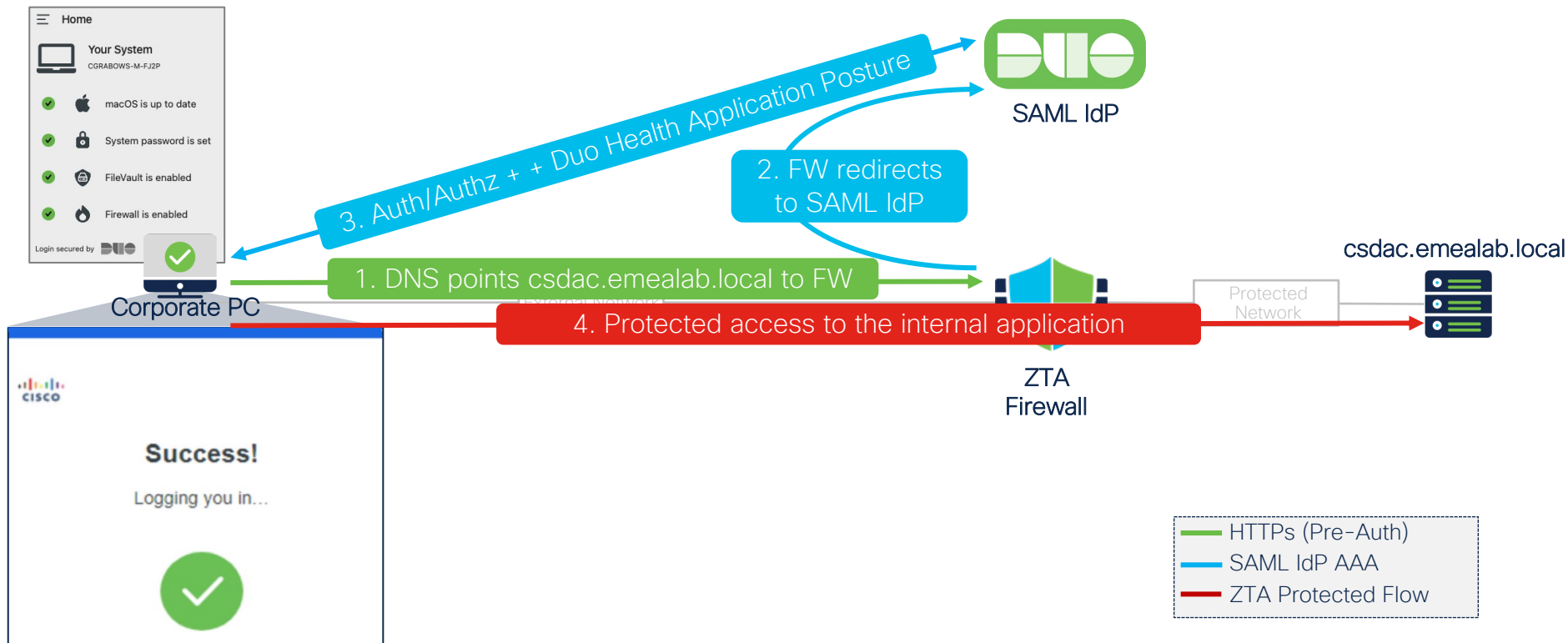
Time	Event Type	Action	Source IP	Destination IP	Destination Port / ICMP Code	Zero Trust Application	Zero Trust Application Group	Zero Trust Application Policy	Source User
2023-10-06 13:31:48	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@cisco.netsectmesdcloud.onmicrosoft.com
2023-10-06 13:26:20	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@cisco.netsectmesdcloud.onmicrosoft.com
2023-10-06 13:21:37	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@cisco.netsectmesdcloud.onmicrosoft.com
2023-10-06 13:16:29	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@cisco.netsectmesdcloud.onmicrosoft.com



Zero Trust Access – Failed Authentication



Zero Trust Access – Compliant Endpoint



Zero Trust Access – Non-Compliant Endpoint



Personal PC

1. DNS points csdac.emealab.local to FW

ZTA Firewall

csdac.emealab.local

External Network

Protected Network

2. FW redirects to SAML IdP

SAML IdP

3. Auth/Authz + Duo Health Application Posture

We're sorry. Access is not allowed.

- We're sorry, access is not allowed because you are using a personal device.

To fix this problem, please reach out to your administrator or IT Helpdesk

Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device
8:12:47 AM OCT 3, 2023	Denied Endpoint is not trusted	samitstuser	Generic SAML Service Provider - Single Sign-On	N/A	> Windows 10, version 22H2 (19045.3448) As reported by Device Health

✓ Windows 10, version 22H2 (19045.3448)
As reported by Device Health

Hostname	PERSONAL-PC
Chrome	117.0.5938.132
Flash	Not installed
Java	Not installed

Device Health Application

Installed

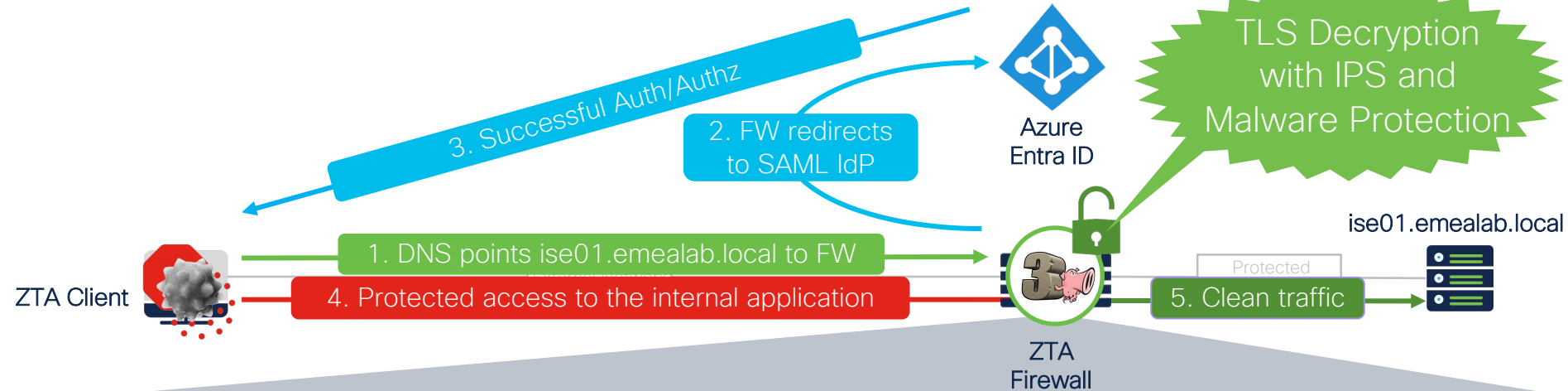
Firewall	On
Encryption	Off
Password	Set
Security Agents	Running: Windows Defender

Almere Stad, FL, Netherlands
64.103.36.135

Not a Trusted Endpoint
determined by Device Health



Zero Trust Access – Successful Auth/Authz



Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

Event Type

Intrusion

Malware

Refresh

Showing all 27 events (8 19)

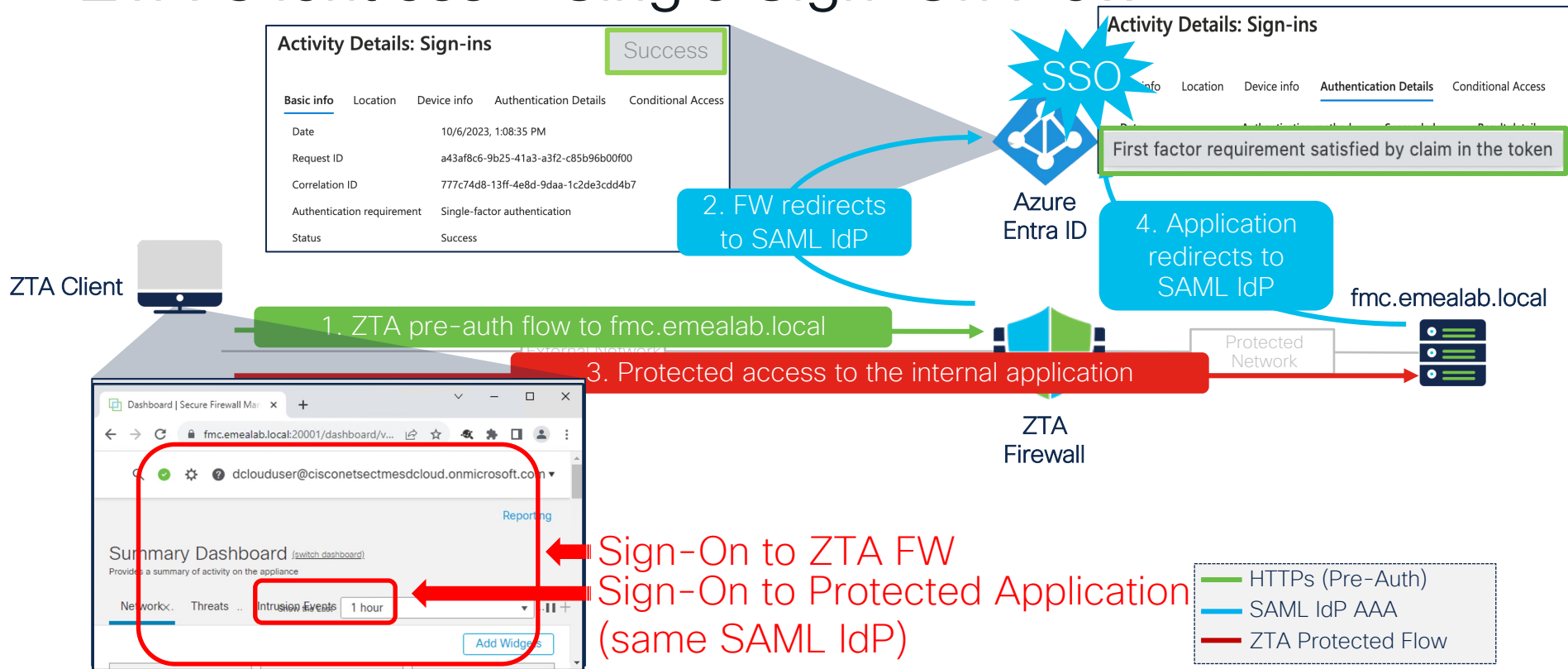
Last 1 month

Go Live

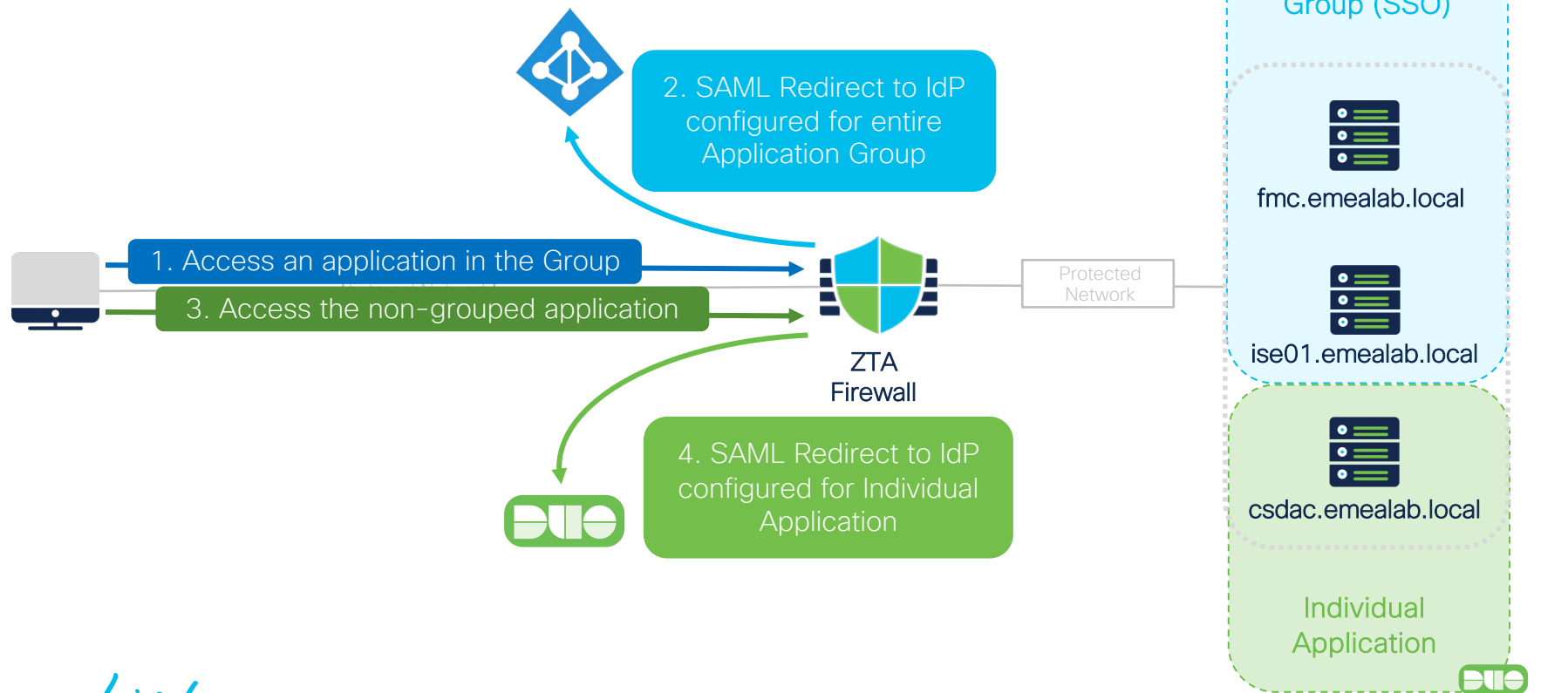
	Time	Event Type	Action	Source IP	Destination IP	Destination Port / ICMP Code	Source User	
>	2023-10-03 09:59:30	Malware	Malware Block	172.16.135.101	172.16.134.96	443 (https) / tcp	dclouduser@cisconetsectmesdcloud.onmicrosoft.com	
>	2023-10-03 09:59:28	Intrusion	Alert	172.16.135.101	172.16.134.96	443 (https) / tcp	dclouduser@cisconetsectmesdcloud.onmicrosoft.com	



ZTA Clientless - Single Sign-On Flow

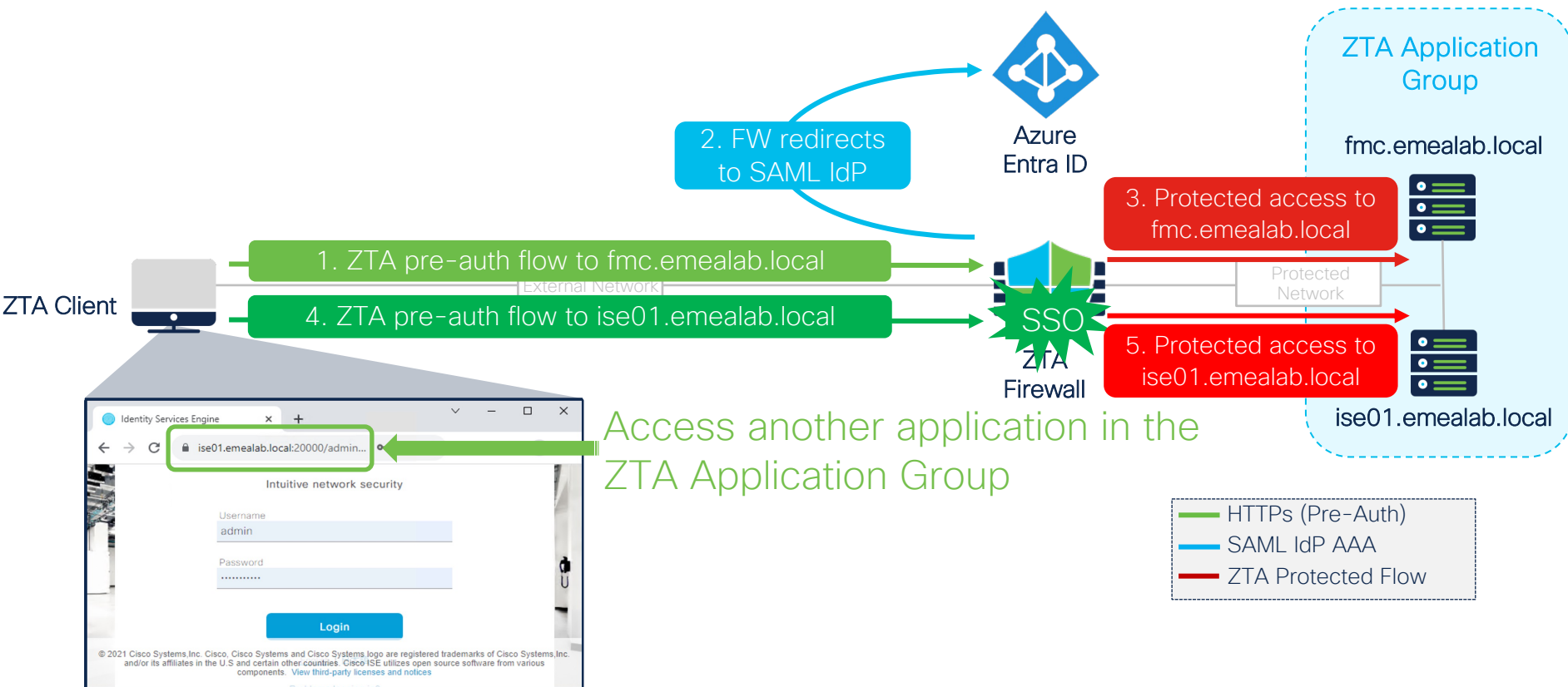


ZTA Individual vs. Grouped Applications





ZTA Application Group Flow



Zero Trust Access - Recommendations

- Only SAML IdPs are supported e.g. Azure AD, Duo, Ping ID, One Login, Okta
- DNS needs to be configured to attract application traffic to the ZTA firewall's interface.
- ZTA application protection supported for Internet and internal access use-case (with proper DNS configuration)
- ZTA is supported on routed mode in HA/Cluster*/Multi-Instance deployments
- License requirements:
 - Essentials license for basic ZTA access
 - IPS and/or Malware Defense for application traffic inspection
 - ZTA does not work in evaluation mode
- ZTA traffic is not subjected to Access Control Policy (ZTA policy takes precedence)

* - Not supported on individual mode cluster

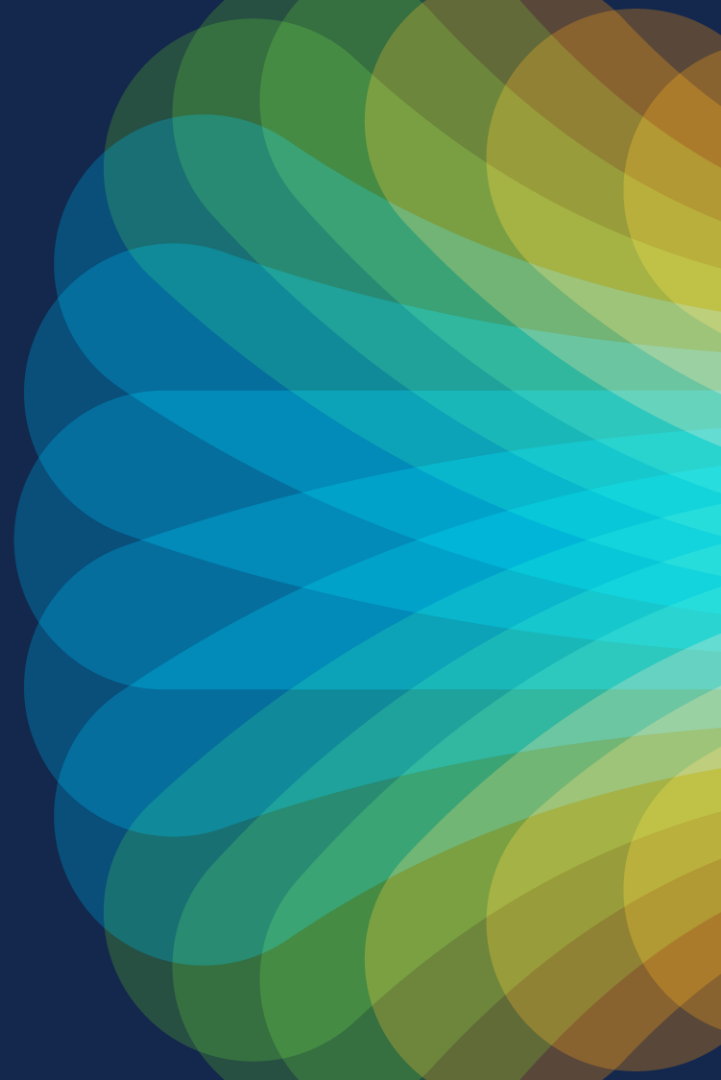
Zero Trust Access - Recommendations

- Supports HTTPs applications only (HTTP, RDP, SSH not supported)
- ZTA supports interactive web applications (requires user SAML login)
- ZTA is not a reverse-proxy:
 - Firewall does not rewrite HTTP requests
 - The flow is based on HTTP redirects
 - TLS decryption is mandatory – Snort validates ZTA HTTP cookie in the HTTP request
- ZTA will not work for non-HTTP traffic tunneled through TCP 443 interface.
- ZTA preserves original client IP address – ensure symmetric traffic between client and application through the firewall (superseded by Source-NAT in 7.4.1)
- A pre-auth certificate matching FQDNs of protected applications is required
- Not supported if protected application redirects between ports or does strict HTTP Host Header validation

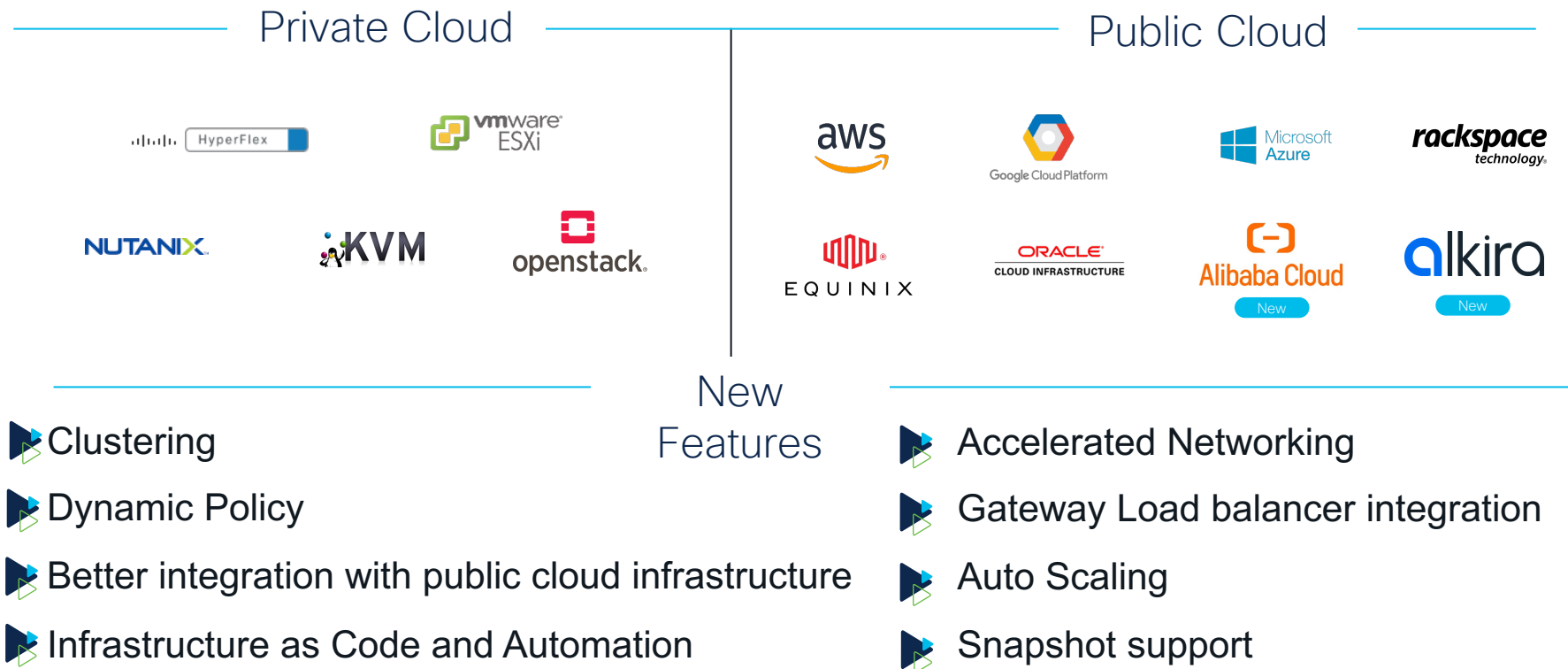
Key Takeaways

- Browser based application access (no agent)
- Reduce attack surface by enforcing security controls
- Leverage SAML SSO for applications with common IdP

Hybrid Cloud



Simplifying Cloud Environments



Nutanix and Hyperflex

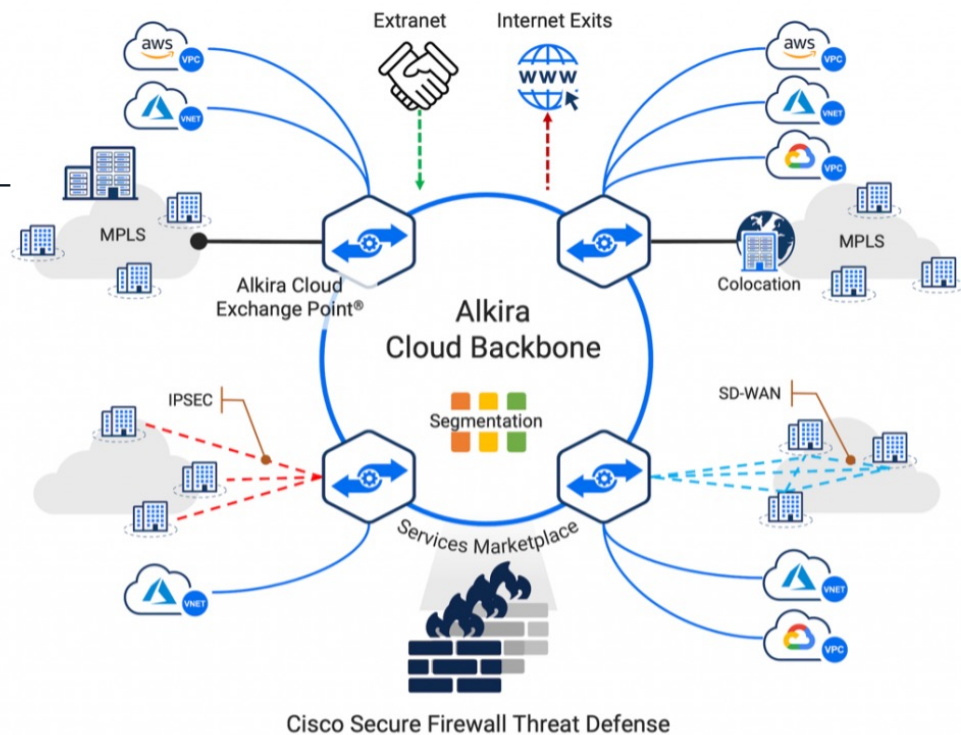
Hyper Convergence Infrastructure

- Cisco Secure Firewall now supports
 - Nutanix AHV
 - Cisco HyperFlex
- Received Nutanix Alliances New Partner of the Year award 2021
- Securing workloads deployed on Nutanix AHV & Hyperflex for both East-West & North-South traffic segmentation and inspection



Integration with Alkira

- Simplified network and security architecture
- Deeper visibility and control in multi-cloud environments
- Unified security policy
- Greater visibility



Use Cases

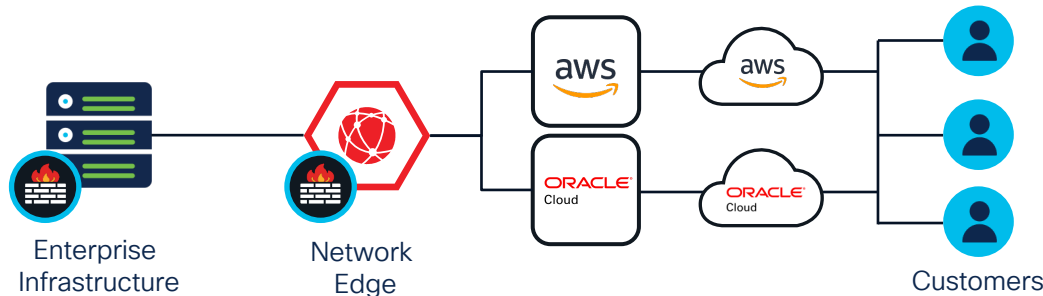
Deploy a virtual firewall in minutes

No need to
purchase additional hardware

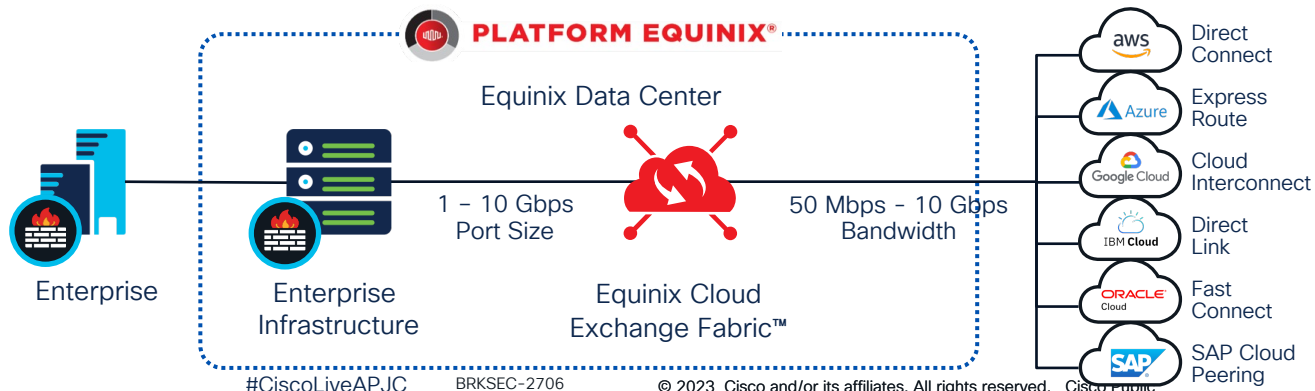
Protect corporate apps from public endpoints

Built-in integration to
Cisco Life!

Use Case 1: Protect data with hybrid cloud firewall



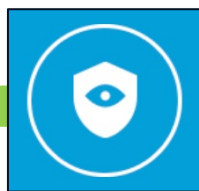
Use Case 2: Directly connecting to multiple clouds in multiple locations



Secure Firewall Virtual Capabilities



AVC



NGIPS



AMP



URL



VPN
(S2S & RAVPN)



SI

AVC - Application Visibility and Control
NGIPS - Next-Generation Intrusion Prevention System
AMP - Advanced Malware Protection
VPN - Virtual Private Network
URL - URL filtering
SI - Security Intelligence



Firewall

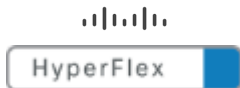
Stateful firewall
NAT
Static and dynamic routing

vmware®

openstack.

aws

Microsoft
Azure



KVM

NUTANIX
Your Enterprise Cloud Platform™

Google Cloud

ORACLE®
CLOUD INFRASTRUCTURE

CISCO *Live!*

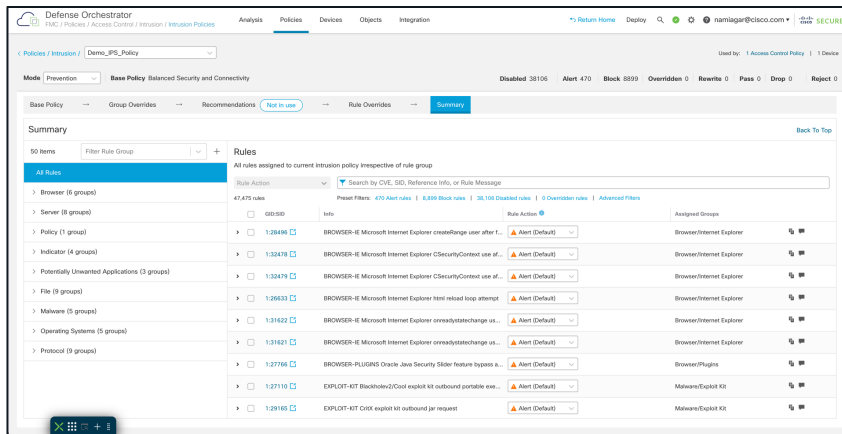
Cloud-delivered Firewall Management Center

Key benefits

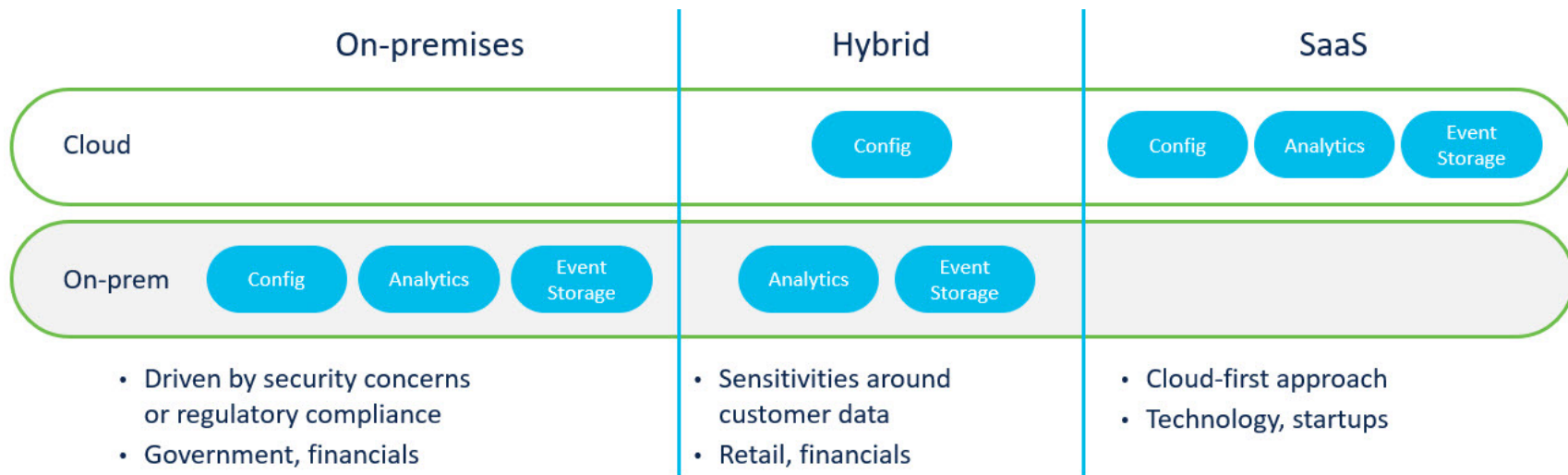
- Eliminate change management and update overhead
- Cisco ensures uptime, increasing resiliency
- No learning curve for on-premise FMC users

Key features

- Hybrid management support
- Support up to 1000 devices
- Periodic configuration snapshots
- Easy migration from on-premises FMC to cdFMC
- Real-time Security policy updates for multi-cloud environments
- Secure SaaS applications like O365 using real-time community feeds
- Flexibility between Hybrid and cloud eventing



FMC Deployment: On-Prem, Hybrid, or Cloud



Increasing customer cloud acceptance



Core Principles

Infrastructure as Code



- Automation is the way to go
- Spend time solving new problems
- Increase value of business in the time spent



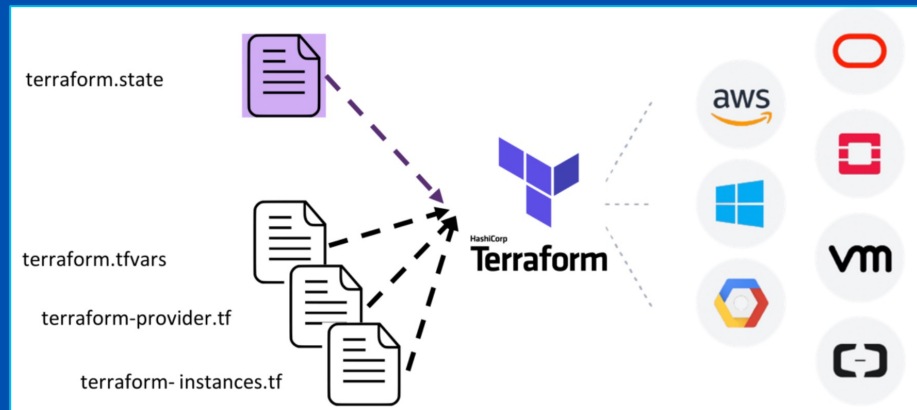
- Failure is Normal
- Studying causes and handling exceptions instead of <<Hotfixes>>



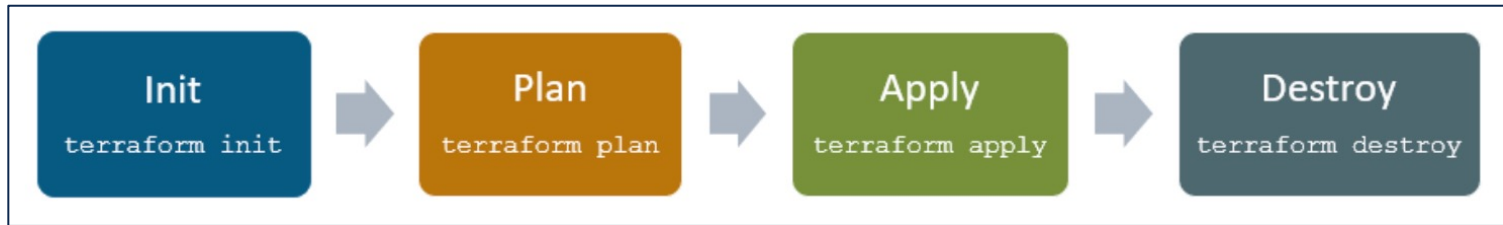
- Continuity at all stages
- Testing, Integration, Deployment, Monitoring and Feedback

Terraform

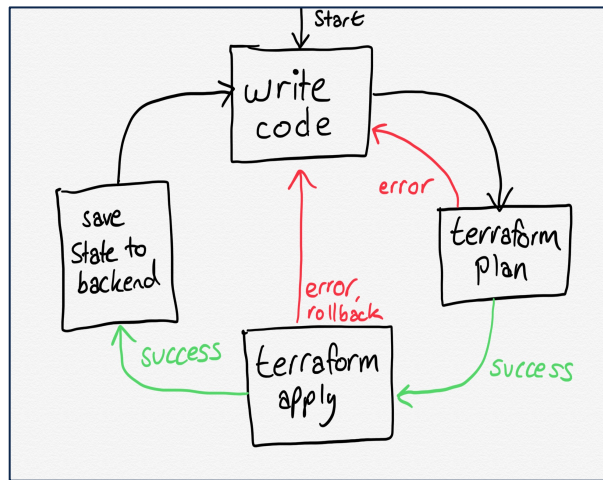
- Open-source infrastructure as Code tool developed by HashiCorp
- Define and Provision the complete infrastructure using **declarative language**
- Supports many providers such as AWS, Azure, GCP, VMware, Cisco, Openstack
- Supports Client only architecture, so no need for additional configuration management on a server



Terraform Lifecycle



- **terraform init** initializes the working directory which consists of all the configuration files
- **terraform plan** is used to create an execution plan to reach a desired state of the infrastructure.
- **terraform apply** then makes the changes in the infrastructure as defined in the plan
- **terraform destroy** is used to delete all the old infrastructure resources, which are marked tainted after the apply phase.



NEW Cloud Resource Page

<https://developer.cisco.com/secure-firewall/cloud-resources/>

Explore Cisco Secure Firewall resources for cloud

Get started with AWS now!

Extensive list of resources to leverage "Infrastructure as Code" for Cisco Secure Firewall in AWS. Utilize validated templates, videos and documentation to ease your deployment.

Use Cases for FTD platform

Multiple FTD Instances in multiple AZ

Multiple FTD Instances in a single AZ

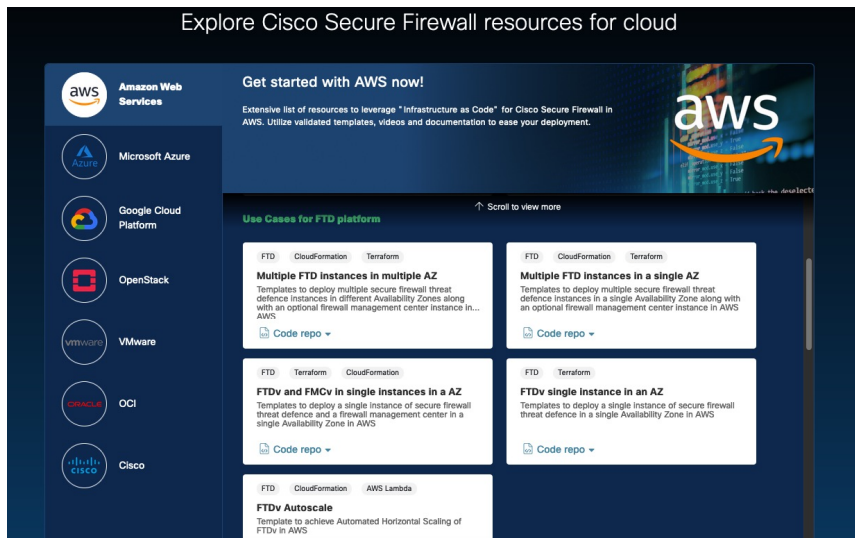
FTDv and FMCv in single instances in a AZ

FTDv single instance in an AZ

FTDv Autoscale

FTDv Autoscale

Template to achieve Automated Horizontal Scaling of FTDv in AWS



Explore Cisco Secure Firewall resources for cloud

Get started with VMware now!

Are you moving your applications to the public cloud? Now there is a cloud-ready firewall that can be automatically deployed and implemented using "Infrastructure as Code" (IaC). This is the process of provisioning and managing the complete infrastructure of a company using machine-readable definition files. The premise is built on a software engineering approach to everyday operations.

Use Cases for FTD Platform

Single FTD Instance

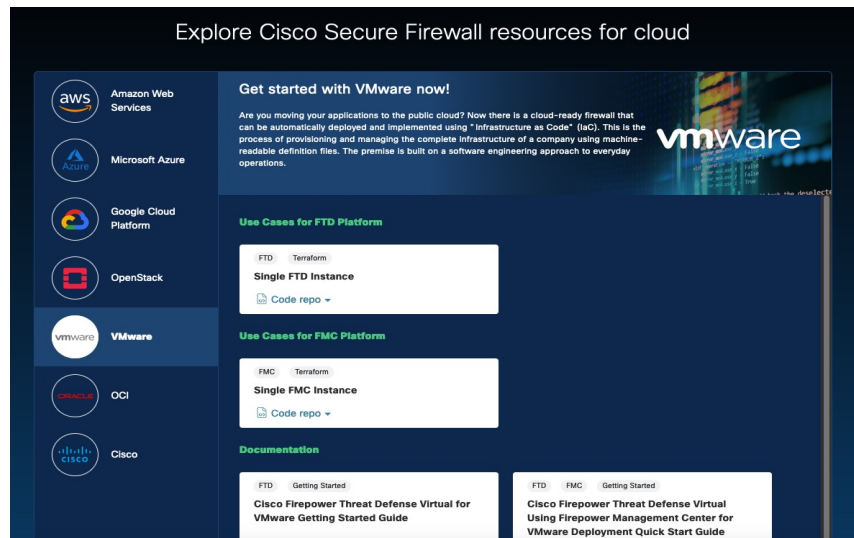
Use Cases for FMC Platform

Single FMC Instance

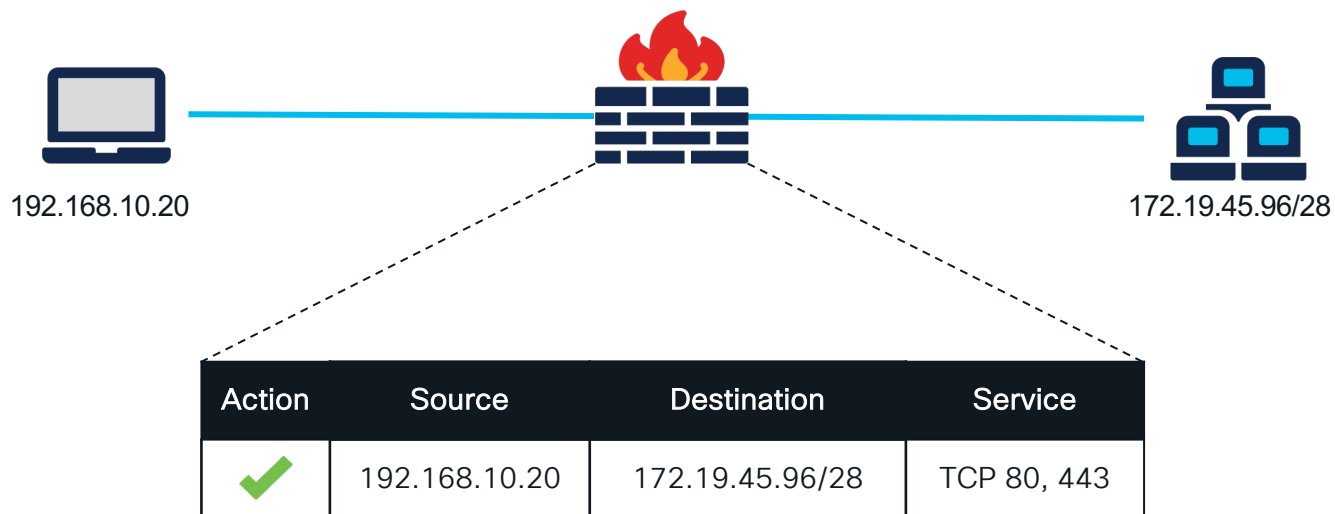
Documentation

Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide

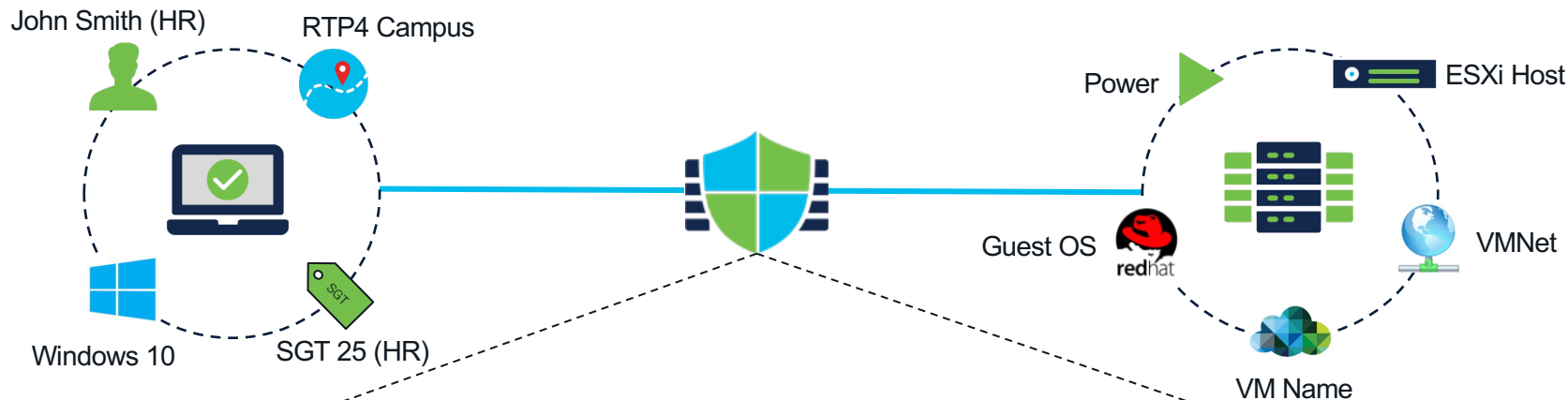
Cisco Firepower Threat Defense Virtual Using Firepower Management Center for VMware Deployment Quick Start Guide



Traditional Firewall Policies



Intent Based Policies

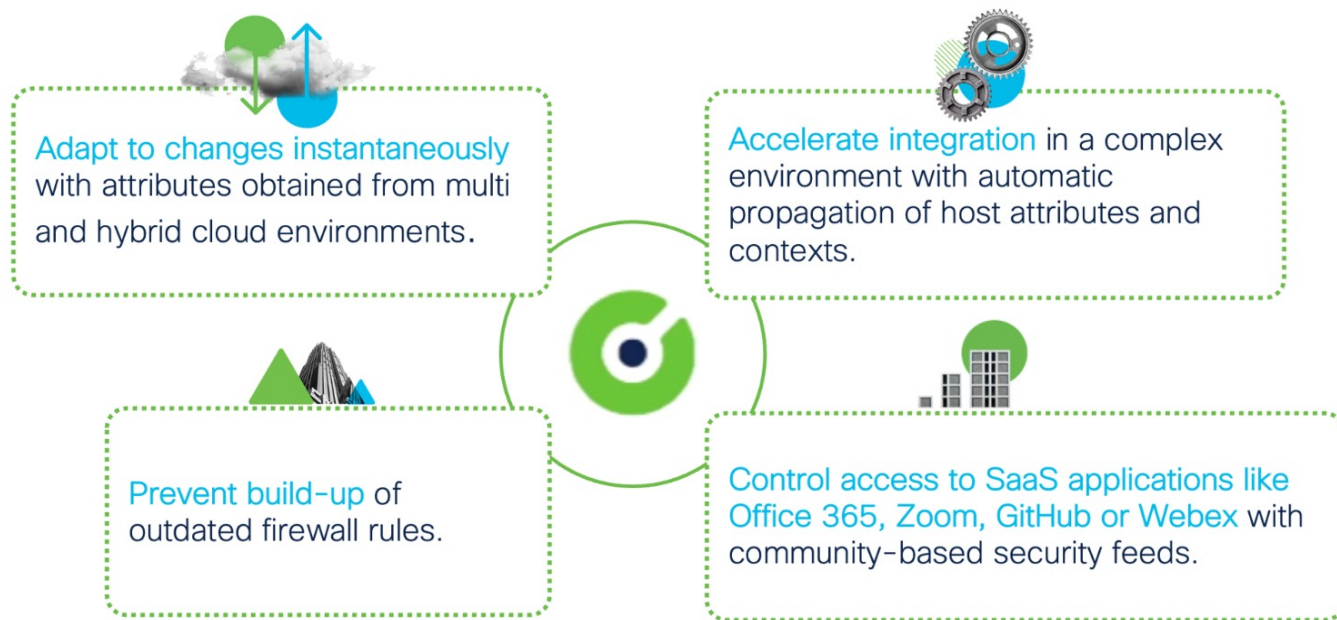


Action	Source	Destination	Service
✓	HR Users in RTP4 Campus on Windows10	PoweredOn servers in UAT VMNet containing HR-Prod in the VM Name	TCP 80, 443

What is CSDAC

- Cisco Secure Dynamic Attribute Connector (CSDAC)
- Imports attribute maps from a dynamic environment
- These dynamic feeds are provided to FMC
- FMC enforces them to the FTDs without policy deployment

Benefits



Supported Connectors

Cloud Connectors



Azure



Azure Service
Tags



vCenter/
NSX-T



Google
Cloud



AWS

Public Feeds Connectors



Office365



GitHub



Webex



Zoom

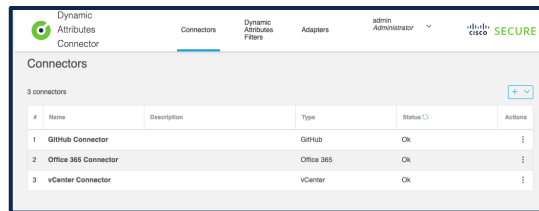


Generic
TXT

Available Form Factors



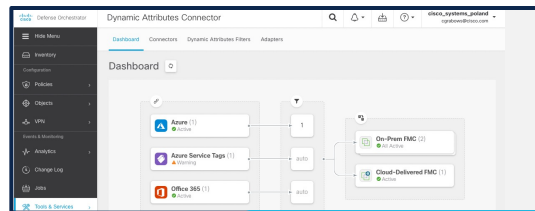
CSDAC
(Linux Machine)



Standalone



CSDAC in CDO's
Tools & Services

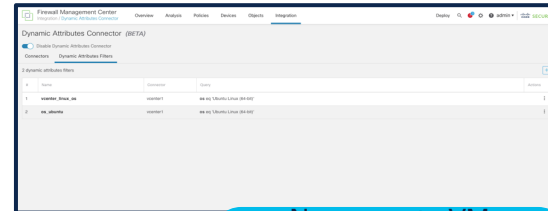


No separate VM
required!!

Cloud Delivered



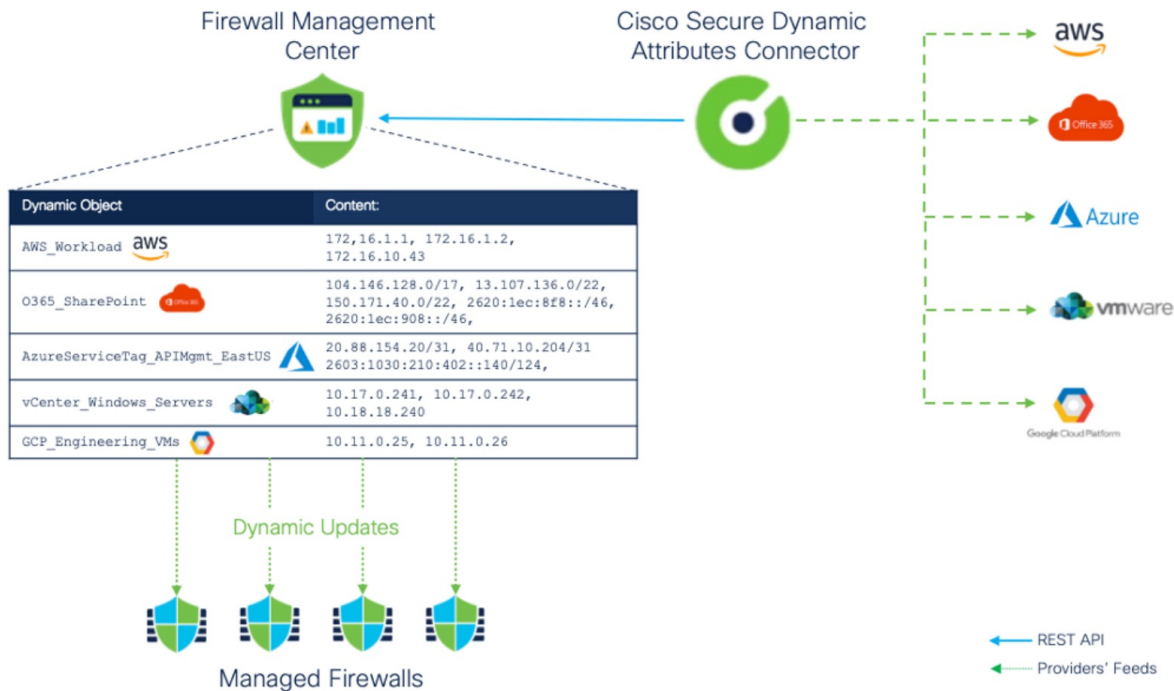
CSDAC in FMC



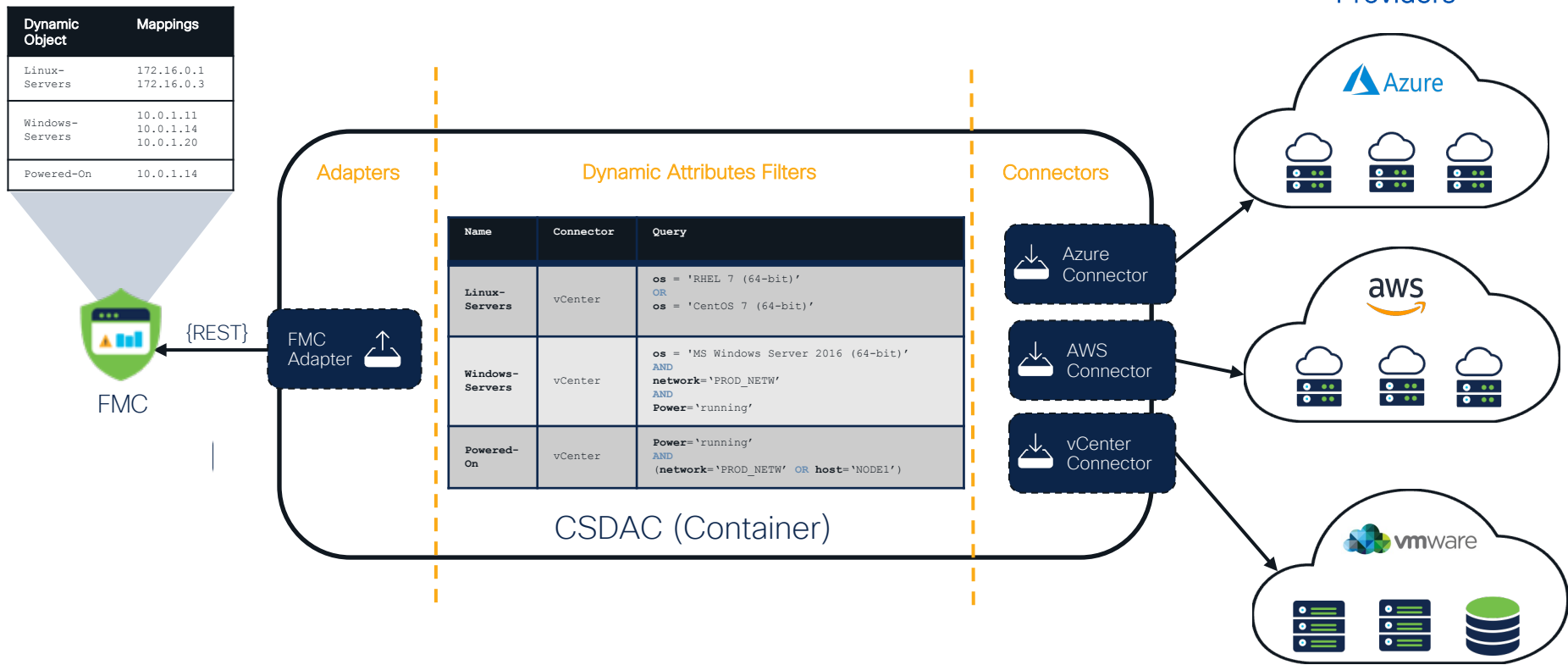
No separate VM
required!!

Built In

CSDAC Working



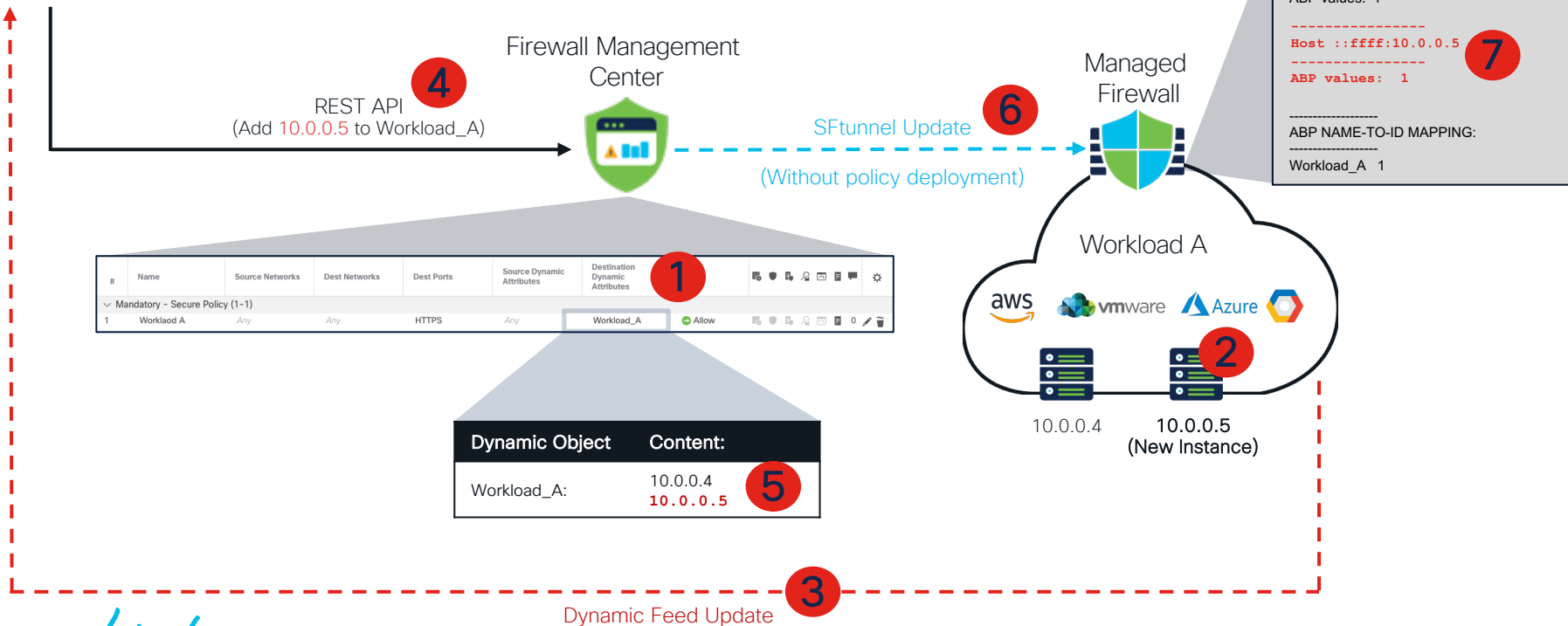
CSDAC Architecture



CSDAC Working



Cisco Secure Dynamic
Attributes Connector



Key Takeaways

- Change policies instantly without firewall deployment
- Control access to SaaS applications
- Available as standalone, CDO and FMC



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic featuring a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from red at the top to blue at the bottom. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, creating a sunburst or starburst effect that blends into the wavy bands.

cisco *Live!*

Let's go

#CiscoLiveAPJC