Return to the office: hybrid and secure access on the new enterprise workplace"

Marcio Drumond
Technical Solutions Architect

January 2022

about me …

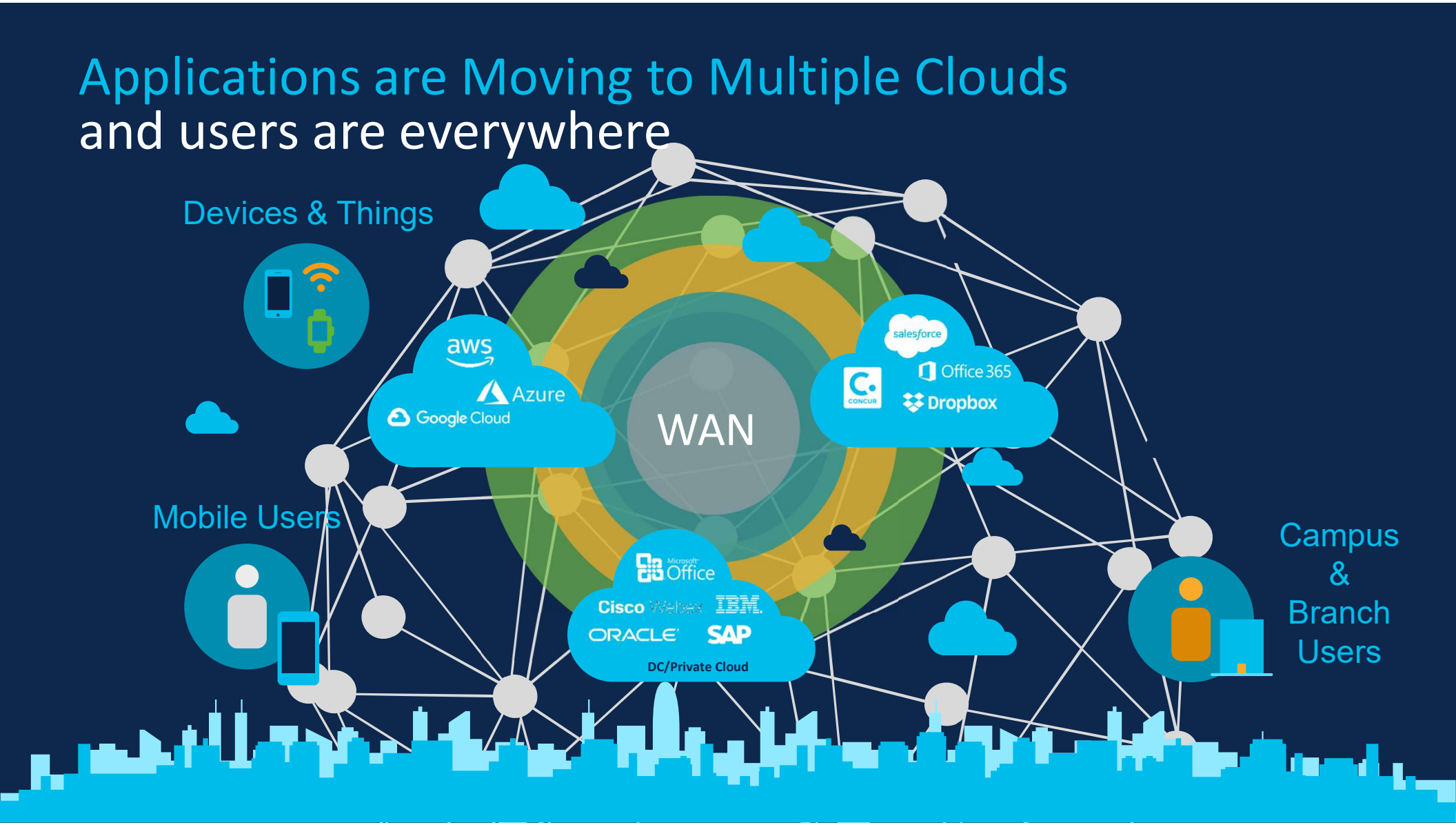
Marcio Drumond

- Technical Solutions Architect
- Based in the UK, is a member of the EMEAR SP Specialists team, focusing on *SP as an Enterprise*.
- More than 20 years of experience in Global Service Provider Networks and Solutions. Holds the CCIE #23113 certification
- **Topics of Expertise:** Enterprise Networking**:** SD- WAN, SDA, Intent Based Networking, Digital Network Architecture. EN Routing, Switching and Wireless.

Agenda

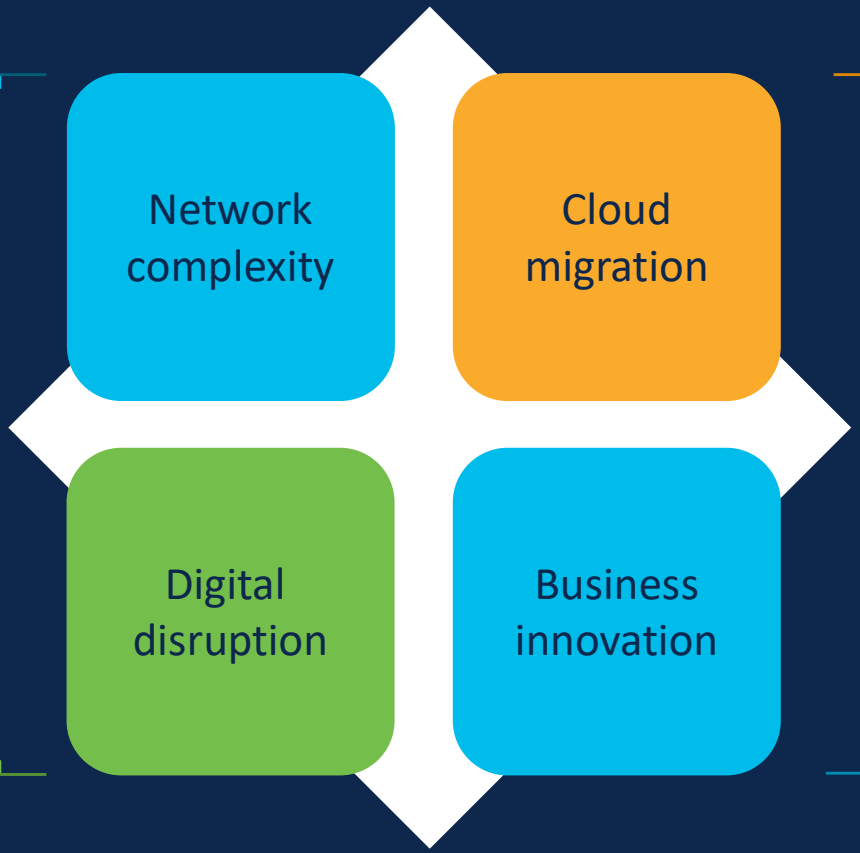
1. New times challenges
2. Intent Based Networking
3. Cisco SDWAN and SASE
4. Cisco SDA and DNA Assurance and Automation
5. Cisco Catalyst 8k and 9k

Applications are Moving to Multiple Clouds
and users are everywhere



The new IT landscape

Traditional network operations are too expensive for today's complex networks.



Network architecture needs updating to support a multicloud world.

Networking trends are creating immense challenges for IT.

IT teams can become centers of innovation for new business-relevant technologies.

75%

of technologists believe their response to the pandemic has created more IT complexity than they have ever experienced

Source: Cisco AppDynamics, “Agents of Transformation 2021”

Network operating expenses are on the rise

3:1

Ratio of OpEx to CapEx on network operations, labor & tools[1]

95%

Network changes performed manually

75%

of OpEx spent on changes and troubleshooting

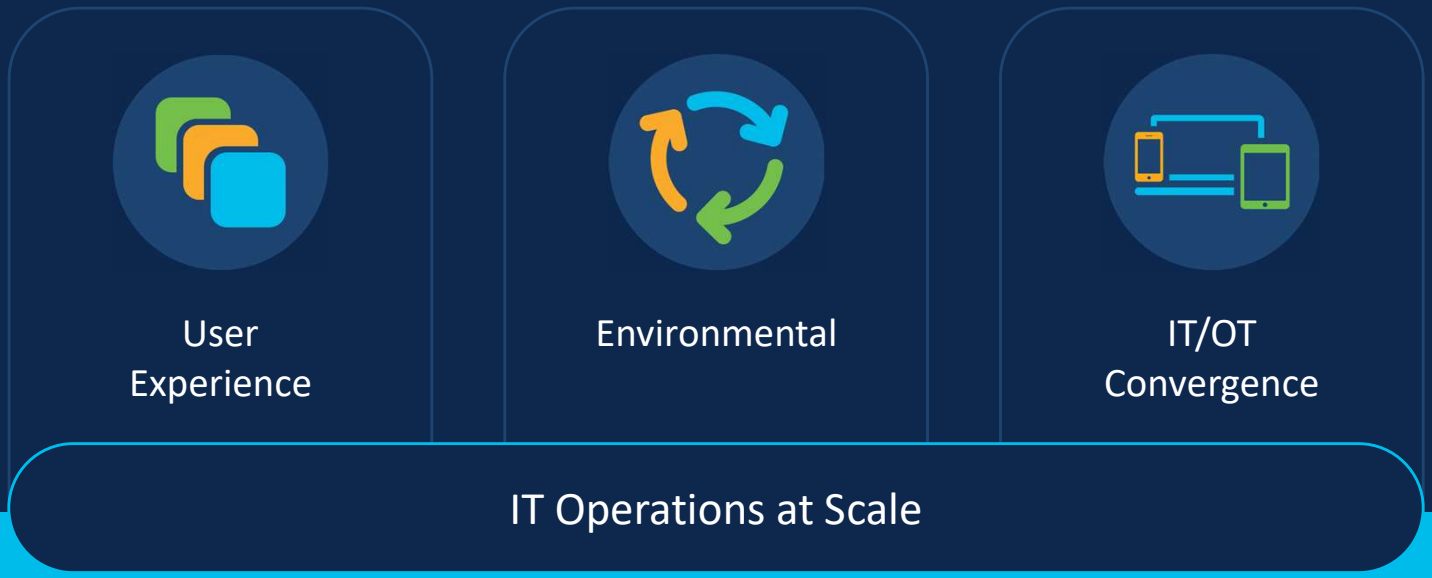
70%

of policy violations are due to human error

[1]Cisco McKinsey Study

Pace of change exceeds human scale

Businesses must overcome technology boundaries



How to make hybrid work…work?

Enterprise Networks of the Future need to have

Resiliency and high availability

Optimal performance and Zero downtime

Highly available and redundant design

Protocols High Availability

Security and visibility

Transport Security and Segmentation

Application Visibility

Trusted Solutions

Intelligence and data analytics

Open Interfaces

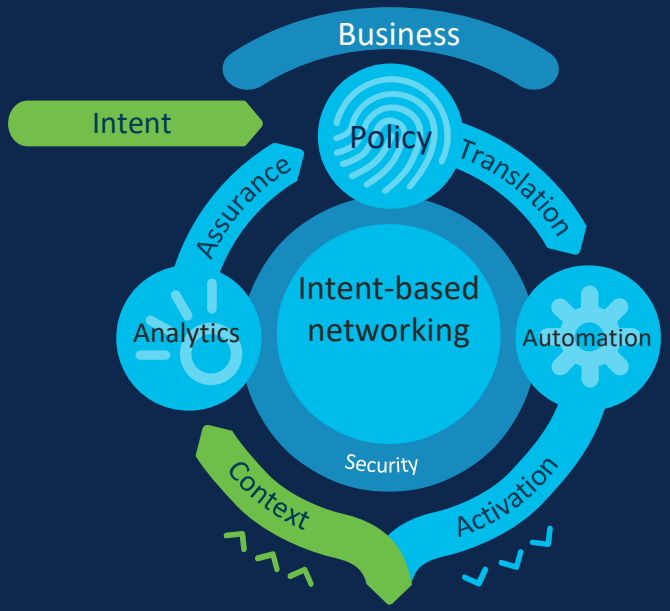
Telemetry and analytics

Data Analysis

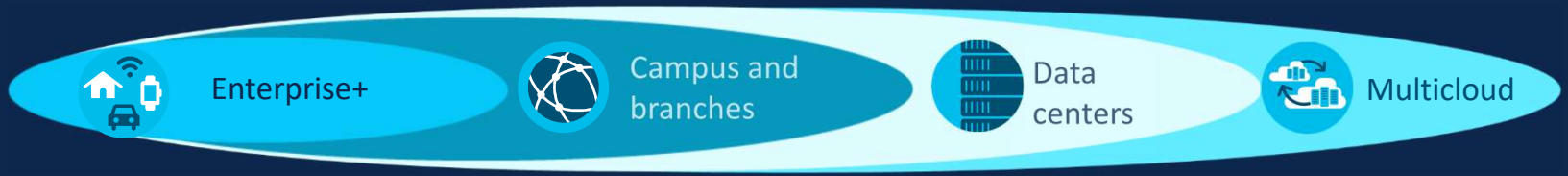
Open standards solutions, value of investment, operational efficiency

Intent-based networking

IT success requires automating the operation and management of your network.

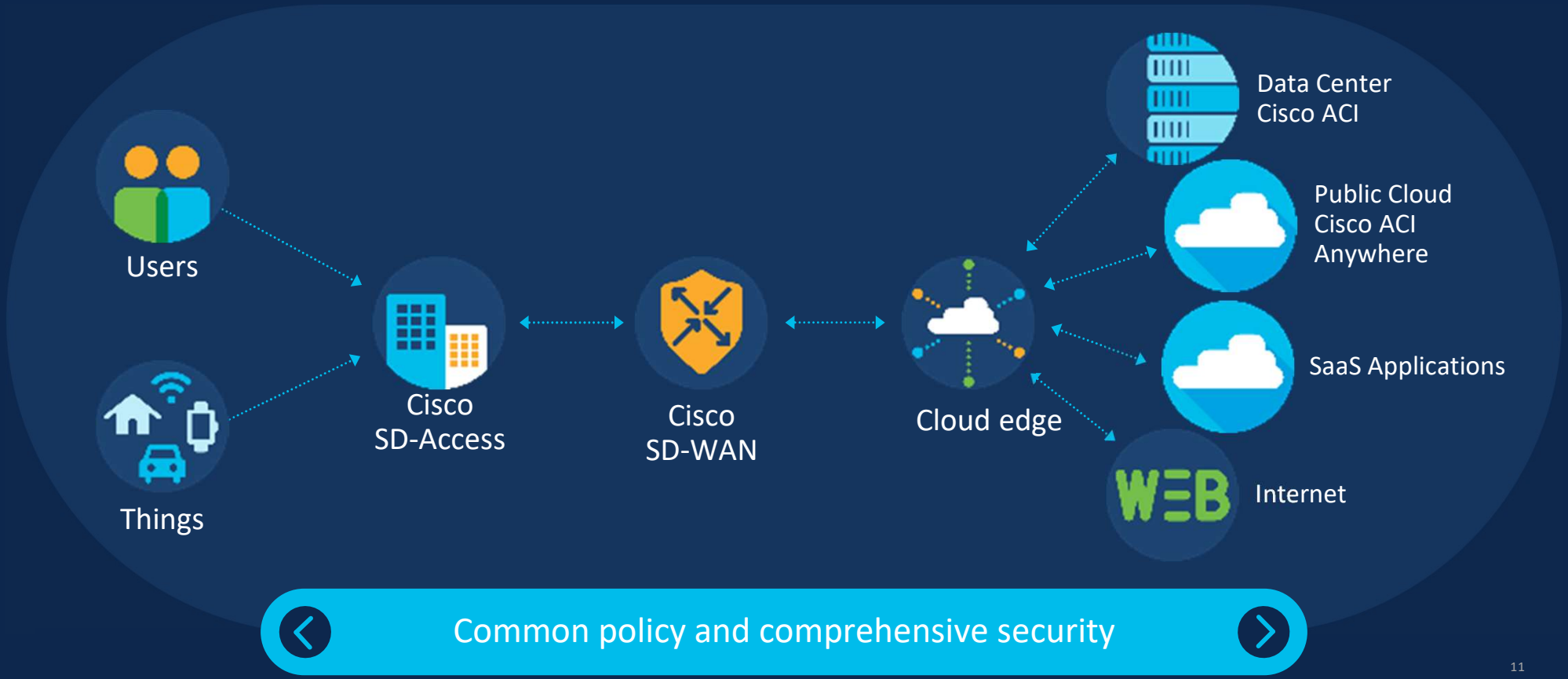


- Comprehensive automation
- Analytics and assurance
- Consistent security



Users and things ⟷ Applications and services

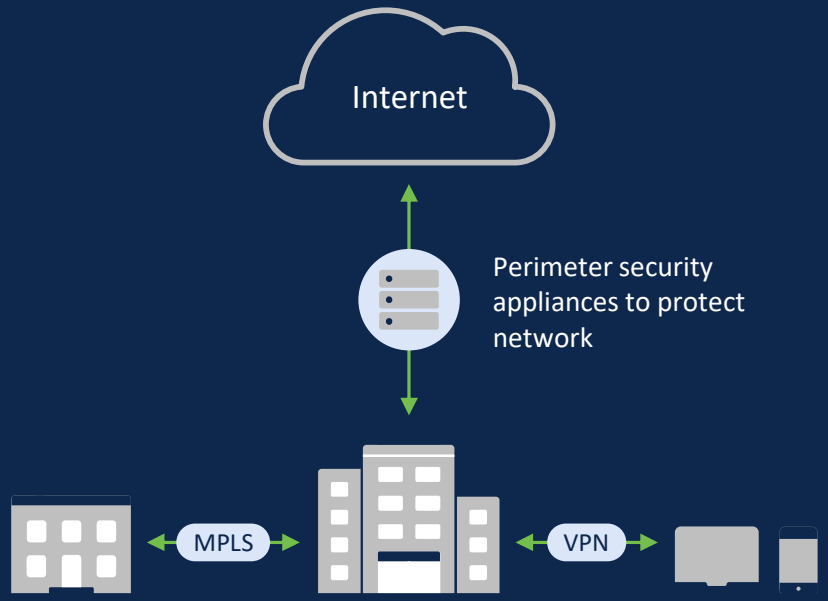
Cisco intent-based networking solutions span access to applications



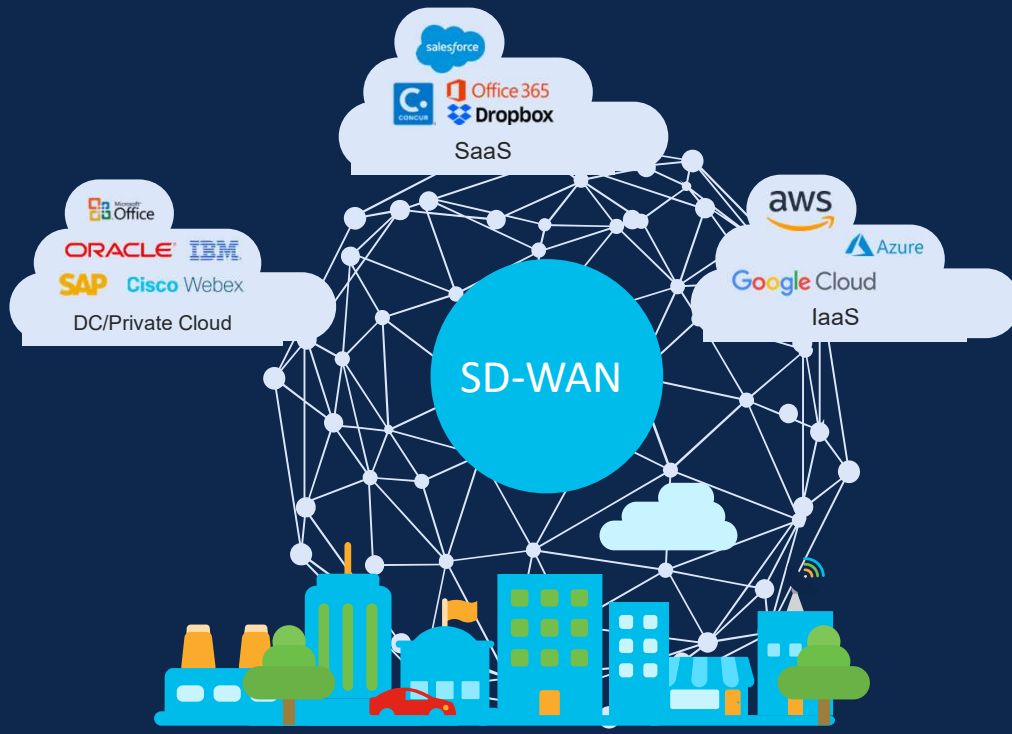
Cisco SD-WAN and SASE

Network transformation

Internet/cloud is new “center of universe”

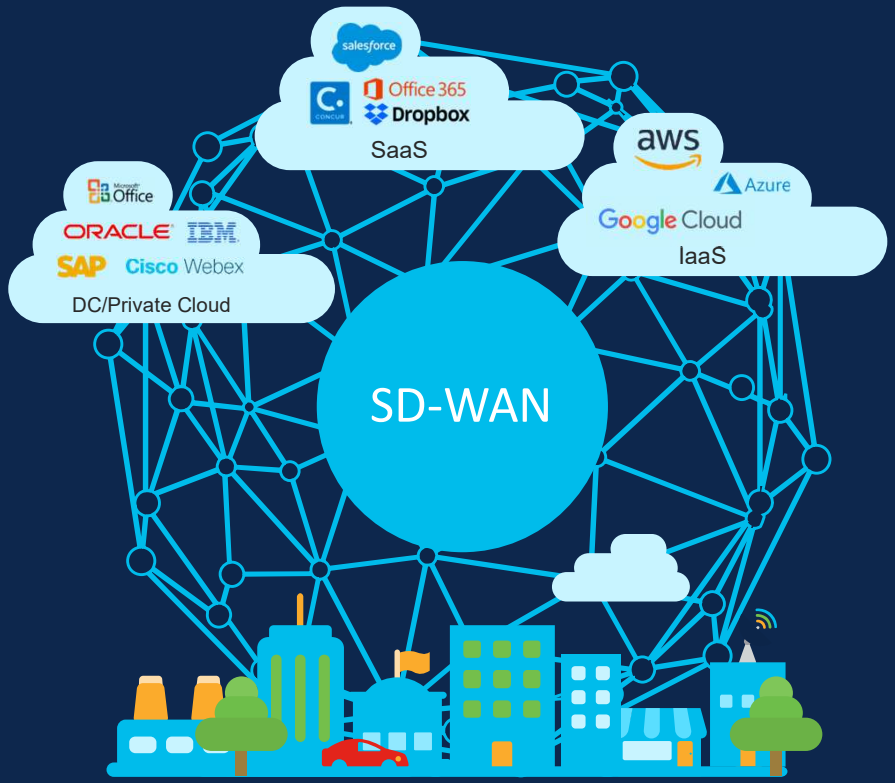


DC-centric



Internet/cloud-centric

Secure SD-WAN is now business critical



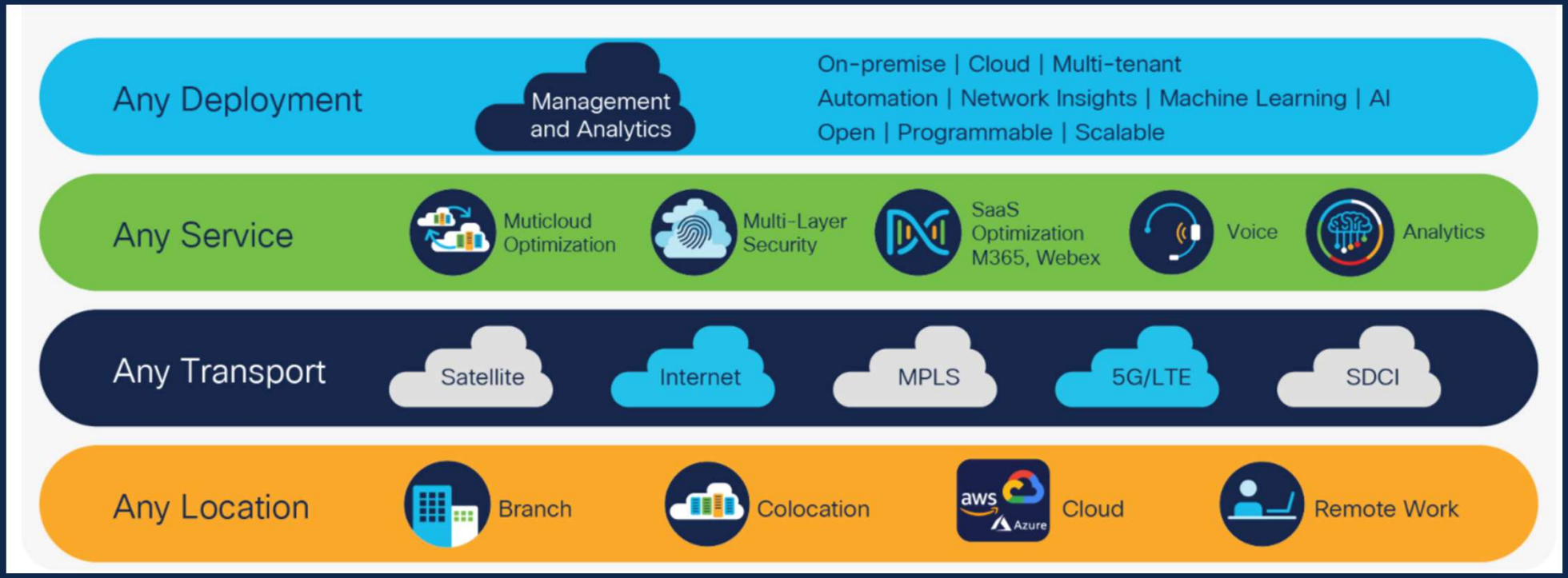
Segmentation

Identity

Observability

SASE

Cisco SD-WAN


Any Deployment
Management and Analytics
On-premise | Cloud | Multi-tenant
Automation | Network Insights | Machine Learning | AI
Open | Programmable | Scalable
Any Service
Muticloud Optimization
Multi-Layer Security
SaaS Optimization M365, Webex
Voice
Analytics
Any Transport
Satellite
Internet
MPLS
5G/LTE
SDCI
Any Location
Branch
Colocation
aws
Azure
Cloud
Remote Work

Benefits of Cisco SD-WAN

Predictable app experience

Support for evolving business application strategy

Cloud OnRamp for IaaS, SaaS and Colocation

Right security, right place

Secure segmentation across entire network stack

Full edge security stack from branch to cloud and colocations

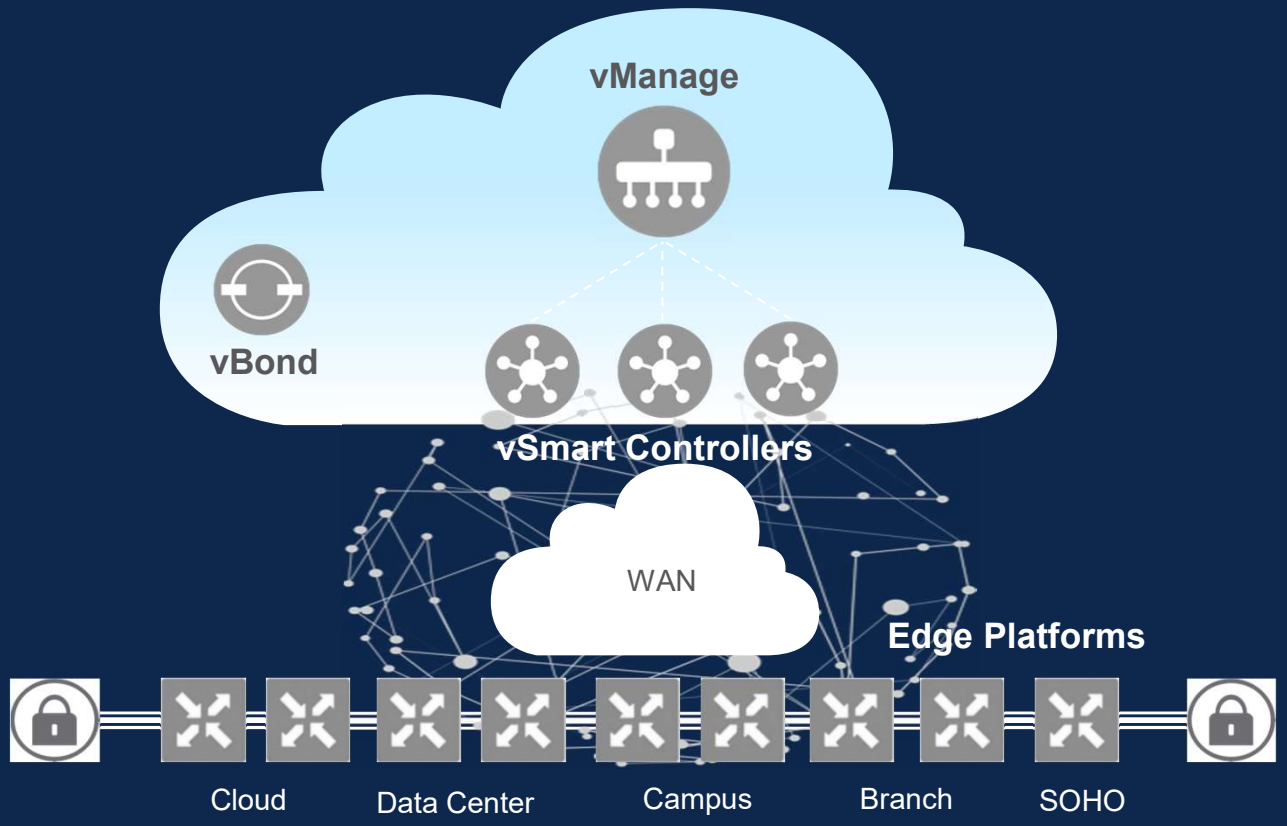
Enterprise grade, simplified

Intent-based networking with multi-domain policy

Proven deployments to over 10,000+ sites

One user interface for Security and SD-WAN across branch, cloud, and co-location

Cisco SD-WAN Components



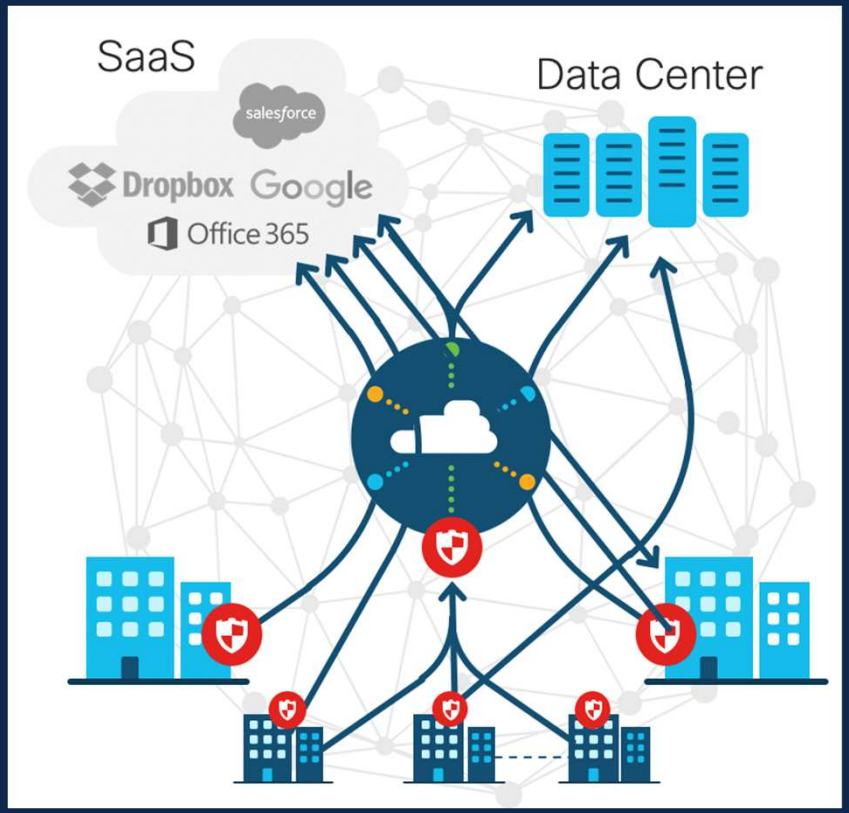
Orchestration Plane
Cisco vBond

Control Plane
Cisco vSmart

Data Plane
Physical/Virtual
Cisco vEdge/cEdge

Management Plane
Cisco vManage

Cisco SD WAN in SP as an Enterprise



Flexibility in path selection

Virtualize traffic service chains to dynamically change, add, remove routes to DC and cloud services

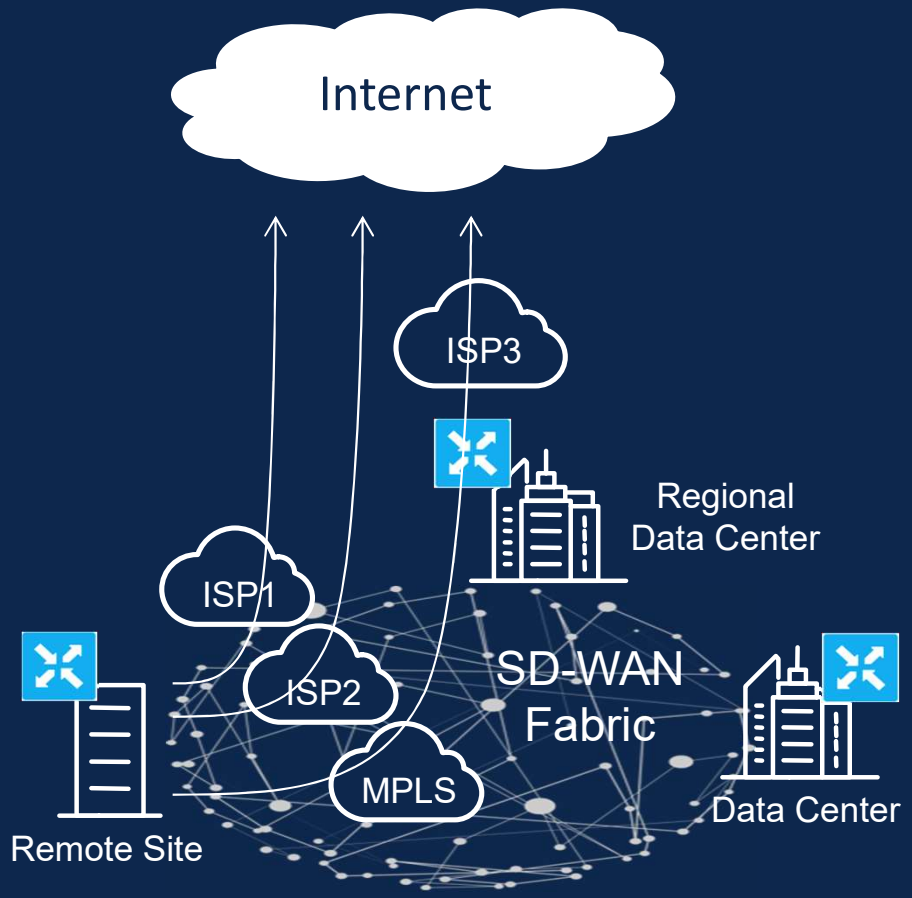
Reduced latency

Increased bandwidth, with direct physical connection & avoiding backhaul

Optimize Connectivity

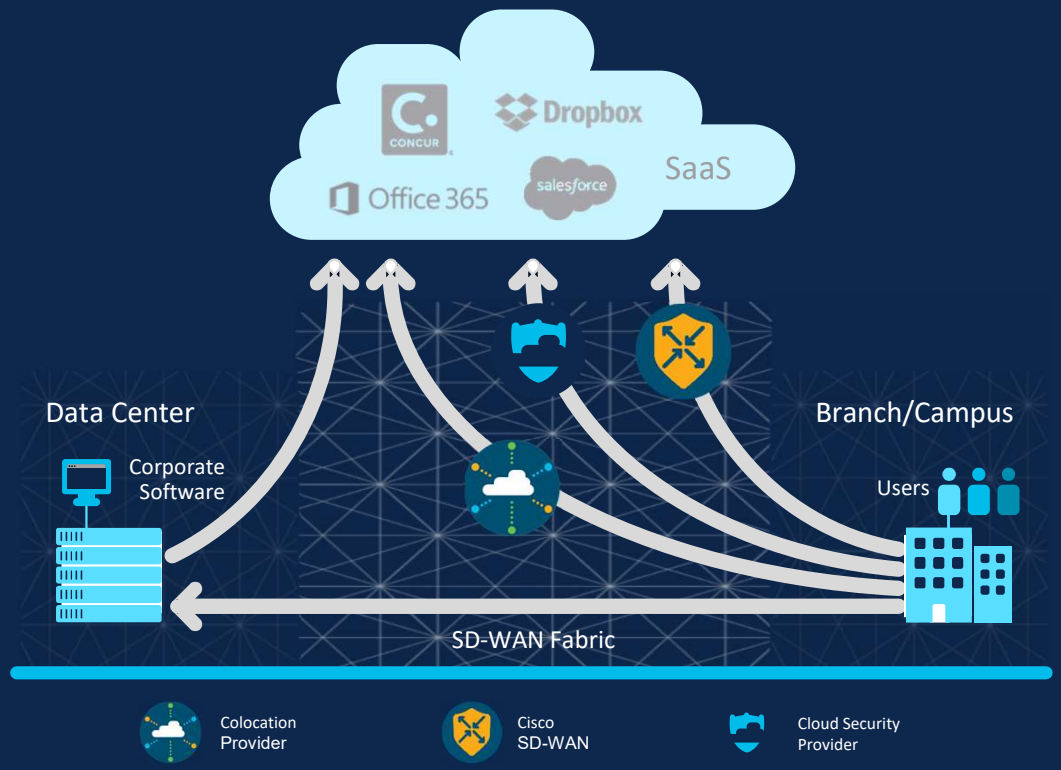
Manage different connections, via Internet or multiple circuits within same Provider backbone – based on performance and traffic requirements

Direct Internet Access



- Can use one or more local DIA exits or backhaul traffic to the regional hub through the SD-WAN fabric and exit to Internet from there
  - Per-VPN behavior enforcement
- VPN default route for all traffic DIA or data policy for selective traffic DIA
- Network Address Translation (NAT) on the vEdge/cEdge router only allows response traffic back
  - Any unsolicited Internet traffic will be blocked by IP table filters
- For performance-based routing toward SaaS applications use Cloud onRamp

SaaS Optimization

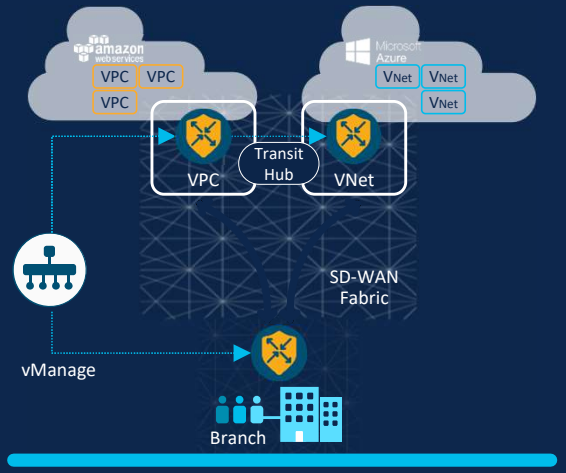


Optimization via Multipath

Up to 40% faster Office 365 Performance

Increased reliability and utilization of best path for SaaS applications

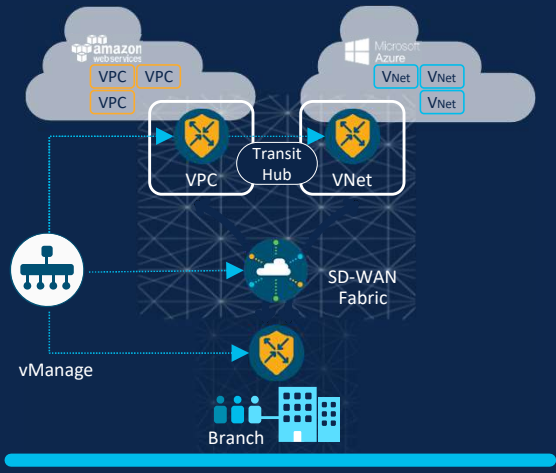
Extending SD-WAN to IaaS



Internet connection to IaaS cloud

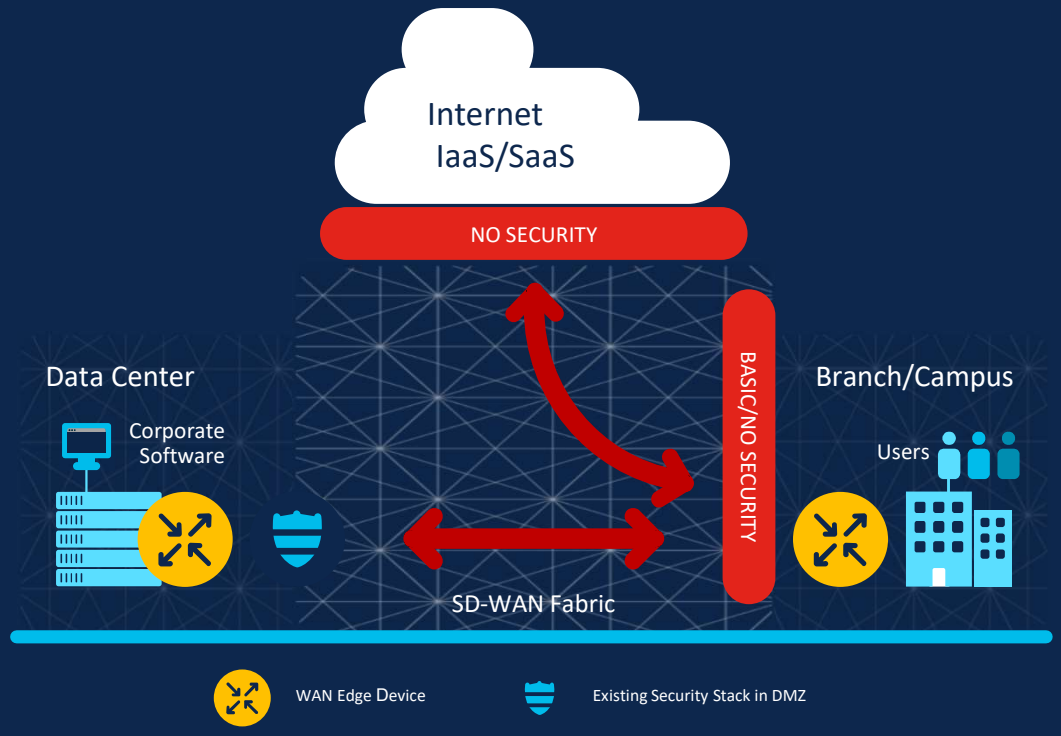
Cloud OnRamp Automation to IaaS

- Cisco WAN Edges deployed in a Transit Hub, acting as virtual aggregation routers
- Partial extension of SD-WAN Fabric
- Automated deployment process with vManage



Connect to IaaS cloud via co-location

SD-WAN leverages new security challenges



Internal & External Threats

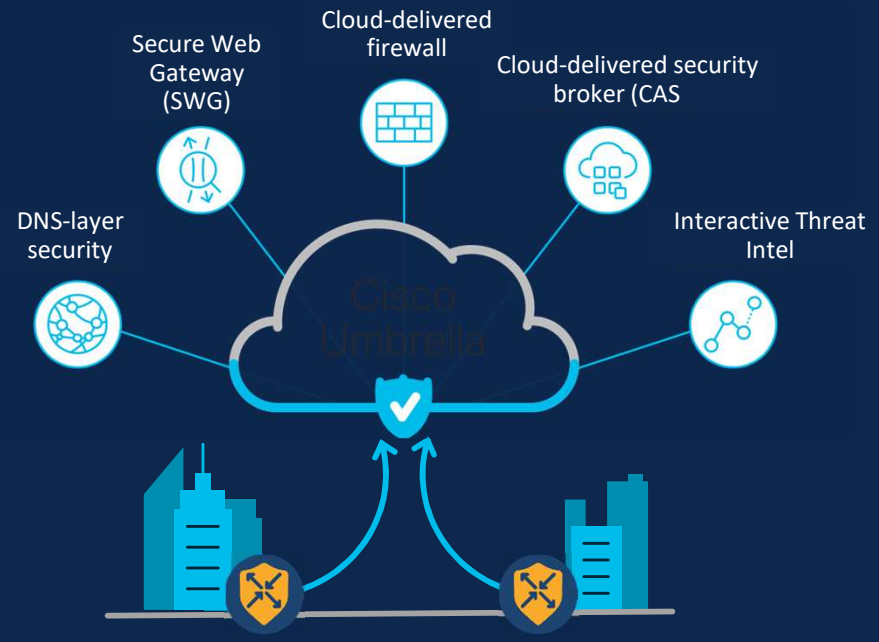
External

- Exposure to malware & phishing due to direct internet and cloud access
- Data breaches
- Guest access liability

Internal

- Untrusted access (malicious insider)
- Compliance (PCI, HIPPA, GDPR)
- Lateral movements (breach propagation)

Secure Access Service Edge
Transitioning to a Cloud-First Security Model



Cisco SD-WAN + Umbrella

What is SASE?

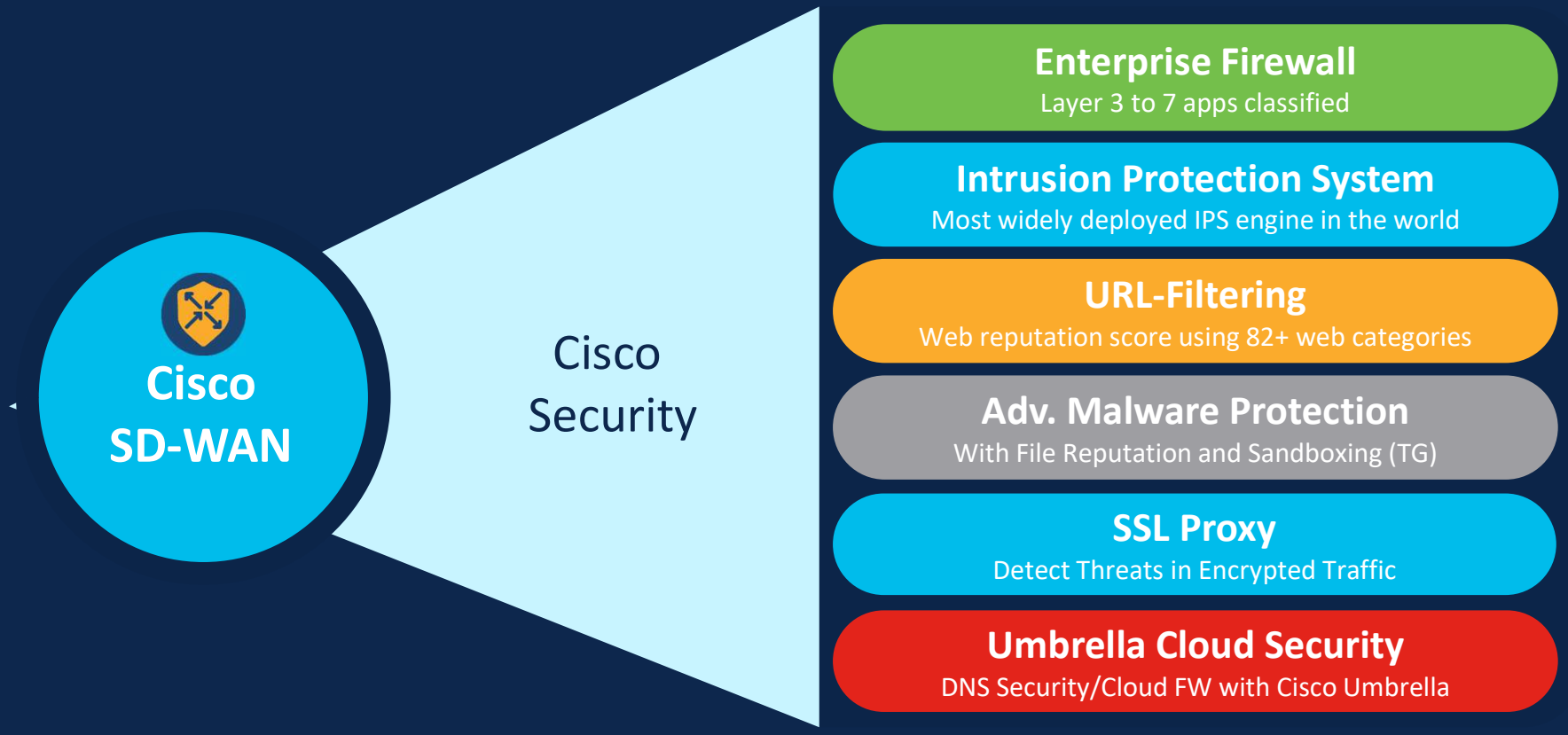
"SASE combines network security functions (such as SWG, CASB, FWaaS and ZTNA), with WAN capabilities (i.e., SDWAN) to support the dynamic secure access needs of organizations. These capabilities are delivered primarily aaS and based upon the identity of the entity, real time context and security/compliance policies." –Andrew Lerner,*

https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/

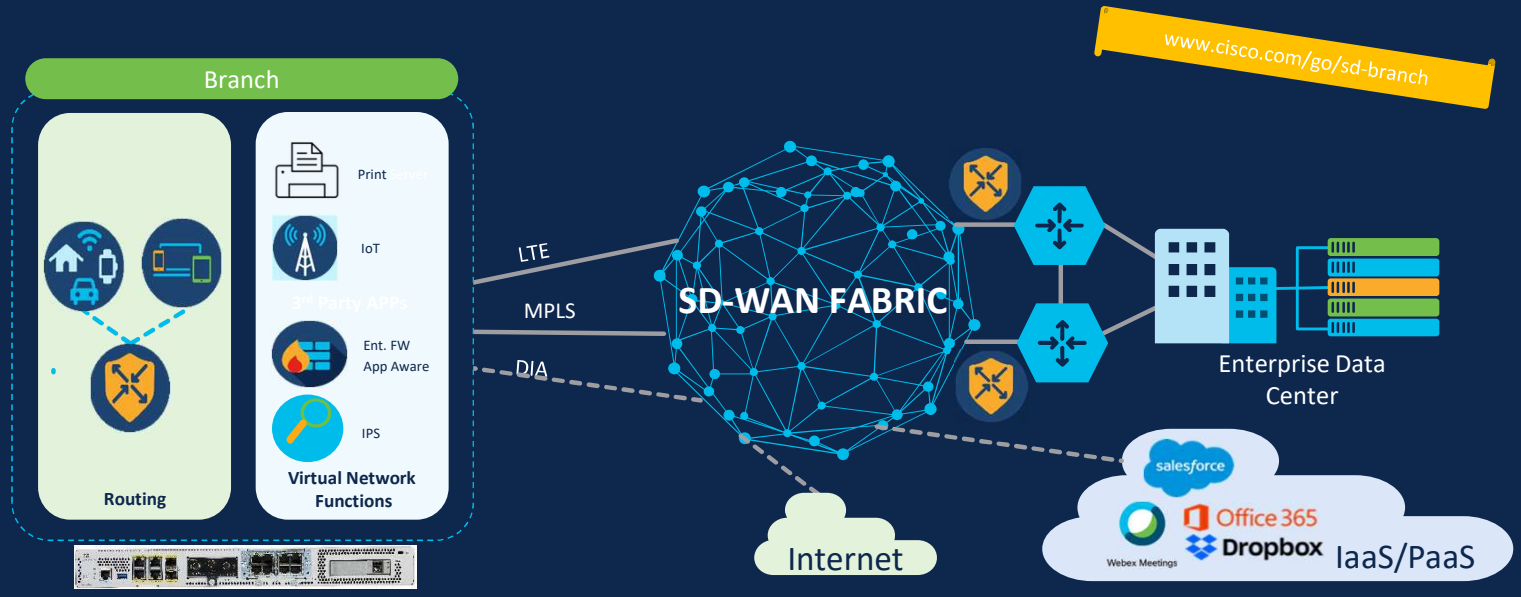
* ZTNA = Zero Trust Network Access

Cisco SD-WAN Security & SASE Solution

Consistent across on-prem and cloud



Enterprise Virtual Branch Office / SD-Branch

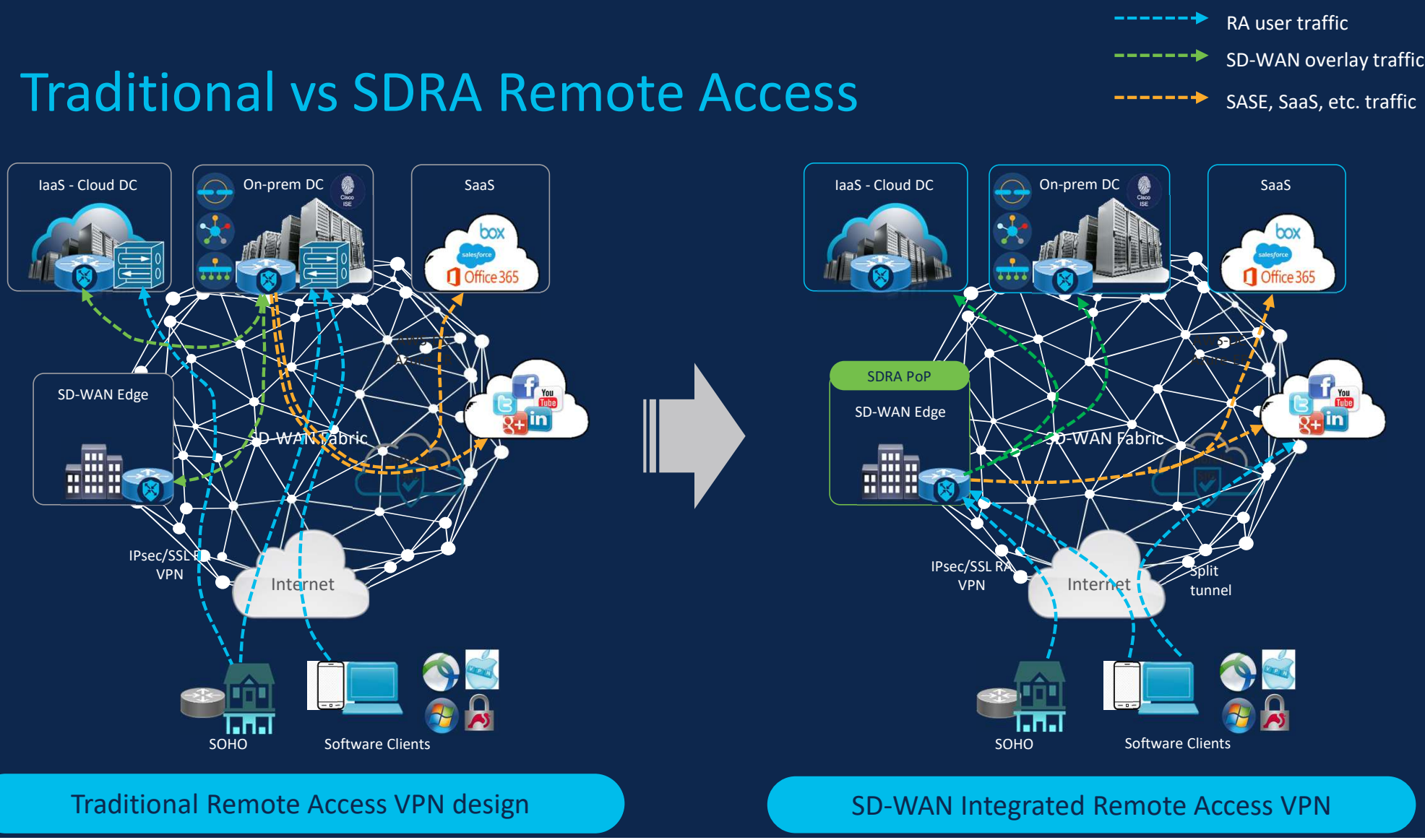


Consolidated Routing & Security with virtualized apps

Zero-touch Provisioning with vManage

Quick & Easy Delivery of Software-based Services

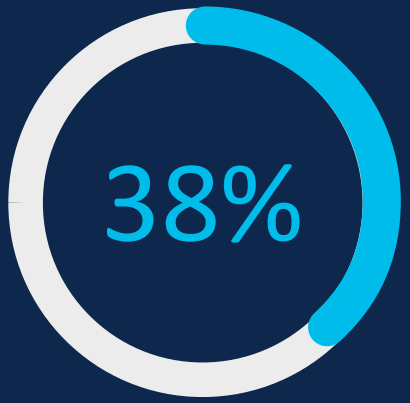
Traditional vs SDRA Remote Access



Traditional Remote Access VPN design

SD-WAN Integrated Remote Access VPN

Business Value of Cisco SD-WAN



Lower five-year cost of WAN operations

Faster to implement policy/ configuration changes

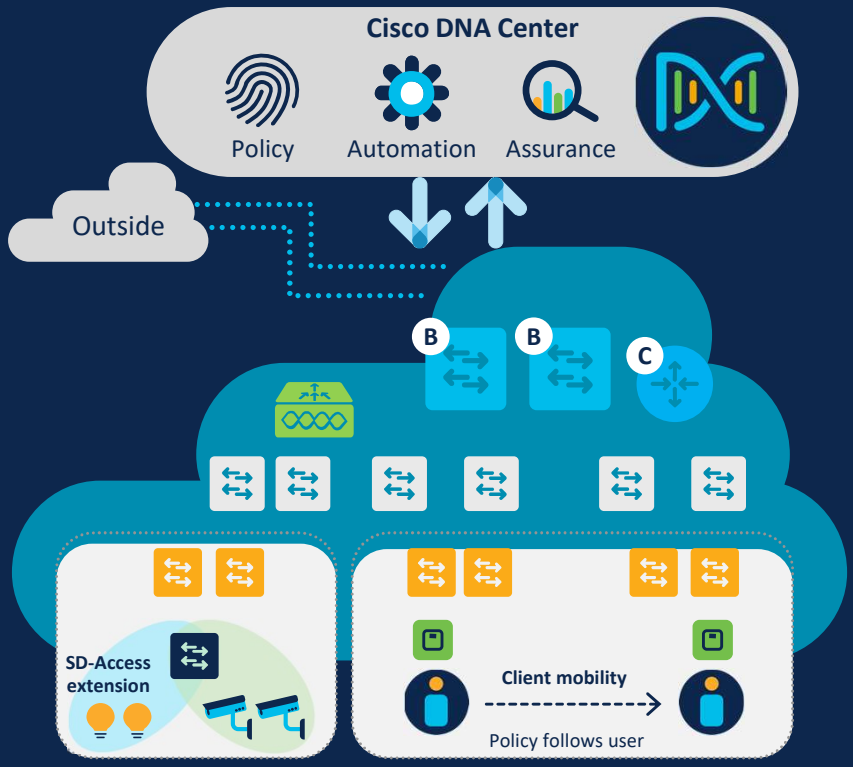
Less unplanned downtime

Full IDC report available on www.cisco.com/go/sdwan

Cisco SDA and DNA Assurance and Automation

Cisco Software-Defined Access (SD-Access)

The foundation for Cisco's intent-based network



Deep visibility

Identify and group endpoints. Map their interactions and define access policies

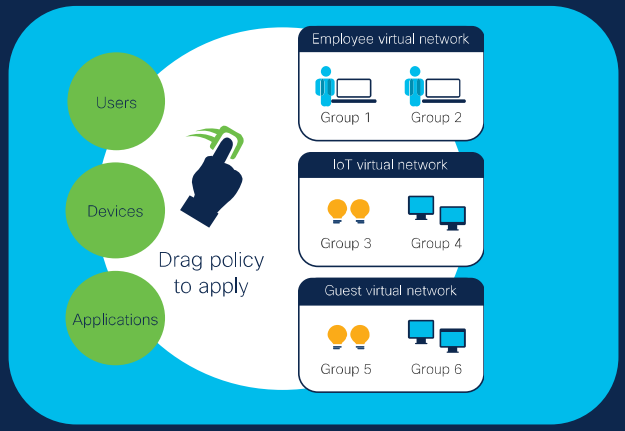
Group-based policy and segmentation

Enforce group-based access policies and secure network through segmentation

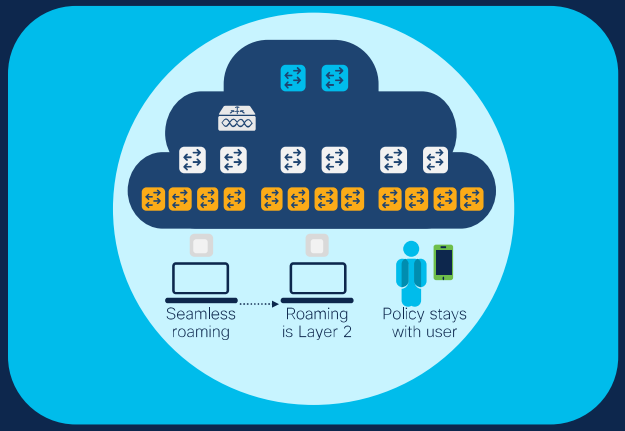
Policy consistency throughout

Use Cisco's multidomain architecture for consistent access and security policies throughout the enterprise

Why SDA?



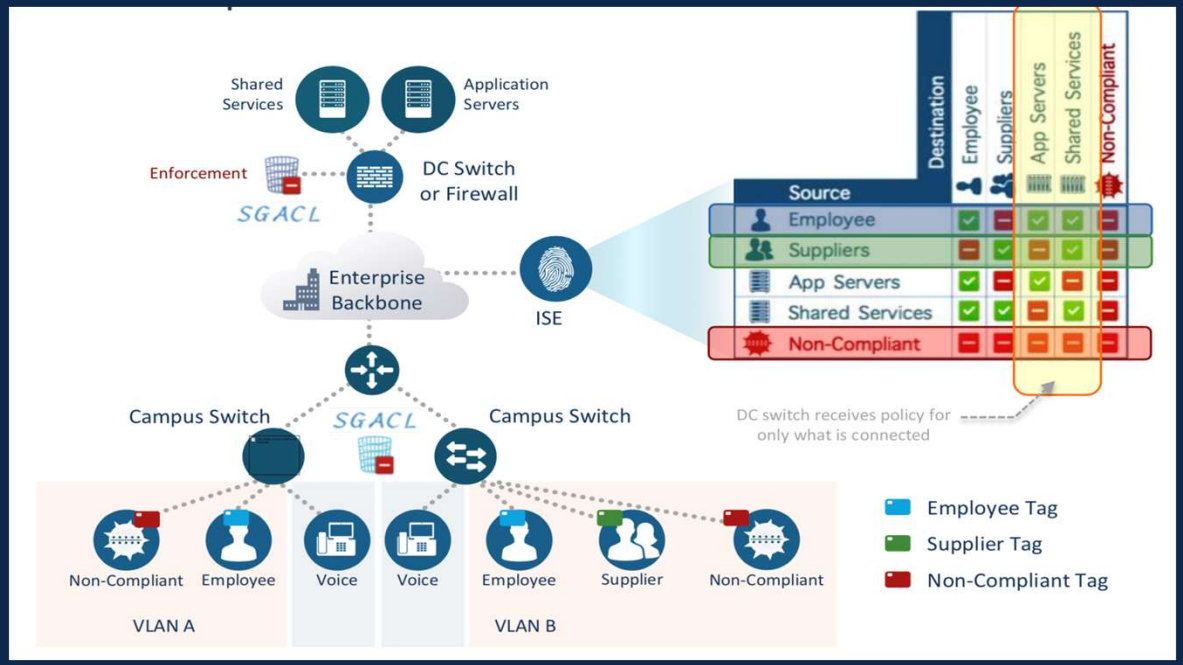
SD-Access segments the network and securely onboards client devices



Enforces the policy consistently over wired and wireless networks

Extends secure access policies to IoT devices

Segmentation and policy based routing

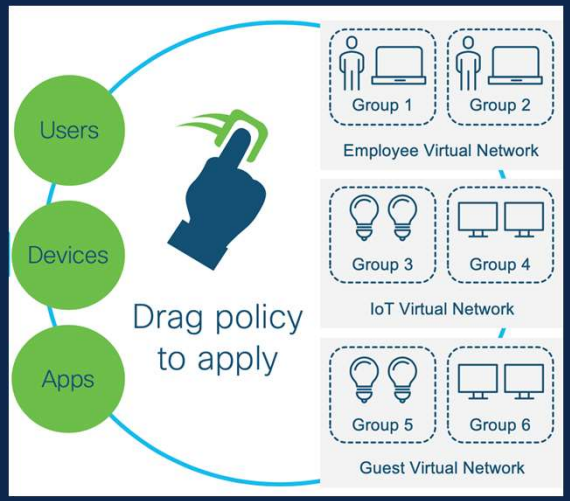


Before SD-Access

- VLAN and IP address based
- Create IP based ACLs for access policy
- Deal with policy violations and errors manually

After SD-Access

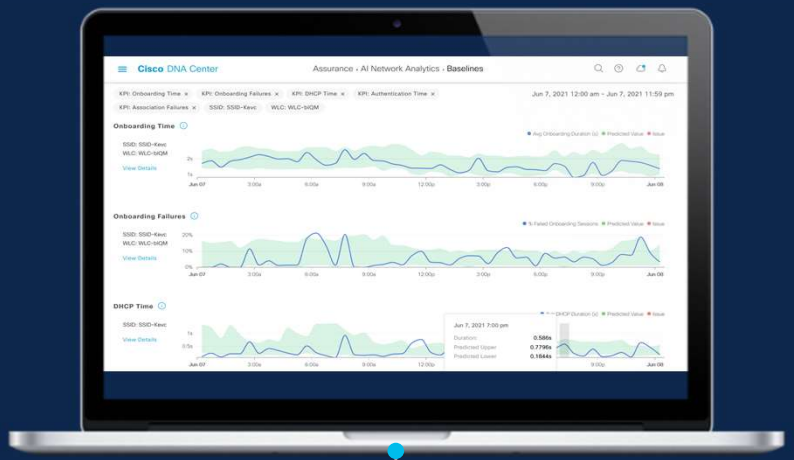
- No VLAN or subnet dependency for segmentation and access control
- Define one consistent policy
- Policy follows Identity



Cisco DNA Center is a foundational platform technology

Command and control center for Cisco Catalyst

Cisco DNA Center



Physical and virtual infrastructure

Cisco and third party

NetOps

Automation and workflows simplify building and maintaining large scale networks. AI/MR streamlines and simplifies complex tasks

AIOps

AI/ML and insights to ensure the health, performance and reliability of applications and infrastructures

SecOps

AI/ML and DPI Identify and classify endpoints, enforce security policies and mitigate threats for a complete workplace zero trust solution

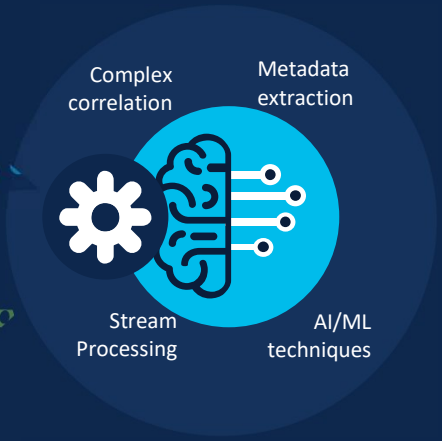
DevOps

Mature APIs, SDKs, and closed-loop integrations, untangle the complexities of interconnecting third party systems

Cisco DNA Assurance

From network data to business insights

Network telemetry and contextual data | Complex event processing | Correlated insights | Suggested remediation



Visibility:
Personalized baselining

Insight:
Intelligent analysis

Action:
Accelerated remediation

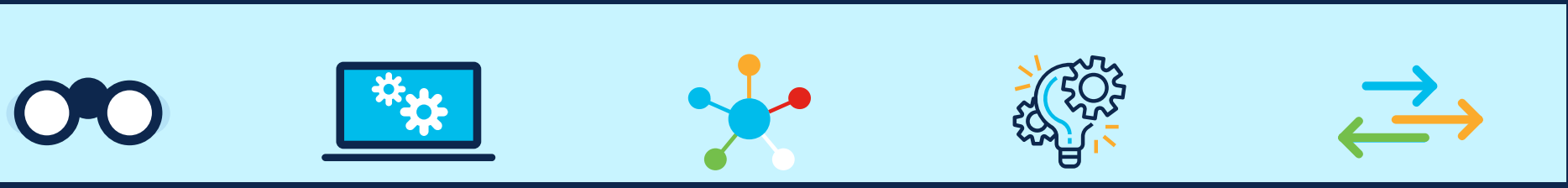
Everything as a sensor

Over 150 Actionable insights

Client | Applications | Wireless | Switching | Routing

Cisco DNA Automation

Delivers essential capabilities to automate network deployment and management



Visibility

Discovery, inventory, single pane of glass

Intent

Policies, configurations

Deploy

Provision, plug-and-play

Manage

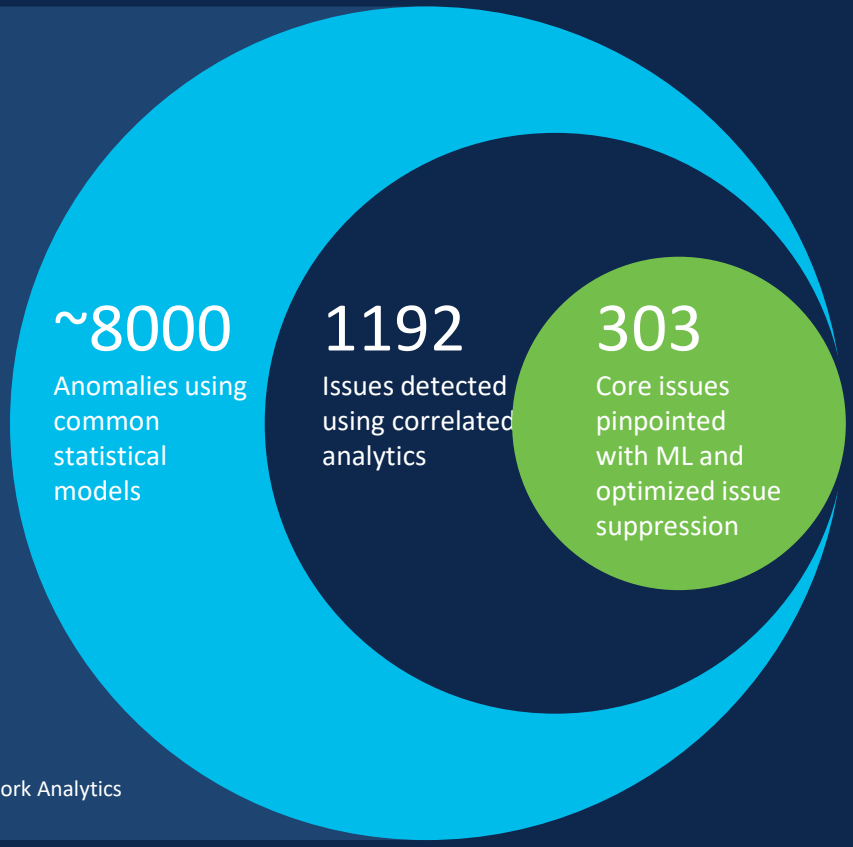
Software image management, changes, compliance

Extend

Assurance, security, third-party applications

Cisco DNA Assurance aided by AI/ML reduces noise fo greater IT efficiency

Issues generated for 11 customers over 3-month period

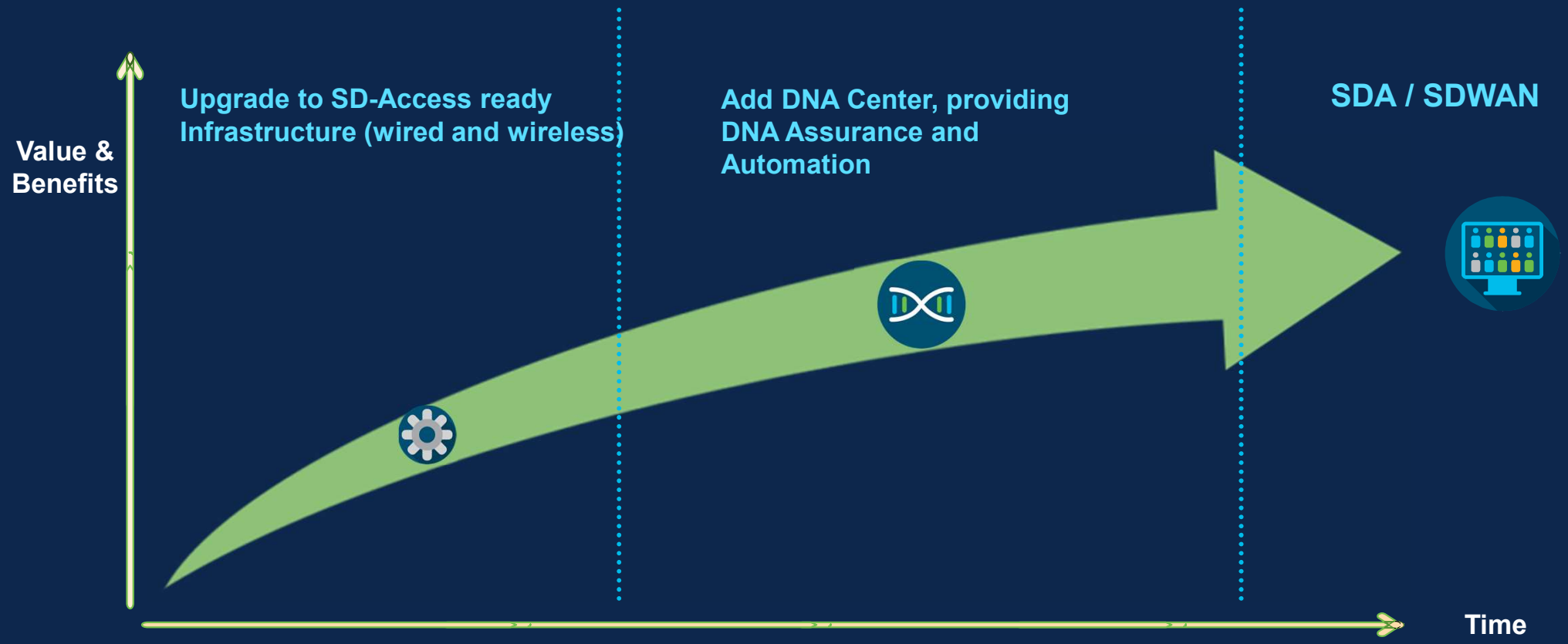


- Traditional NMS
- Cisco DNA Assurance
- Cisco DNA Assurance with Cisco AI Network Analytics

Fewer issues = less troubleshooting

Relevant issues = big events first

Journey to Intent Based Networks



Cisco DNA is intent-based networking for the campus, branch, and SD-WAN

Lets you focus on business innovation rather than the network

Automate for simplicity

67%

provisioning time savings

Define policy and segment network

80%

reduction in IT operational expenses

Defend against security threats

47%

reduced breach impact

Assure performance

90%

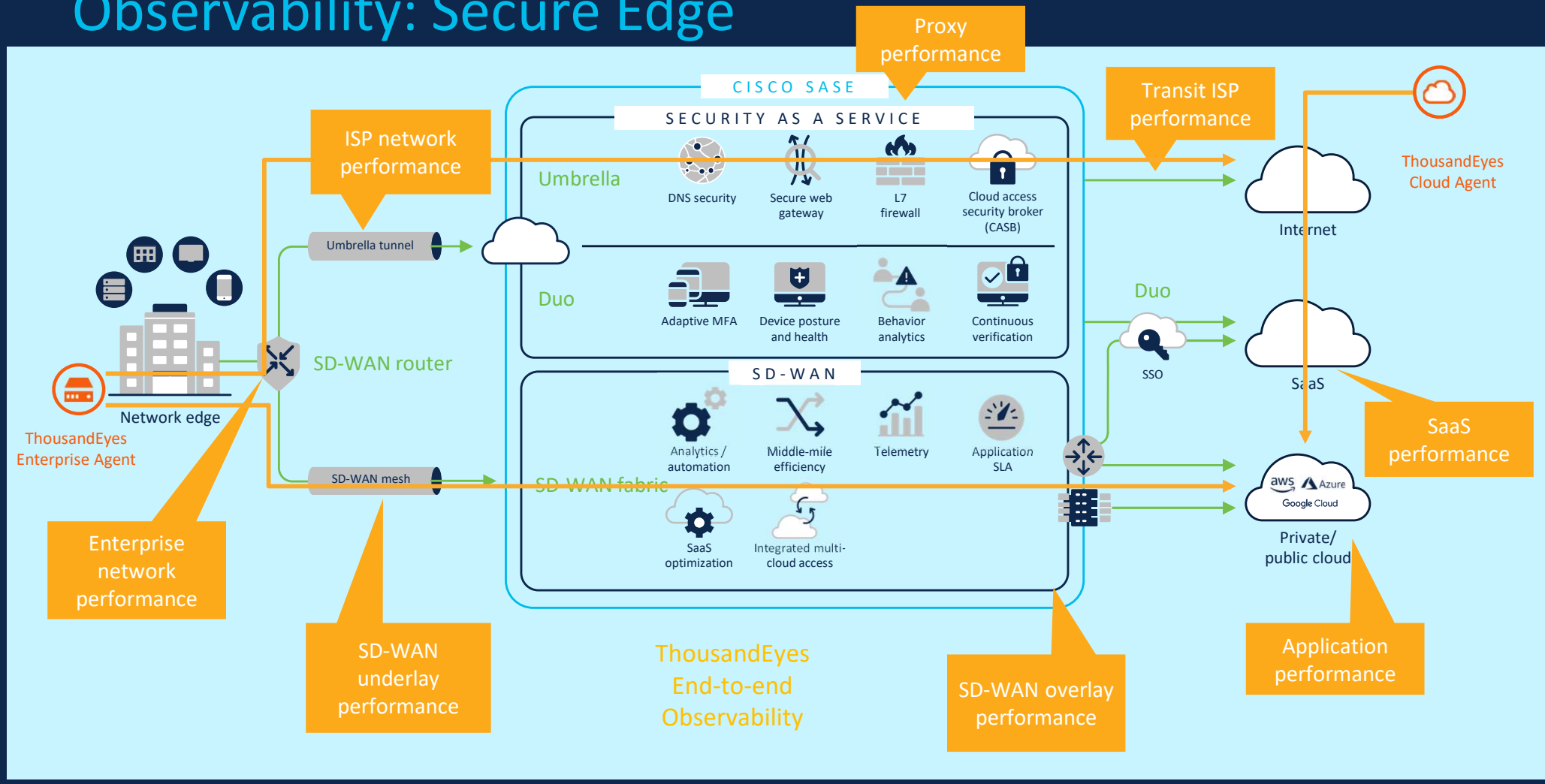
reduction in time for issue detection and resolution

Optimize application experience

45%

reduced application latency

Observability: Secure Edge



Location intelligence applied to your business

1 

"How can I ensure my campus is safe to reopen?"

— Gary | Workspace Services Team

2 

"I want to see how my business is impacted by COVID19."

— Jason | Global Strategy Head

3 

"How can I provide personalized customer experiences while ensuring social distancing?"

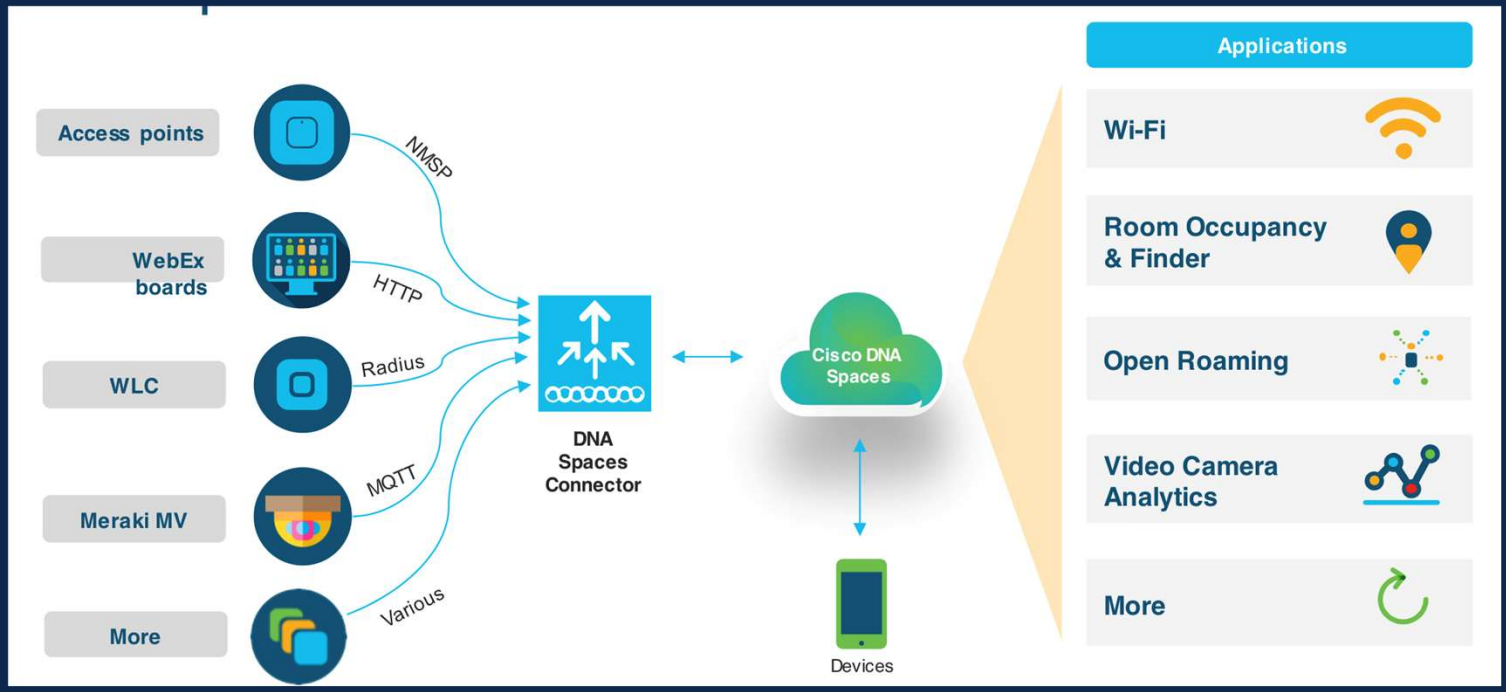
— Mary | Chief Customer Office

4 

"How can I optimize my assets deployed across healthcare facilities during and after a post-COVID world?"

— Sarah | Nursing Director

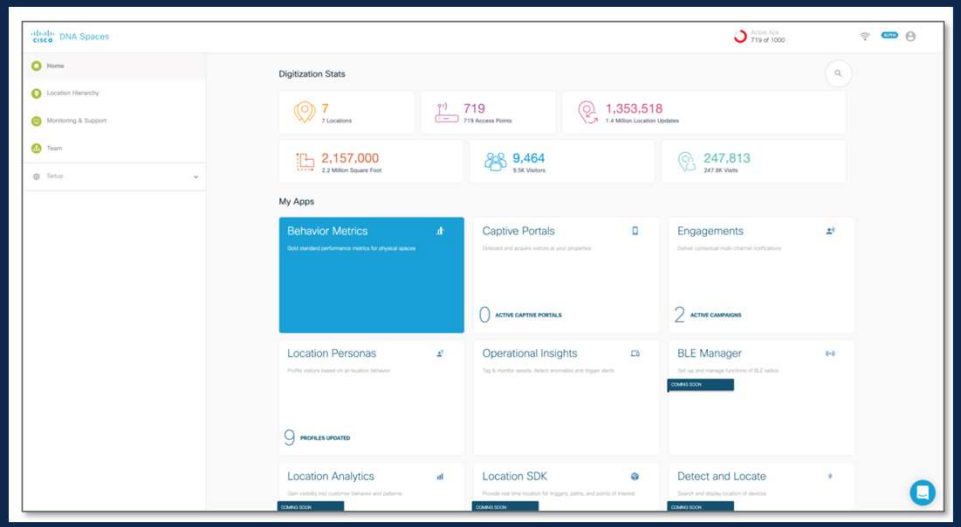
Cisco DNA Spaces

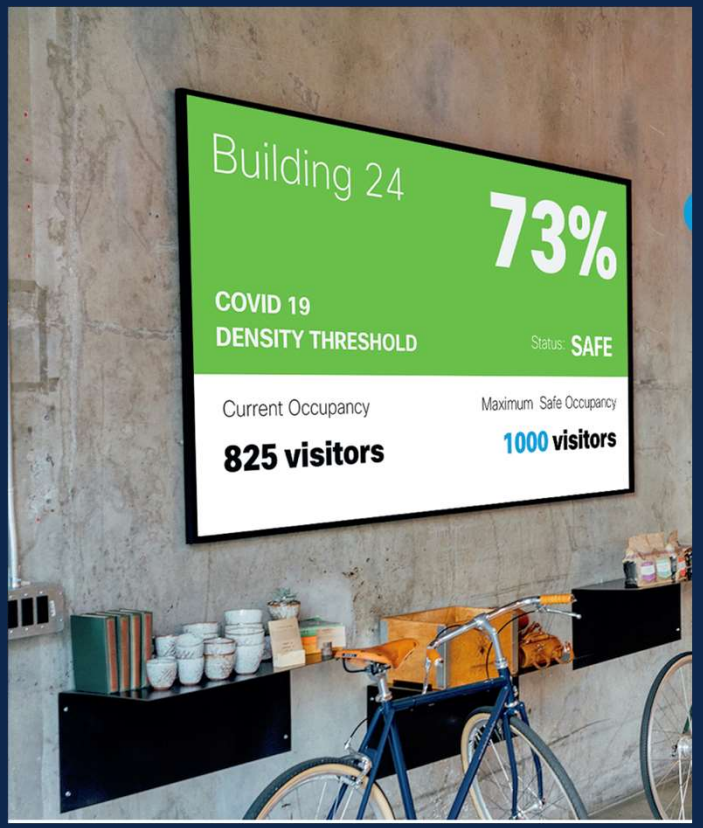


Cisco DNA Spaces

Workspaces

- Insights into employee and visitor behavior to measure workspace utilization, understand patterns
- Understand how conditions in the office and events impact employee behavior
- Trigger notifications, alerts and business workflows based on behavior of people and things
- Track and locate assets and monitor asset telemetry





Cisco Catalyst 8k and 9k

Catalyst 8000

Human centric design powered by machine centric intelligence

Custom ASIC enabled Scale

Scalable on-chip services at Aggregation

Secure containers
Application hosting

x86

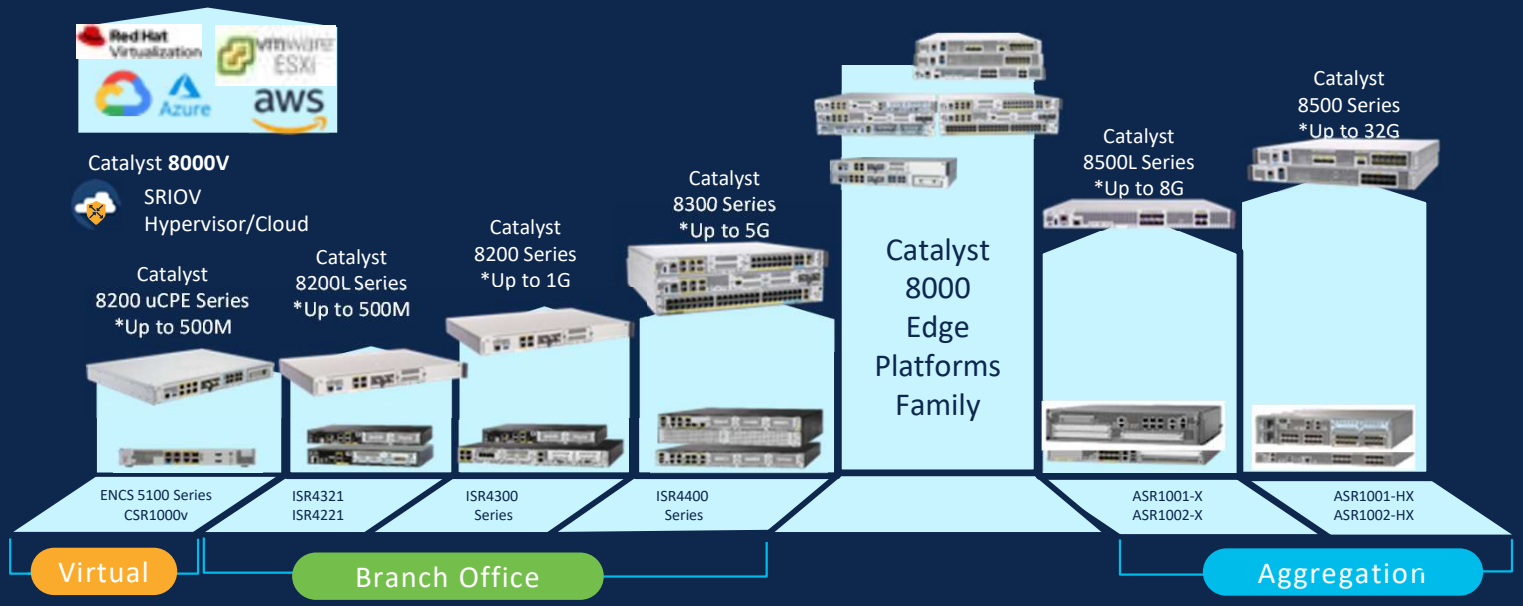
x86 multicore CPU

Model-driven APIs
Streaming telemetry

Open and Extensible Cisco IOS XE

Cisco Catalyst 8k Routing Portfolio

Refreshed from Branch to Cloud



*Perf. Numbers are Agg. IPsec IMIX

Cisco Catalyst 9000 Portfolio

Foundation of intent-based networking


CISCO