



Cisco Security

Firepower – Il business enabler per la sicurezza

31 Gennaio 2025

Webinar

Federico Frosini – Business Development Manager – TD SYNEX

Giacomo Casati – Security Presales Specialist – TD SYNEX

Andrea Pezzoni – Security Presales Specialist – TD SYNEX

Francesco Bagnoli – System Architect - Cisco

Agenda

- Cisco Security Overview – *Federico Frosini*
- Cisco Firepower Deep Dive – *Francesco Bagnoli*
- Sinergie ed integrazioni – *Giacomo Casati*
- Q&A

Superare il Silo

La sfida della Cyber Security è uscire dai sistemi chiusi e migrare verso un ECOSISTEMA della sicurezza

I problemi legati al ciclo di vita dei prodotti di Cyber Security:

- Mancanza di risorse e di skill
- Difficoltà di monitoraggio
- Difficoltà a scalare in modo organico
- Molti punti di Fail
- Scarsa visibilità generale
- Lentezza nell'evolvere
- Perimetro in espansione



La risposta a questi problemi è il concetto di Piattaforma:

- Unico stack di prodotti da conoscere e gestire
- Scalabilità basata su cloud e virtualization
- Sicurezza a 360°
- Velocità di implementazione – Soluzione unica
- Sistemi distribuiti e gestiti

Cisco Security Strategy

More products leads to more complexity within your business and IT environment

Exfiltration
Ransomware
Lateral movement
Web threats
Stolen credentials
Spam



76

Average number of security tools per enterprise

78%

Organizations report that high number of security tools is driving cybersecurity complexity*

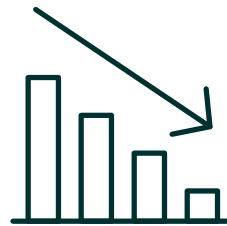
Cisco Security Strategy

Customer top priorities address the challenges



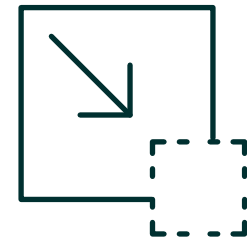
Boost Productivity

Empower users to
do their best work



Optimize Costs

Address inefficiencies



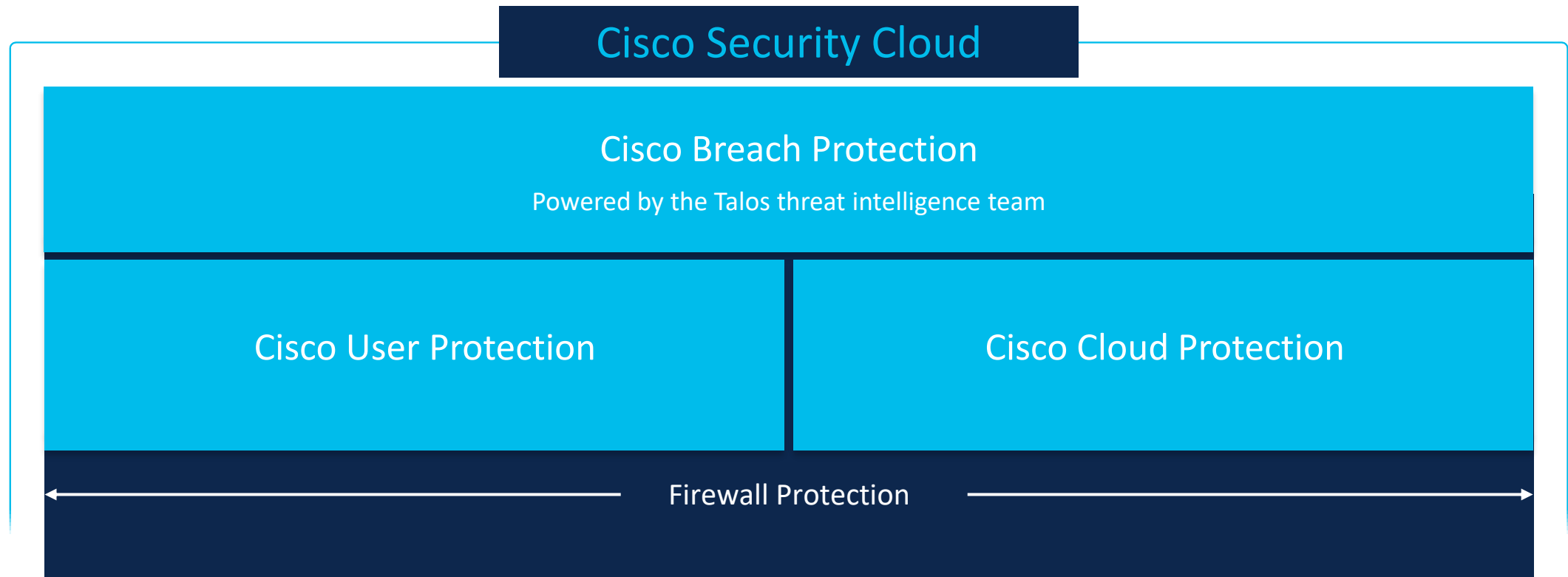
Minimize Risk

Secure your organization

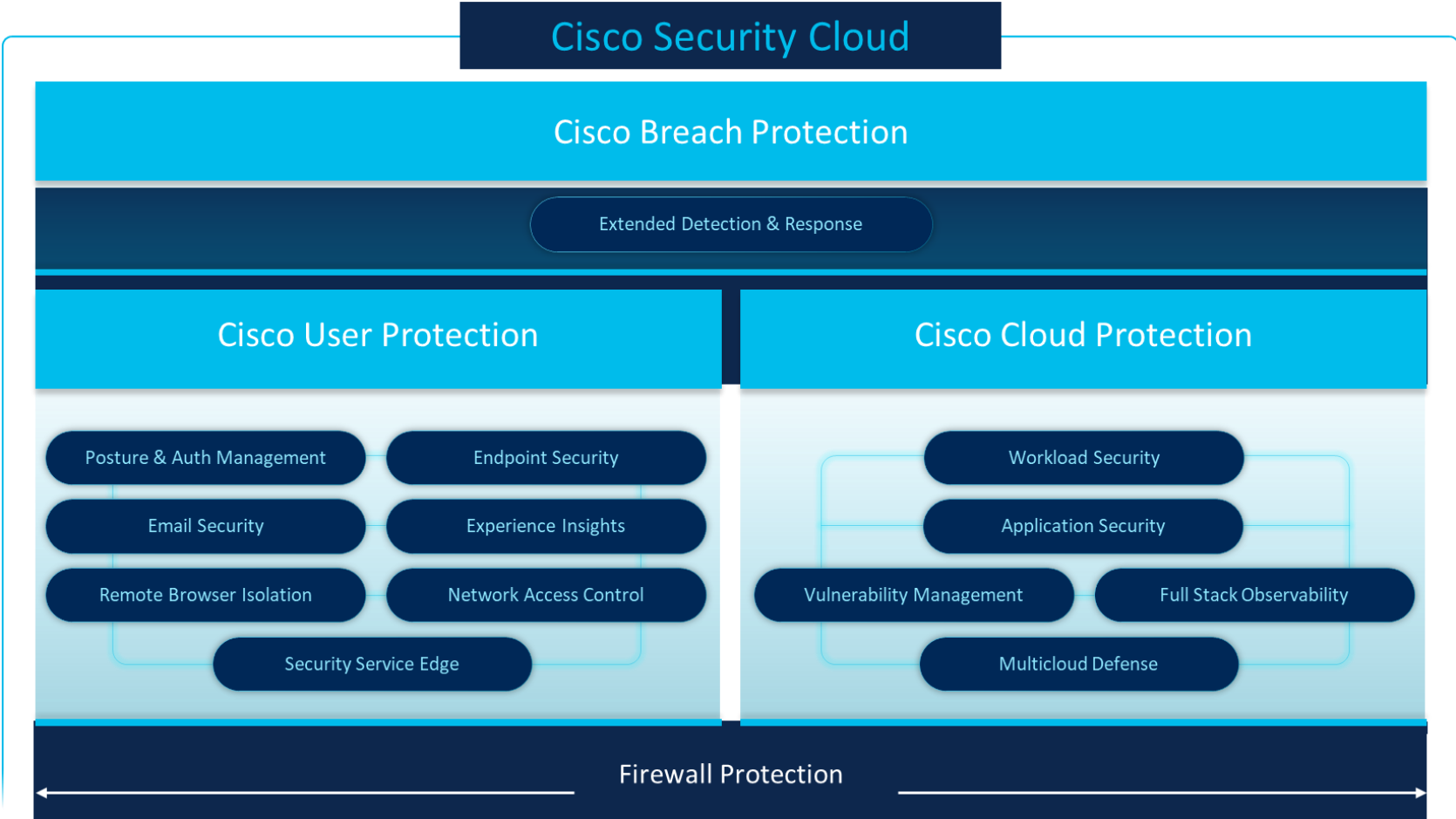
Cisco Security Strategy



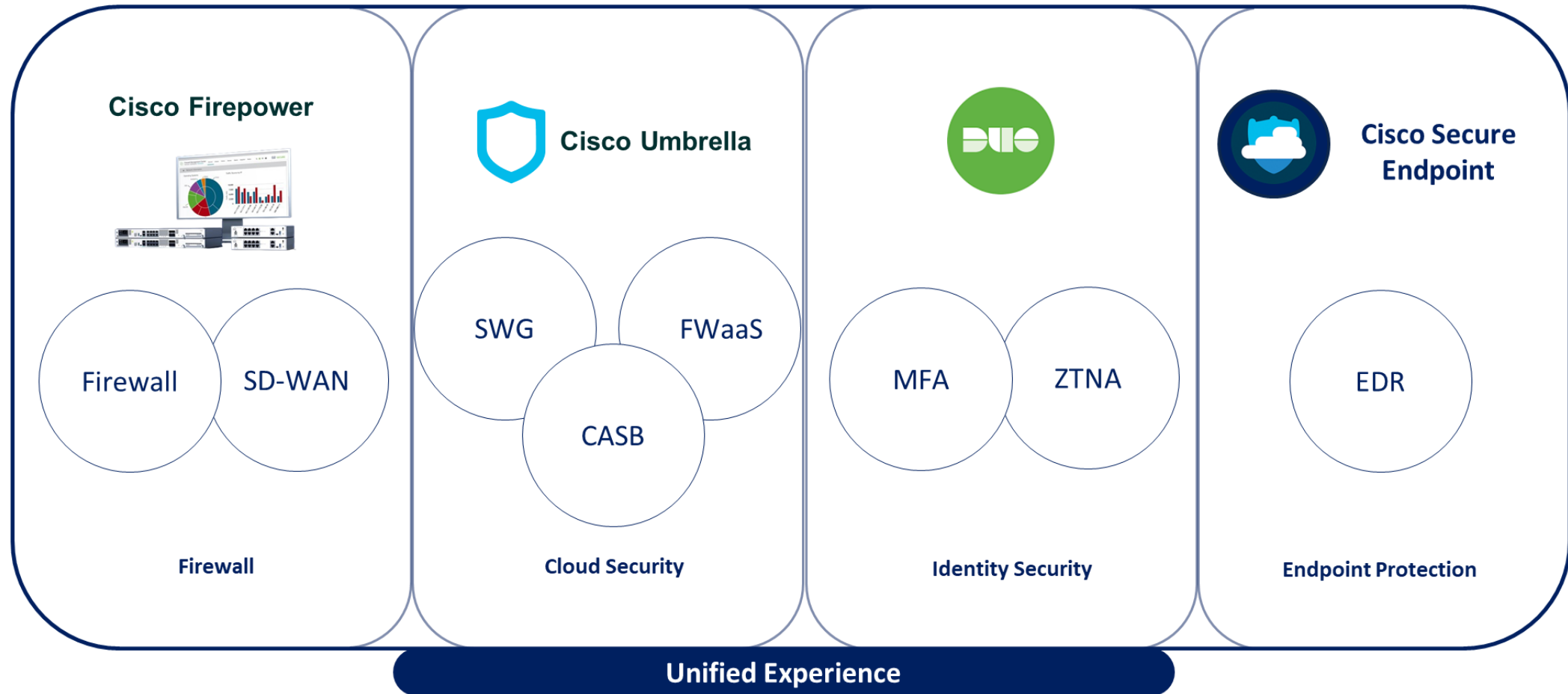
Cisco Security Strategy



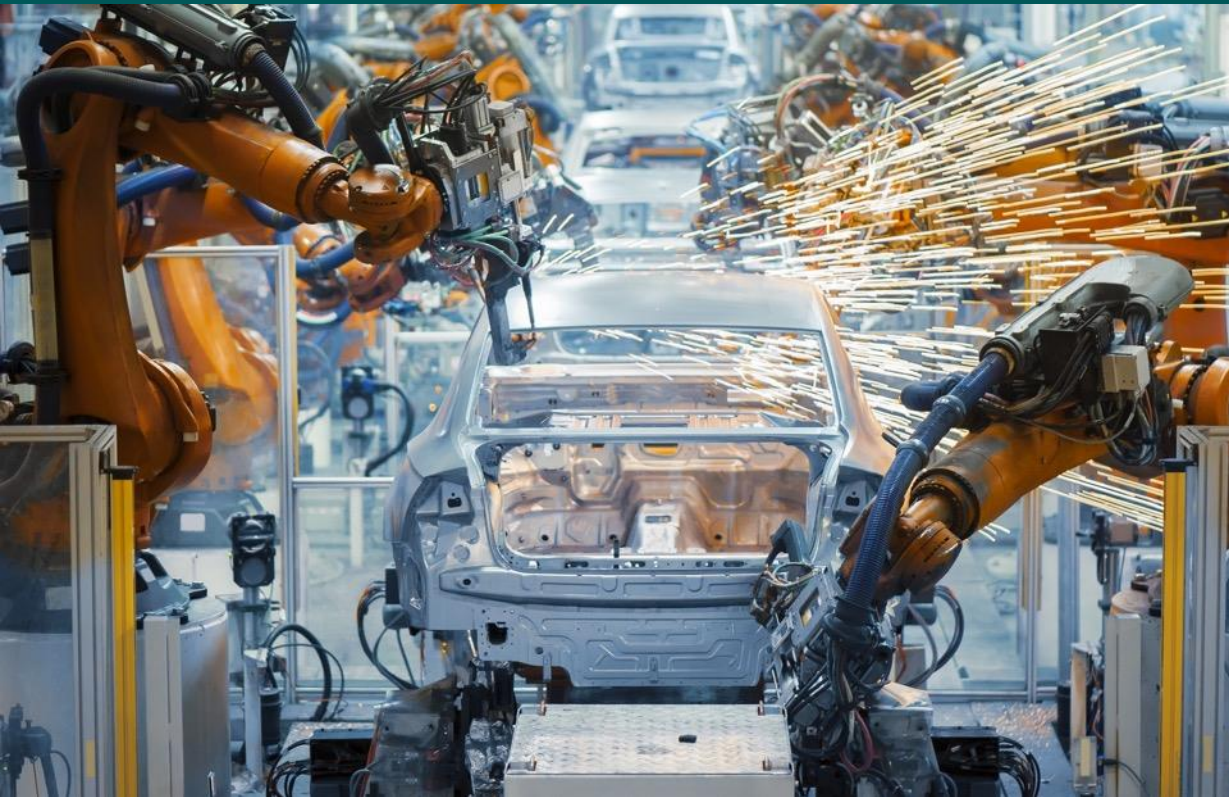
Cisco Security Strategy



Cisco Security for SMB



Industry Digitization Increases the Threat Landscape

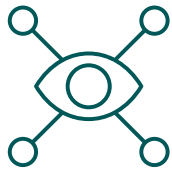


- More connected automation devices
- IoT devices accessing the cloud
- Shadow IT in industrial networks
- Remote access from third parties
- Malware intrusions
- New regulatory requirements

The role of IT is expanding to help secure industrial operations

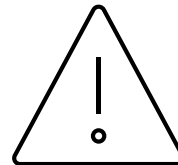
Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT



Visibility

OT asset inventory
Communication patterns



Security Posture

Device vulnerabilities
Risk scoring



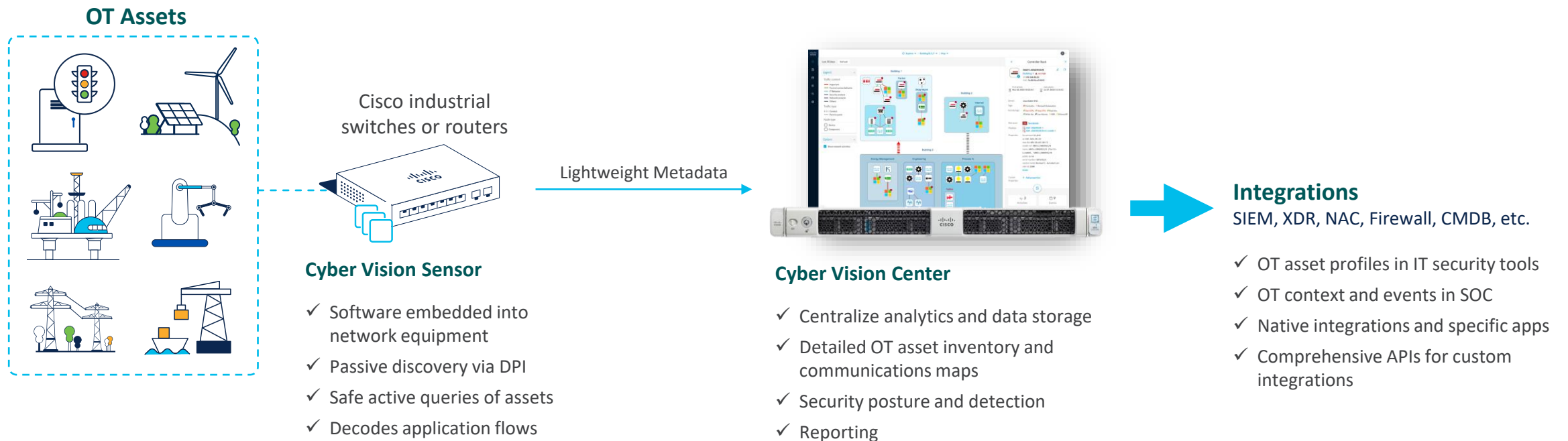
Operational Insights

Track process/device modifications
Record control system events

Context and insights that are foundational to building reliable and secure OT networks

Unique 2-Tier Architecture

OT visibility that can be deployed at scale



OT visibility sensors embedded into network equipment sees more and is easier to scale

Cisco Cyber Vision Portfolio

Cyber Vision Center

Hardware Appliance
UCS based servers with Hardware RAID



- CV-CNTR-M6N
- 24 core CPU
 - 128 GB RAM
 - 3.2TB drives

Software Appliance
Virtual Machines



VMWare ESXi OVA



HyperV VHD

Minimum requirements
Intel Xeon, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces



Amazon Web Services



Microsoft Azure

Minimum requirements
Intel Xeon, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Cyber Vision Sensors



Catalyst IE3300 and IE3400 Switches



Catalyst IE3400HD IP67 Switch



Catalyst IR1101 LTE/5G Gateway



Catalyst IR8300 Multiservice Router



Catalyst IE9300 Rugged Aggregation Switches



Catalyst 9300/9400



IC3000 Industrial Compute

Network-Sensors

Deep Packet Inspection built into network-elements eliminating the need for SPAN

Hardware-Sensor

DPI via SPAN to support brownfield



The bridge to possible

Cisco Secure Firewall: Doubling Down on SD-WAN and AI

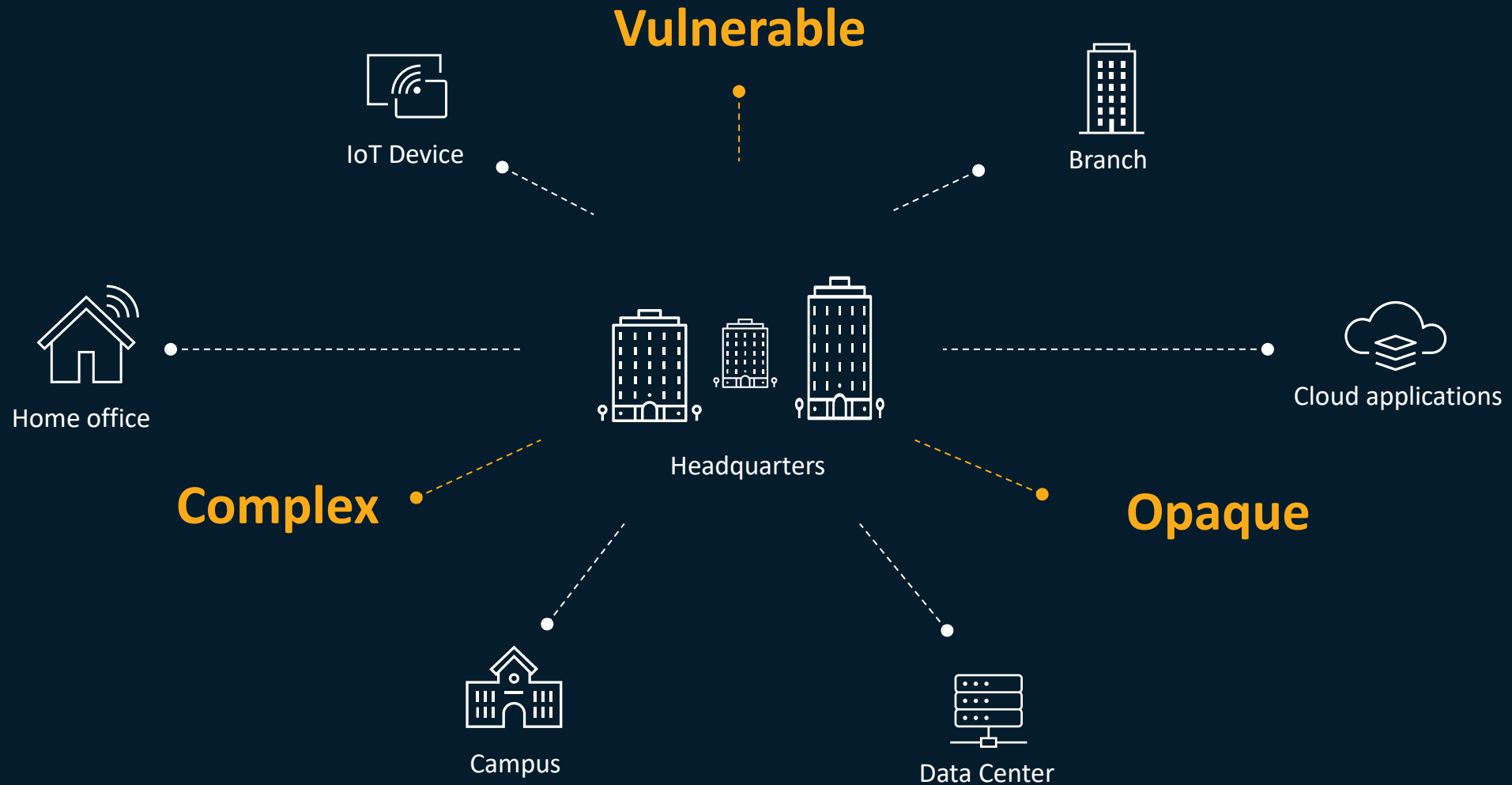
The highest performing, AI-powered, SD-WAN firewall on the market

1200 Series and FTD 7.6 What's New

CISCO *Live!*

#CiscoLive

Your network is expanding and becoming...



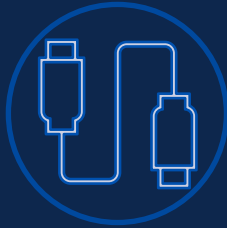
Your network is expanding and becoming...



Challenges of distributed branch offices



More devices to buy, higher CapEx



More devices to onboard, globally



More devices to update & maintain



More people to find, hire & train

Inconsistent

Opaque

Unscalable

Introducing the new Secure Firewall 1200 Series

The highest performing, compact firewall for distributed enterprise branches.

Up to
3x
performance
over rivals

Up to
> 2x
Price/Performance
over rivals



Superior performance in a
compact footprint

Deployment efficiency,
eliminate additional HW

AI/ML-based detection and
management

Introducing the new Secure Firewall 1200 Series

The highest performing, SD-WAN enabled compact firewall for distributed enterprise branches.

Superior performance in a compact footprint

- Boost employee productivity with up to 3x faster speed when connecting to headquarters or cloud apps.
- Power up IoT devices directly with UPoE+, or increase performance of desktop firewall with SFP+ ports.

Deployment efficiency, eliminate additional HW

- Deploy SD-WAN at multiple branch locations faster with built-in onboarding templates and zero-touch provisioning.
- Eliminate the need to purchase, deploy, and manage multiple networking devices at branch.

AI/ML-based detection and management

- AI/ML- driven detection of encrypted malware, common threats, and 0-day vulnerabilities.
- AI Assistant for streamlined firewall operations and policy lifecycle management for on-prem or cloud.

Secure Firewall 1200 Series family

1220 CX

2x1G or10G SFP+
6 Gbps

1210 CP

4x UPoE+
3 Gbps

1210 CE

3 Gbps



Cisco's compact firewalls

Comparison of performance

 **> 3x**
Performance
increase

	1010	1010E
Firewall	0.9 Gbps	0.9 Gbps
IPSec	0.4 Gbps	0.4 Gbps
Ethernet	8 x 1000BASE-T	8 x 1000BASE-T
PoE	-	2 x PoE+

Cisco Secure Firewall hardware portfolio



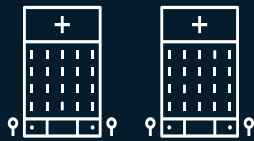
1010



Small and Medium Business (SMB)



1100 Series



Branch Office



1200 Series



Midsize Enterprise



3100 Series



Large Enterprise Datacenter



2022

3100 Series

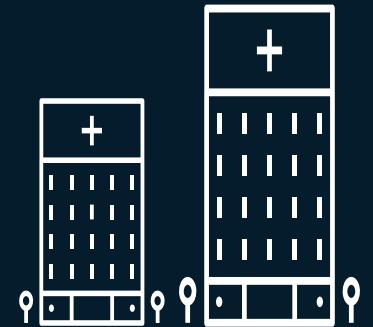


2023

4200 Series



9300 Series



Service Provider



2024

New

New in FTD 7.6

SD-WAN Templates for Deployment

Simplicity

SD-WAN template creation

Easily enable SD-WAN on existing all Cisco firewalls zero-touch provisioning.

The screenshot shows the 'Create VPN Topology' configuration page in the Cisco Firewall Management Center. The page is titled 'Create VPN Topology' and has a search bar in the top right corner. The left sidebar contains navigation options: Home, Overview, Analysis, Policies, Devices (highlighted), Objects, and Integration. The main content area is divided into several sections:

- Topology Name ***: A text input field containing 'SDWAN'.
- VPN Type**: Four radio button options for selecting the VPN topology:
 - SD-WAN Topology** (Selected): Includes a description: 'Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.' Below it is a sub-section 'Select VPN Topology' with a radio button for 'Hub and Spoke'. A 'Prerequisites' link is at the bottom right of this card.
 - Route-Based VPN**: Description: 'Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.' Below it is a sub-section 'Select VPN Topology' with radio buttons for 'Hub and Spoke' and 'Peer to Peer'.
 - Policy-Based VPN**: Description: 'Secures traffic between peers based on a static policy using protected networks.' Below it is a sub-section 'Select VPN Topology' with radio buttons for 'Hub and Spoke', 'Peer to Peer', and 'Full Mesh'.
 - SASE Topology**: Includes a warning message: 'You cannot configure a SASE topology without configuring Umbrella connection settings. More info Configure Umbrella Connector'. A 'Refresh' button is at the bottom right of this card.

At the bottom right of the configuration area, there are 'Cancel' and 'Create' buttons.

SD-WAN template management

Easily enable SD-WAN on all existing Cisco firewalls with zero-touch provisioning.

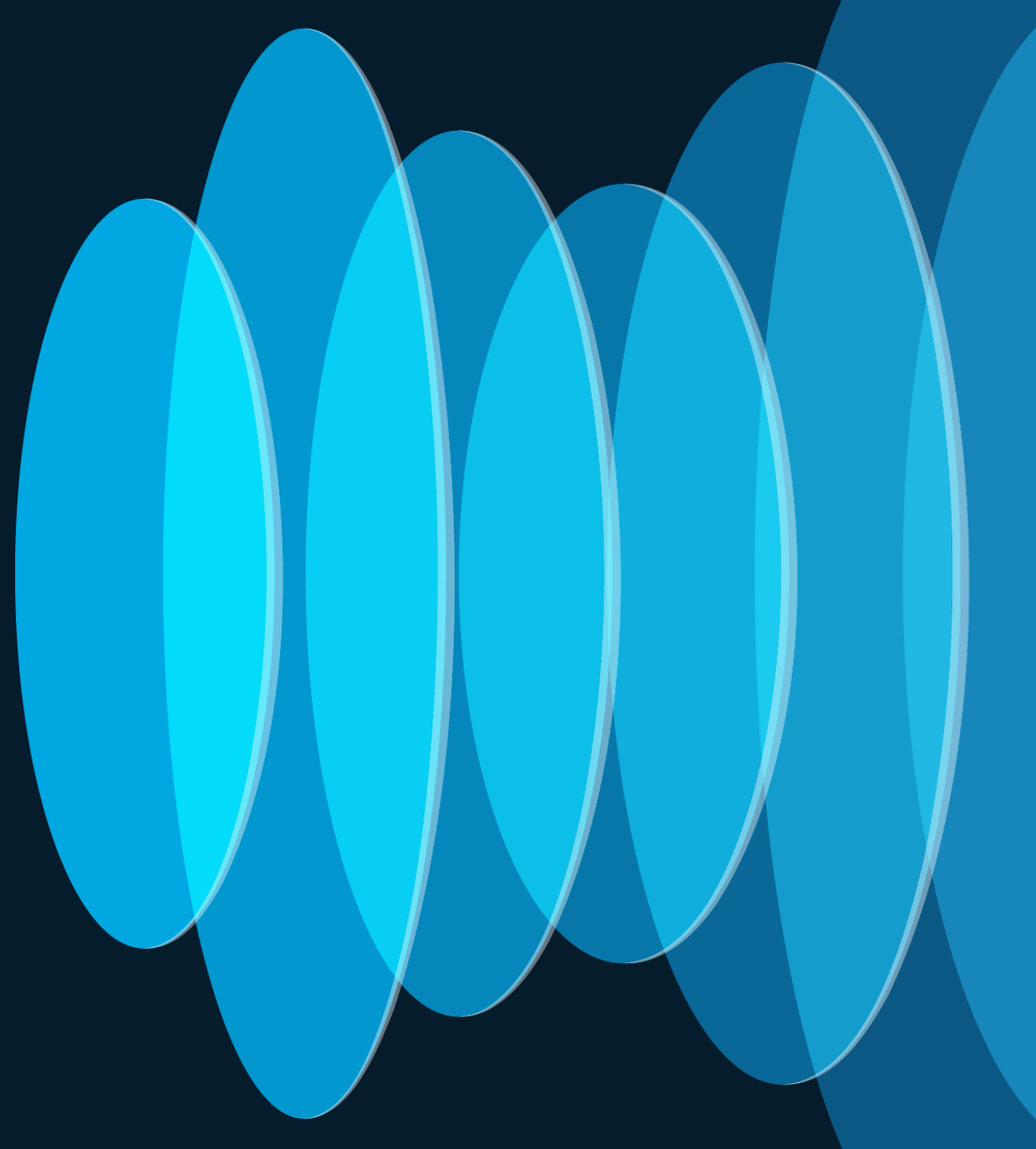
The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo and the text 'Firewall Management Center' and 'Devices / VPN'. The left sidebar contains navigation options: Home, Overview, Analysis, Policies, Devices (highlighted), Objects, and Integration. The main content area is titled 'Devices' and contains a grid of menu items. The 'Template Management' item is highlighted with a blue box. Other items include Device Management, VPN, Troubleshoot, Site To Site, Remote Access, Dynamic Access Policy, File Download, Threat Defense CLI, NAT, QoS, Packet Tracer, Platform Settings, Packet Capture, FlexConfig, Snort 3 Profiling, Certificates, Troubleshooting Logs, Upgrade, Threat Defense Upgrade, and Chassis Upgrade.

The screenshot shows the Cisco Firewall Management Center (FMC) interface with the 'VPN' tab selected. The top navigation bar includes the text 'Template' and 'Interfaces', 'Inline Sets', 'Routing', 'DHCP', 'VPN' (highlighted), 'Template Settings', and 'Associated Devices'. The main content area is titled 'Site-to-Site VPN Connections' and contains a table with two columns: 'VPN Topology' and 'VPN Connections'. The table lists two VPN topologies: 'SDWAN-VPN-64512' and 'SDWAN2-VPN-64512-lsp2'. The 'SDWAN-VPN-64512' entry is highlighted with a blue box. The table also lists the VPN Interface and Local Tunnel IKE ID for each topology.

VPN Topology	VPN Connections
SDWAN-VPN-64512 Type: SD-WAN Topology Role: Spoke	VPN Interface: Outside1-lsp1 Local Tunnel IKE ID: \$LocalIKE-S...
SDWAN2-VPN-64512-lsp2 Type: SD-WAN Topology Role: Spoke	VPN Interface: Outside2-lsp2 Local Tunnel IKE ID: \$LocalIKE-S...

New in FTD 7.6

AI/ML-Enhanced
Detection for 0-day and
Encrypted Threats



Cisco Talos empowers firewalls with AI/ML intelligence



~800B security events/day



~9M emails blocked/hour



~2,000 new samples/minute



~2,000 domains blocked/second



Cisco AI for Security is trained on one of the largest security data sets in the world

60+

Government and law enforcement partnerships

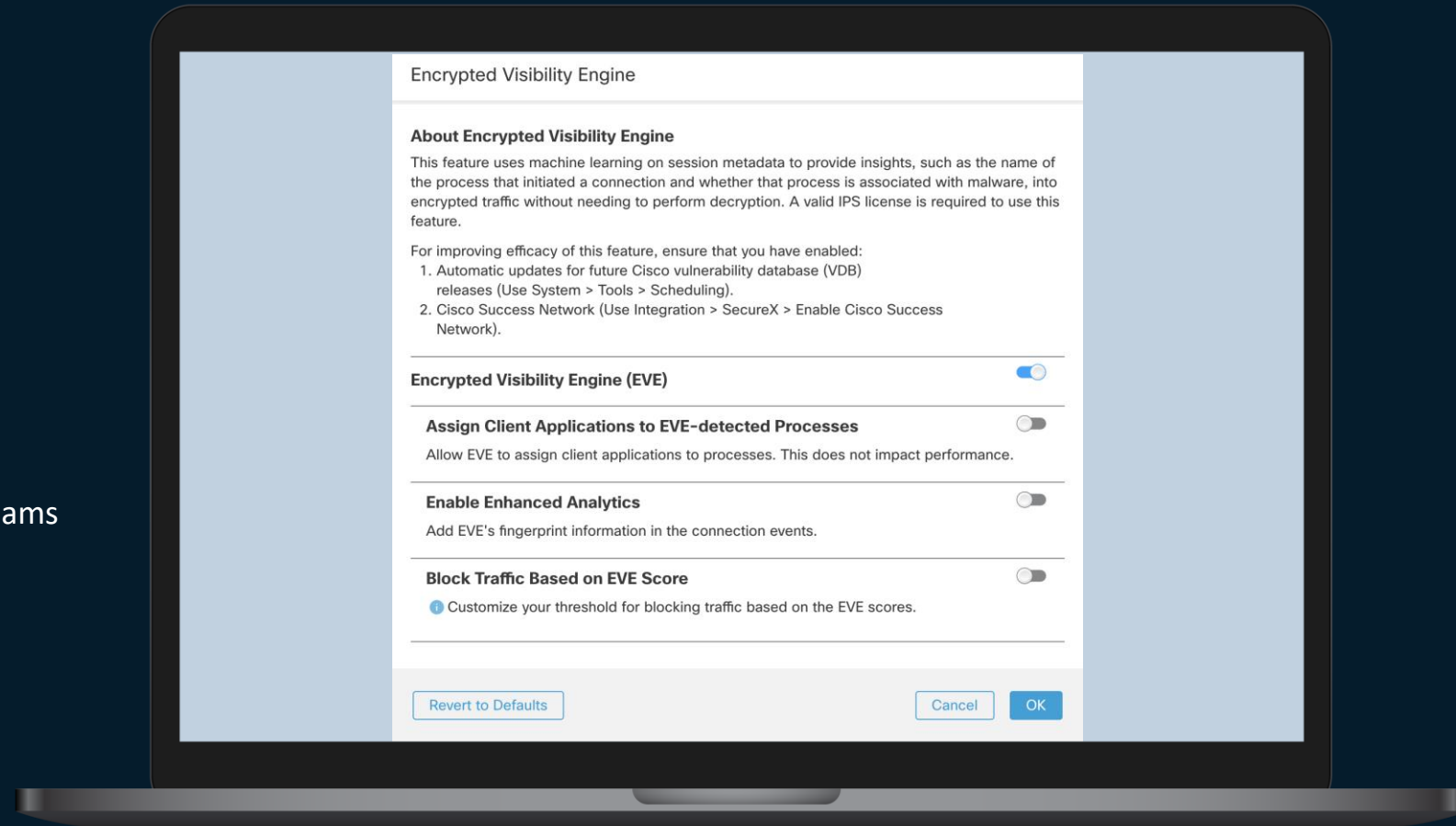
200+

Vulnerabilities discovered per year

Gain control over encrypted threats

Without decryption, encrypted visibility engine 2.0 uses AI/ML to block encrypted threats for thorough security, simplicity, privacy and performance

- Simplify encrypted traffic inspection
- Preserved privacy and compliance
- Accelerate firewall performance
- Application visibility and control in encrypted streams
- TLS 1.3 and QUIC protocol support



SnortML: Zero-day protection

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation bar includes 'Firewall Management Center', 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Deploy'. A search icon and a notification bell with '4' are also present. The user is logged in as 'admin'. Below the navigation bar, there are links for 'Bookmark This Page', 'Create Report', 'Dashboard', 'View Bookmarks', and 'Search'. A 'Predefined Searches' dropdown menu is visible. The main content area is titled 'Events By Priority and Classification' with a '(switch workflow)' link. A date range filter is set to '2024-05-01 00:00:00 - 2024-05-31 15:11:31' with an 'Expanding' status. Under 'Search Constraints', there is an 'Edit Search' link. Three tabs are shown: 'Drilldown of Event, Priority, and Classification', 'Table View of Events', and 'Packets' (which is selected). The 'Event Information' section is expanded, showing the following details:

- Message: (snort_ml) potential threat found in HTTP parameters via Neural Network Based Exploit Detection (411:1:1)
- Time: 2024-05-06 13:28:55
- Classification: Unknown Traffic
- Priority: low
- Ingress Security Zone: BPInline
- Egress Security Zone: BPInline
- Device: 10.7.117.156
- Ingress Interface: 10.20.0.1
- Egress Interface: 10.30.0.1
- Source IP: 10.20.34.251
- Source Port / ICMP Type: 5793 / tcp
- Destination IP: 10.30.10.157
- Destination Port / ICMP Code: 80 (http) / tcp
- HTTP Hostname: 10.30.10.157
- HTTP URI: /joomla/index.php?option=com_saxumastro&view=savedreading&publicid=1'+AND+EXTRACTVALUE(66,CONCAT(0x5c,CONCAT_WS(0x203a20,USER()),DATAB.

- A machine learning detection engine detecting known vulnerability types
- Proactive blocking of 0-day exploits
- Identifies variations of attacks

Generative AI application detector

Eliminate risks of exposing sensitive information into GenAI platforms.

Firewall Management Center
Policies / Application Detectors

Search Deploy nazmul

Import/Export | Custom Product Mappings | User Third-Party Mappings

Filters: Category: generative ai

Create Custom Detector

Name	Detection Type	Details	Port(s)	Type	State
AutoGPT Provides a generative AI platform to autonomously complete a range of tasks.	TCP	AutoGPT		Basic	On
Bing AI Offers an AI based search engine.	TCP	Bing AI		Basic	On
ChatGPT An AI which is trained to follow an instruction in a prompt and provide a detailed response.	TCP	ChatGPT		Basic	On
ChatGPT An AI which is trained to follow an instruction in a prompt and provide a detailed response.	TCP	ChatGPT		Basic	On
Chatsonic Offers a conversational AI chatbot.	TCP	Chatsonic		Basic	On
CodeGeex Provides an AI-based coding assistant.	TCP	CodeGeex		Basic	On

"Through 2025, generative AI will cause a spike in the cybersecurity resources required to secure it, causing more than a 15% incremental spend on application and data security."

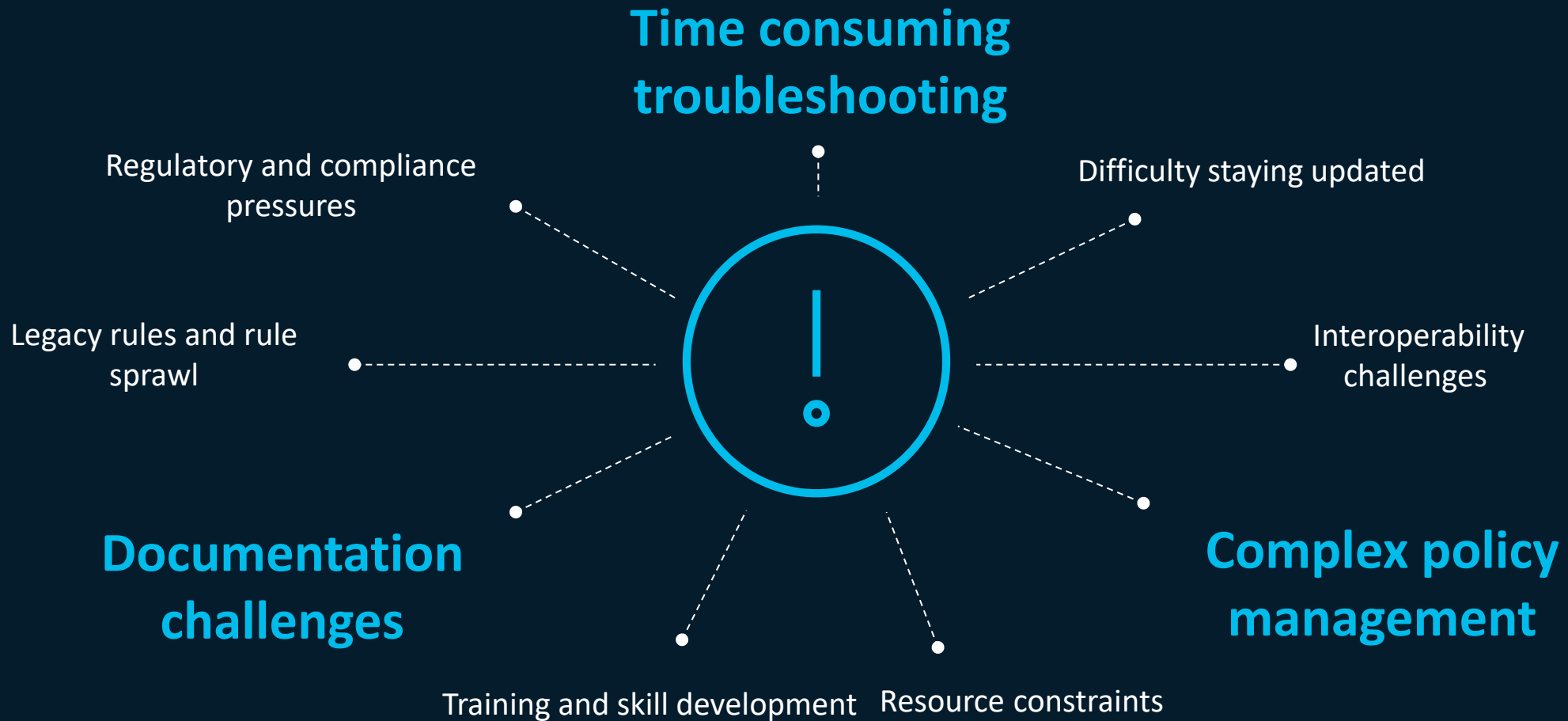
-Gartner

Supports detection and control of 70+ GenAI applications.

New in FTD 7.6

AI Assistant on FMC for Operational
Simplicity

Firewall management is a nightmare!



Cisco AI Assistant for Security now on FMC

Assist

Policy and reporting

Find and report information on policies for faster queries, auditing, and reporting

Augment

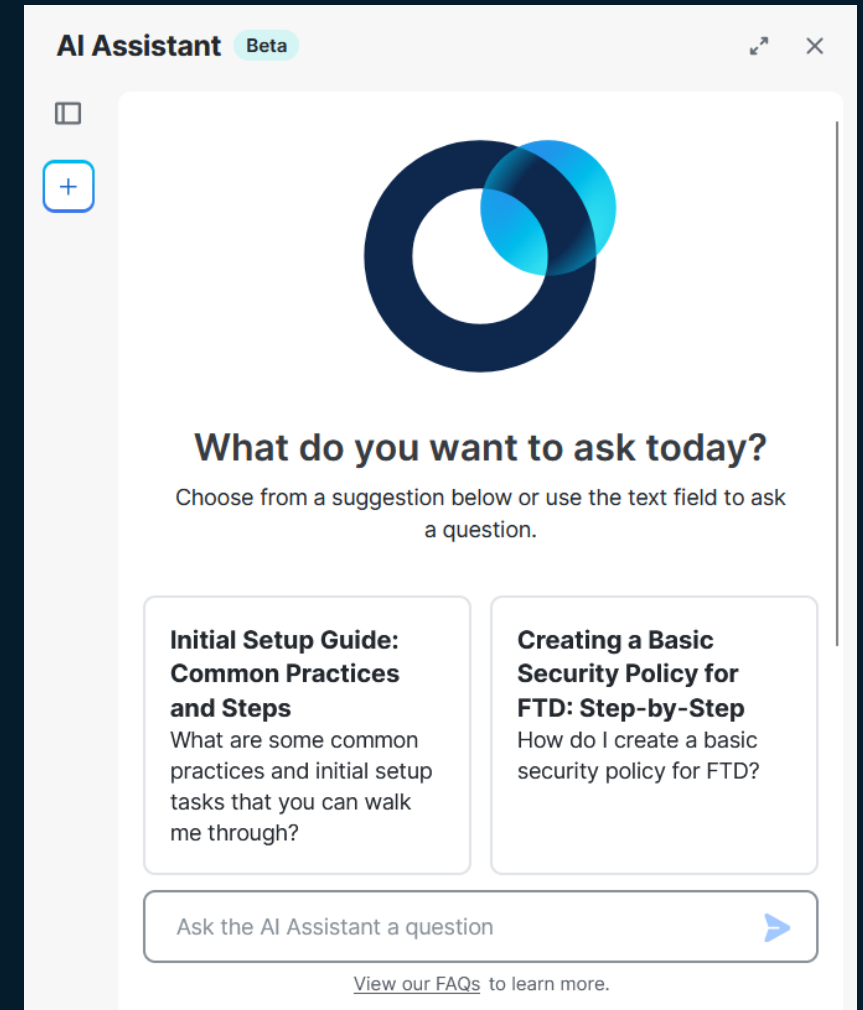
Troubleshooting and detection

Amalgamate all user guides for expedited resolution

Automate

Policy lifecycle management

Find and fix firewall rule misconfigurations for improved security and performance



Available on all FMC solutions from
FTD software version 7.6

Security Cloud Control (formerly CDO)

AI-Native architecture for:

Simplified operations

Enhanced security

Improved clarity

CISCO *Live!*

The dashboard is titled "Top Insights & Alerts" and features a sidebar with navigation options: Dashboard, Inventory, Policies, Objects, VPN, and Troubleshoot and Logs. The main content area is divided into several sections:

- Top Insights & Alerts:** Three cards showing alerts such as "Elephant flow spike observed", "Risky Users accessing privileged apps", and "1% Decrypted traffic towards internet".
- Top Actions:** A "Policy Optimizer" card showing 18263 Rules with anomalies, 5723 Shadowed, and a donut chart for 30524 Total Rules.
- Top Information:** A "Workload Protection Status" card showing 400 Total Assets, 20k Vulnerable, 320k Protected, and 60k Improvements Recommended.
- Risk & Vulnerabilities:** A card showing 14 High and Medium vulnerabilities not covered, with a risk breakdown of 89 Total, 10 High Risk, 4 Medium Risk, and 75 Low Risk.
- Top Risky Destinations Allowed:** A table listing applications like AceProject, AD DSROL, and Contently with their business relevance and categories.

App Name	Business Relevance	Category
AceProject	Very High	email
AD DSROL	Very High	CMR
Contently	Very High	business

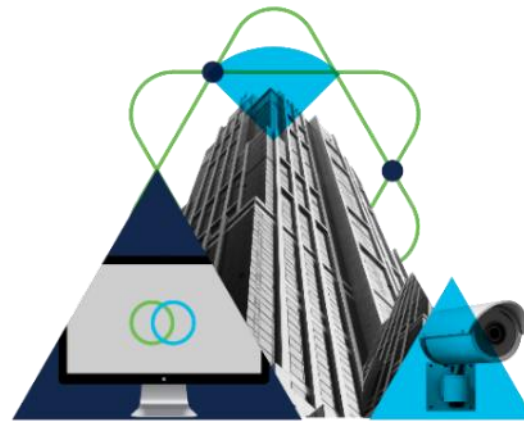
Cisco Secure Zero Trust

A comprehensive approach to securing all access across your people, applications, and environments.



Workforce

Ensure only the right users and secure devices can access applications.



Workplace

Secure all user and device connections across your network, including IoT.

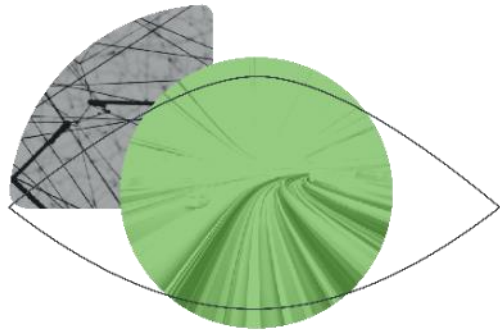


Workloads

Secure all connections within your apps, across multi-cloud.

The Foundations of Zero Trust in Your **Workplace**

Visibility



Grant the right level of network access to users across domains



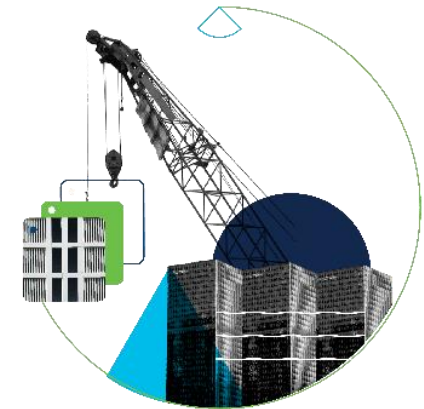
Segmentation



Shrink zones of trust and grant access based on least privilege



Containment



Automate containment of infected endpoints and revoke network access

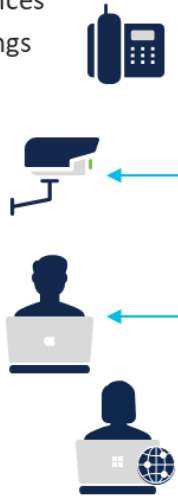
ISE Provides Zero Trust for the Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things



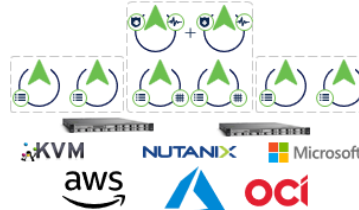
Network Devices

- Switches
- WLCs / APs
- VPN



Cisco ISE

- Shared or Distributed
- VM/Appliance/Cloud
- Up to 2M Endpoints
- RADIUS and TACACS



Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA



Security Services

- Cloud Analytics
- Secure Firewall
- Partners



See It

Secure It

Share It

ISE Capabilities for Zero Trust from Workplace



Establish Trust

- User/Device Authentication
- MFA thru Integrations
- Profiling
- Posture + Context
- Guest
- BYOD Onboarding



Enforce Trust-Based Access

- Network based Authorization Policies
- Micro-segmentation
- Compliance-based CoA
- Device Administration with TACACS+



Continuously Verify Trust


- Integrations :
- Threat Detection
 - Behavior Analysis
 - Vulnerability Assessment













Respond to Change in Trust

- RADIUS Change of Authorization (CoA)
- Adaptive Network Control (ANC)

Why Customers Buy ISE



	Device Administration	TACACS+ Allows for secure, identity-based access to the network devices	https://cs.co/ise-tacacs
	Secure Access	Secure wired, wireless, or VPN access using industry standard protocols RADIUS and 802.1X	https://cs.co/ise-wired
	Guest Access	Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options	https://cs.co/ise-guest
	Asset Visibility	Use the probes in ISE and Cisco devices to classify endpoints and authorize them	https://cs.co/ise-profiling
	Compliance & Posture	Use agentless posture, Cisco Secure Client, MDM, or EMM to check endpoints' posture	https://cs.co/ise-posture
	Context Exchange	Integrate applications and vendors with ISE for endpoint identity, context, and automated Enforcement	https://cs.co/ise-pxgrid
	Segmentation	Group-based Policy with Security Group Tags (SGT) and Security Group ACLs (SGACL) instead of VLAN/ACLs	https://cs.co/segmentation-resources
	Cisco Catalyst Center	ISE integrates with Catalyst Center to automate the network fabric and policies using SDA	https://cs.co/ise-ccc
	EMM/MDM	Endpoint Management is required for provisioning endpoints with certificates and controls for secure network access	https://cs.co/ise-mdm
	Threat Containment	Use Threat Analysis tools to grade an endpoint's threat score and automatically quarantine it	https://cs.co/ise-tcnac









Context Build, Summarize, Exchange with pxGrid

Visibility and Access Control

ISE builds context and applies access control restrictions to users and devices

-  Threat Intelligence
-  Mobility Services Engine
-  System managers
-  Mobile Device Managers
-  Directory Services
-  Vulnerability Scanners

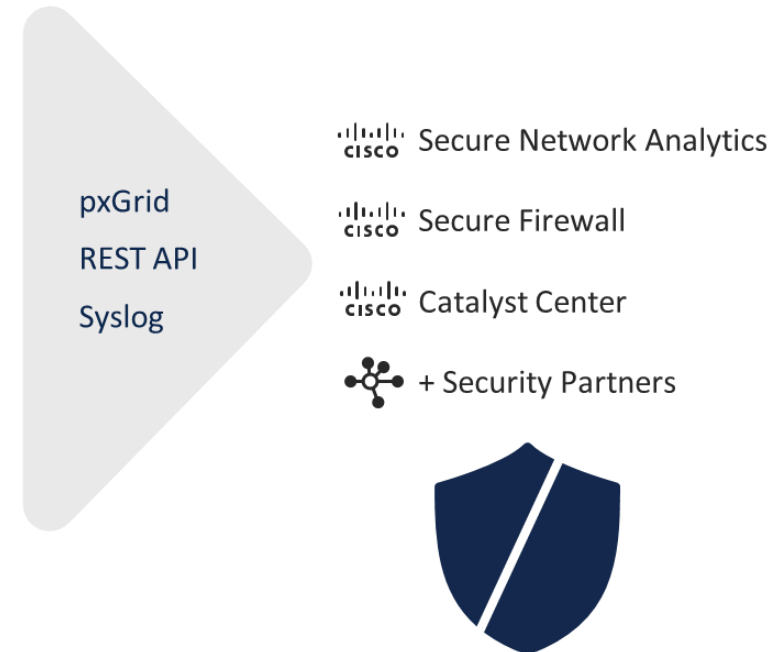


-  Who
-  What
-  When
-  How
-  Where
-  Posture
-  Threat
-  Vulnerability

 Security Group Tag (SGT)

Context Reuse

by eco-system partners for analysis & control



ISE Cisco Security Technical Alliance (CSTA) Partners

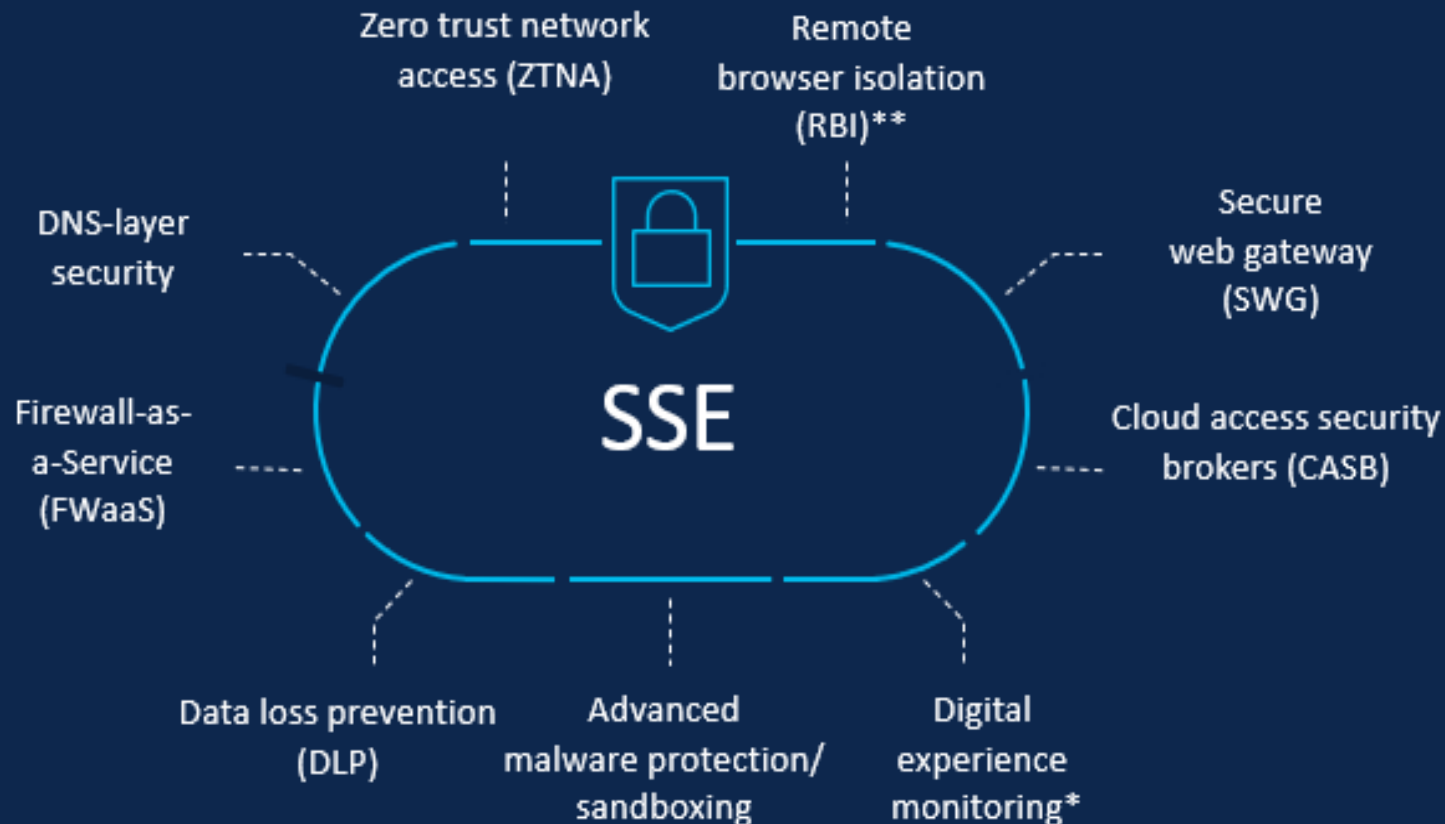
<p>ALEPH NULA</p> <p>Cisco Secure and Aleph NULA Learn more about Cisco Secure and Aleph NULA</p>	<p>ABSOLUTE</p> <p>Cisco Secure and Absolute Learn more about Absolute</p>	<p>CLARITY</p> <p>Cisco Secure and Clarity Learn more about Cisco and Clarity</p>	<p>Culinda</p> <p>Cisco Secure and Culinda Learn more about Cisco Secure and Culinda</p>	<p>CYBERARK</p> <p>Cisco Secure and CyberArk Learn more about Cisco Secure and CyberArk</p>	<p>Huntman</p> <p>Cisco Secure and Huntman Learn more about Cisco and Huntman</p>	<p>IBM</p> <p>Cisco Secure and IBM Max5360 Learn more about Cisco and IBM Max5360</p>	<p>IBM</p> <p>Cisco Secure and IBM QRadar Learn more about Cisco and IBM QRadar</p>	<p>NETWITNESS</p> <p>Cisco Secure and NetWitness NetWitness, an IBM® Cloud Business, is a comprehensive XDR solution that accelerates threat detection and response.</p>	<p>NOOVUS INFINITY INNOVATION</p> <p>Cisco Secure and Noovus Learn more about Cisco and Noovus</p>	<p>NOZOMI NETWORKS</p> <p>Cisco Secure and Nozomi Learn more about Cisco and Nozomi</p>	<p>SOPHOS</p> <p>Cisco Secure and Sophos Learn more about Cisco and Sophos</p>	<p>SOTI</p> <p>Cisco Secure and Soti Learn more about Cisco and Soti</p>	<p>splunk</p> <p>Cisco Secure and Splunk SIEM Learn more about Cisco and Splunk SIEM</p>	
<p>ACALVIO</p> <p>Cisco Secure and Acalvio Learn more about Cisco Secure and Acalvio</p>	<p>aws</p> <p>Cisco Secure and Amazon Web Services (AWS) By focusing on security, simplicity, and transformation, Cisco Secure solutions on AWS help protect and secure customer workloads on AWS.</p>	<p>MICRO FOCUS</p> <p>Cisco Secure and ArcSight Learn more about Cisco and ArcSight</p>	<p>CyberMDX A FORESCOUT COMPANY</p> <p>Cisco Secure and CyberMDX Learn more about Cisco Secure and CyberMDX</p>	<p>CYLERA</p> <p>Cisco Secure and Cylera Learn more about Cisco Secure and Cylera</p>	<p>Cynerio</p> <p>Cisco Secure and Cynerio Learn more about Cisco Secure and Cynerio</p>	<p>illusive</p> <p>Cisco Secure and Illusive Learn more about Cisco Secure and Illusive</p>	<p>Infoblox</p> <p>Cisco Secure and Infoblox Learn more about Cisco and Infoblox</p>	<p>ivanti</p> <p>Cisco Secure and Ivanti Mobilize Learn more about Cisco Secure and Ivanti Mobilize</p>	<p>NUTANIX</p> <p>Cisco Secure and Nutanix Learn more about Cisco and Nutanix</p>	<p>nuansa</p> <p>Cisco Secure and Nuansa Learn more about Cisco and Nuansa</p>	<p>ordr</p> <p>Cisco Secure and Ordr Learn more about Cisco Secure and Ordr</p>	<p>sumo logic</p> <p>Cisco Secure and Sumo Logic Learn more about Cisco Secure and Sumo Logic</p>	<p>SWIMLANE</p> <p>Cisco Secure and Swimlane Swimlane is the leader in cloud-scale, low-code security automation. Supporting use cases beyond the SOC, it enables security teams to overcome process and</p>	<p>Symantec A Division of Broadcom</p> <p>Cisco Secure and Symantec Learn more about Cisco and Symantec</p>
<p>ARMIS</p> <p>Cisco Secure and Armis Learn more about Cisco Secure and Armis</p>	<p>asimily</p> <p>Cisco Secure and Asimily Learn more about Cisco Secure and Asimily</p>	<p>Attivo NETWORKS A SentinelOne Company</p> <p>Cisco Secure and Attivo Networks Learn more about the Attivo Networks</p>	<p>digitaldefense by InSentry</p> <p>Cisco Secure and Digital Defense Learn more about Cisco Secure and Digital Defense</p>	<p>elastic</p> <p>Cisco Secure and Elastic Elastic Security unifies SIEM, endpoint security, and cloud security on an open platform, enabling teams to prevent, detect, and respond to threats.</p>	<p>elastica</p> <p>Cisco Secure and Elastica Learn more about Cisco and Elastica</p>	<p>jamf</p> <p>Cisco Secure and Jamf Learn more about Cisco and Jamf</p>	<p>LINKSHADOW COMBAT THE DARK</p> <p>Cisco Secure and Linkshadow Learn more about Cisco Secure and Linkshadow.</p>	<p>LiveAction</p> <p>Cisco Secure and LiveAction Learn more about Cisco and LiveAction</p>	<p>panaseer</p> <p>Cisco Secure and Panaseer Learn more about Cisco and Panaseer</p>	<p>Pingidentity.</p> <p>Cisco Secure and Ping Identity Learn more about Cisco Secure and Ping Identity</p>	<p>Qualys.</p> <p>Cisco Secure and Qualys Learn more about Cisco and Qualys</p>	<p>TIBCO</p> <p>Cisco Secure and TIBCO Learn more about Cisco Secure and TIBCO</p>	<p>tangoe</p> <p>Cisco Secure and Tangoe Learn more about Cisco Secure and Tangoe</p>	<p>tenable</p> <p>Cisco Secure and Tenable Learn more about Cisco and Tenable</p>
<p>BAYSHORE NETWORKS</p> <p>Cisco Secure and Bayshore Learn more about Cisco and Bayshore</p>	<p>BlackBerry</p> <p>Cisco Secure and BlackBerry Learn more about the BlackBerry</p>	<p>BLUSAPPHIRE INTELLIGENT CYBER DEFENSE</p> <p>Cisco Secure and Blusapphire Learn more about Cisco Secure and Blusapphire</p>	<p>Envoy</p> <p>Cisco Secure and Envoy Learn more about Cisco Secure and Envoy</p>	<p>exabeam</p> <p>Cisco Secure and Exabeam Exabeam is the next-gen SIEM and XDR leader, redefining how security teams use analytics and automation to solve threat detection, investigation, and</p>	<p>ExtraHop</p> <p>Cisco Secure and ExtraHop Learn more about Cisco Secure and ExtraHop</p>	<p>LogRhythm</p> <p>Cisco Secure and LogRhythm LogRhythm provides intelligence and analytics technologies that empower organizations around the globe to rapidly detect, respond to, and neutralize damaging cyber</p>	<p>MEDIGATE by Clouby</p> <p>Cisco Secure and Medigate Learn more about Cisco Secure and Medigate.</p>	<p>MICRO FOCUS</p> <p>Cisco Secure and Micro Focus ArcSight Learn more about Cisco and Micro Focus ArcSight</p>	<p>Radiflow</p> <p>Cisco Secure and Radiflow Learn more about Cisco ISE and Radiflow</p>	<p>RAPID7</p> <p>Cisco Secure and Rapid7 InsightConnect Learn more about Cisco and Rapid7 InsightConnect</p>	<p>RAPID7</p> <p>Cisco Secure and Rapid7 InsightVM Learn more about Cisco and Rapid7 InsightVM</p>	<p>TRAPX SECURITY</p> <p>Cisco Secure and TrapX Learn more about Cisco and TrapX</p>	<p>Trellix</p> <p>Cisco Secure and Trellix DXL Learn more about Cisco and Trellix DXL</p>	<p>Trellix</p> <p>Cisco Secure and Trellix SkyHigh Learn more about Cisco and Trellix SkyHigh</p>
<p>certego</p> <p>Cisco Secure and Certego Certego provides comprehensive and managed security incident response services.</p>	<p>CHECK POINT</p> <p>Cisco Secure and Check Point Learn more about Cisco Secure and Check Point</p>	<p>citrix</p> <p>Cisco Secure and Citrix Learn more about Cisco Secure and Citrix</p>	<p>FIREMON</p> <p>Cisco Secure and Firemon Learn more about Cisco and Firemon</p>	<p>FORTINET</p> <p>Cisco Secure and Fortinet Fortinet helps CSTAs to respond to cybersecurity incidents with its Incident Response, Vulnerability Threat Management, and Threat Intelligence platforms</p>	<p>GLOBO</p> <p>Cisco Secure and Globo Learn more about Cisco Secure and Globo</p>	<p>Microsoft</p> <p>Cisco Secure and Microsoft InTune Learn more about Cisco and Microsoft InTune</p>	<p>mobicconnect</p> <p>Cisco Secure and MobicConnect Learn more about Cisco and MobicConnect</p>	<p>MOSYLE</p> <p>Cisco Secure and Mosyle Learn more about Cisco Secure and Mosyle</p>	<p>SAP</p> <p>Cisco Secure and SAP Learn more about Cisco and SAP</p>	<p>securonix</p> <p>Cisco Secure and Securonix Learn more about Cisco and Securonix</p>	<p>SMOKESCREEN</p> <p>Cisco Secure and SmokeScreen Learn more about Cisco and SmokeScreen</p>	<p>UNCOMMONX</p> <p>Cisco Secure and UncommonX UncommonX specializes in simplifying the complexity surrounding secure or disparate core tools and overly complicated systems.</p>	<p>vmware</p> <p>Cisco Secure and VMware Workspace One Learn more about Cisco and VMware Workspace One</p>	<p>VU</p> <p>Cisco Secure and VU Security Learn more about Cisco Secure and VU Security</p>

cisco.com/go/csta

pxGrid | pxGrid Cloud | pxGrid Direct

<p>XTENDISE</p> <p>Cisco Secure and XTendise Learn more about Cisco ISE and XTendise</p>	<p>TANIUM</p> <p>Tanium Learn more about Cisco and Tanium</p>
---	--

Cisco Secure Access



Seamless access

- Frictionless user experience to all apps
- Unified client intelligently directs ZTNA and VPNaaS traffic
- Access to any app over any port or protocol from anywhere

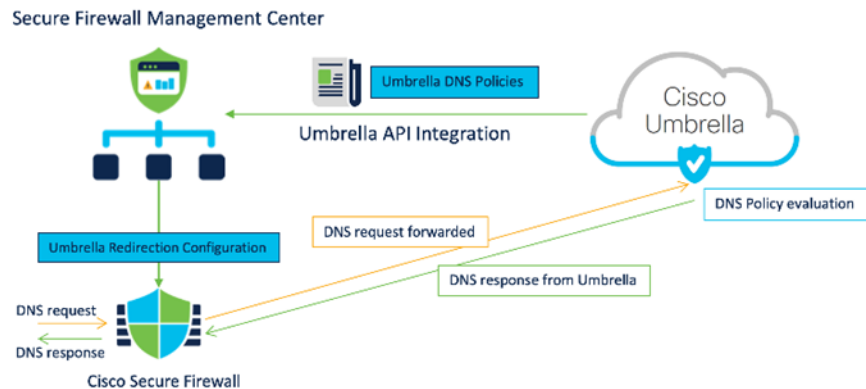
Simple operations

- Resilient cloud native architecture
- Single SSE dashboard and single client
- Integrates with SD-WAN

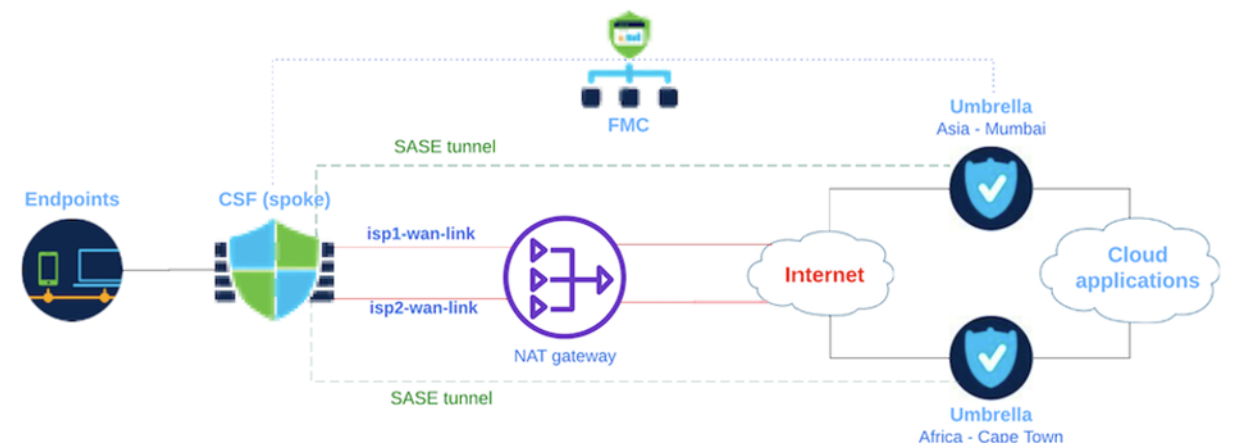
SASE Integration

SASE Deployments Auto Tunnel and Common DNS Security Policy

- Common Security Policies for all branches
- Multi-layered DNS Security
- Faster Protection
- Improved Internet Performance
- Uniform Security policy for Hybrid workers



- SASE use case
- Secure Access– Cloud-delivered Firewall
- Auto-generation and deployment of configuration on Firewall and SSE



“Platforms are the new business model for the digital age, and they are disrupting traditional industries across the globe.”

<https://www.cisco.com/>

<https://cs.co/ise-tacacs>

<https://cs.co/ise-wired>

<https://cs.co/ise-guest>

<https://cs.co/ise-profiling>

<https://cs.co/ise-posture>

<https://cs.co/ise-pxgrid>

<https://cs.co/segmentation-resources>

<https://cs.co/ise-ccc>

<https://cs.co/ise-mdm>

<https://cs.co/ise-tcnac>

<https://www.cisco.com/site/us/en/products/security/firewalls/index.html>

Q&A

PROSSIMI APPUNTAMENTI

7 FEBBRAIO: L'evoluzione delle reti distribuite

14 FEBBRAIO: SonicWall CSE

21 FEBBRAIO: Acronis Awareness e NIS2

<https://events.tdsynnex.it/cyber-unit-missione-protezione/>

TEAM CISCO: it.cisco@tdsynnex.com

SPEAKERS: federico.frosini@tdsynnex.com

giacomoalberto.casati@tdsynnex.com andrea.pezzoni@tdsynnex.com