



Rozvoj informačnej spoločnosti: Inovatívne riešenia pre digitálnu éru s platformou Cisco Meraki

Milan Rášo , Systems Engineer, Cisco Slovakia

20. Jún 2024



Transformácia IT: Hybridný Svet ako Norma

41%

Say **securing user access** to cloud-based applications is their biggest obstacle

86%

See having a **consistent operational model** across on-premises and multicloud is important

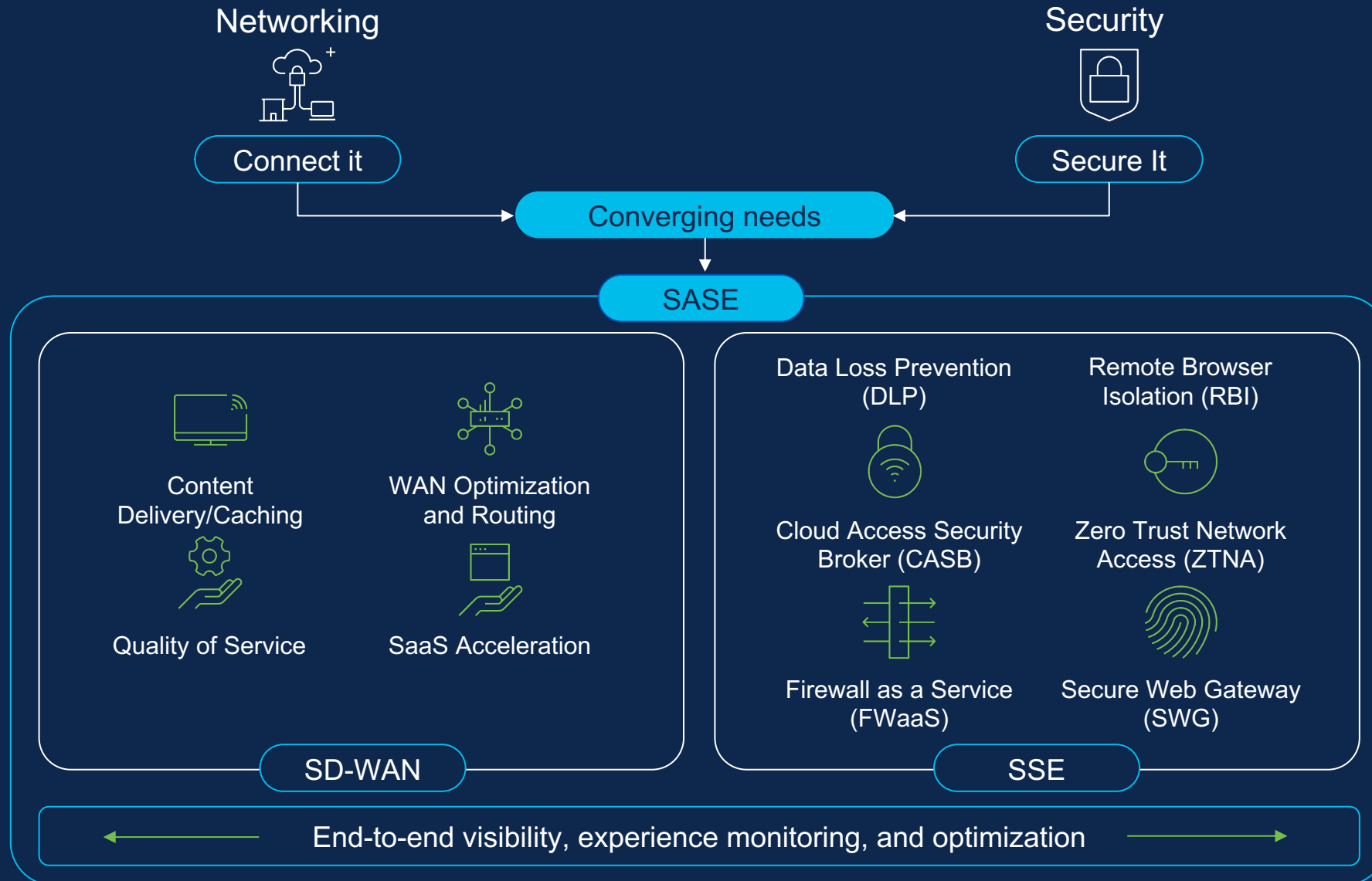
85%

Say they value **simplicity** when it comes to **technology management**

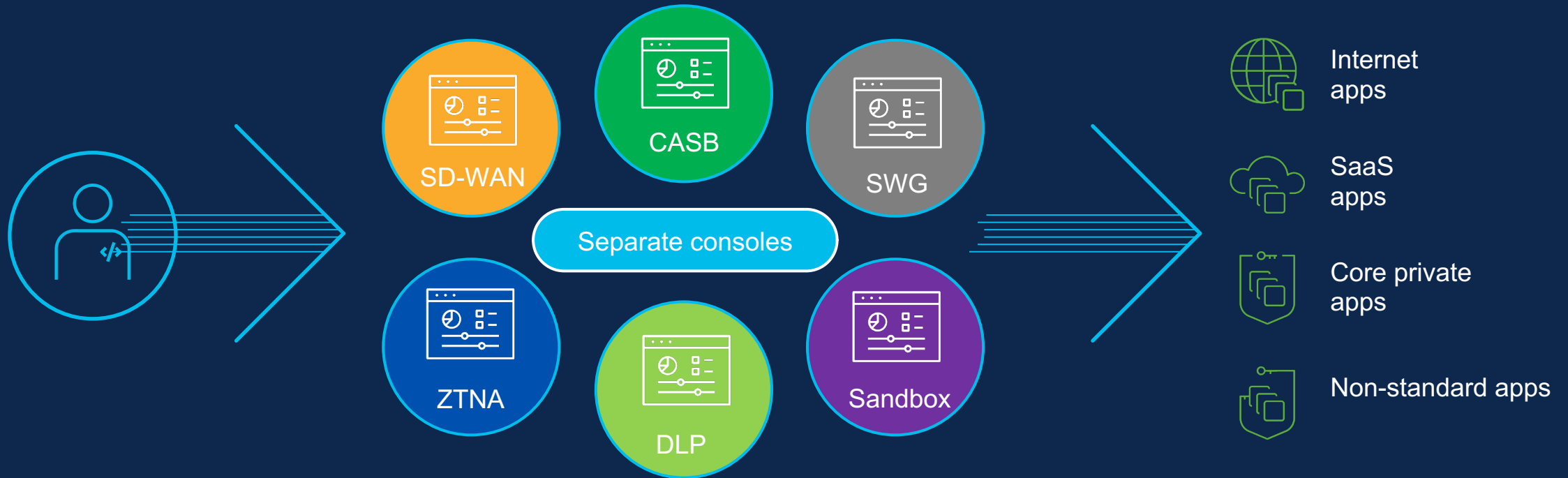


Secure Access Service Edge (SASE)

The architecture for a securely connected experience in today's hyper-distributed environment



Integrované riešenie nie je konvergované riešenie



Multiple products increase cost and inefficiencies

- Licenses/hardware
- Policy management
- Client management
- Reporting
- Elevated staffing levels

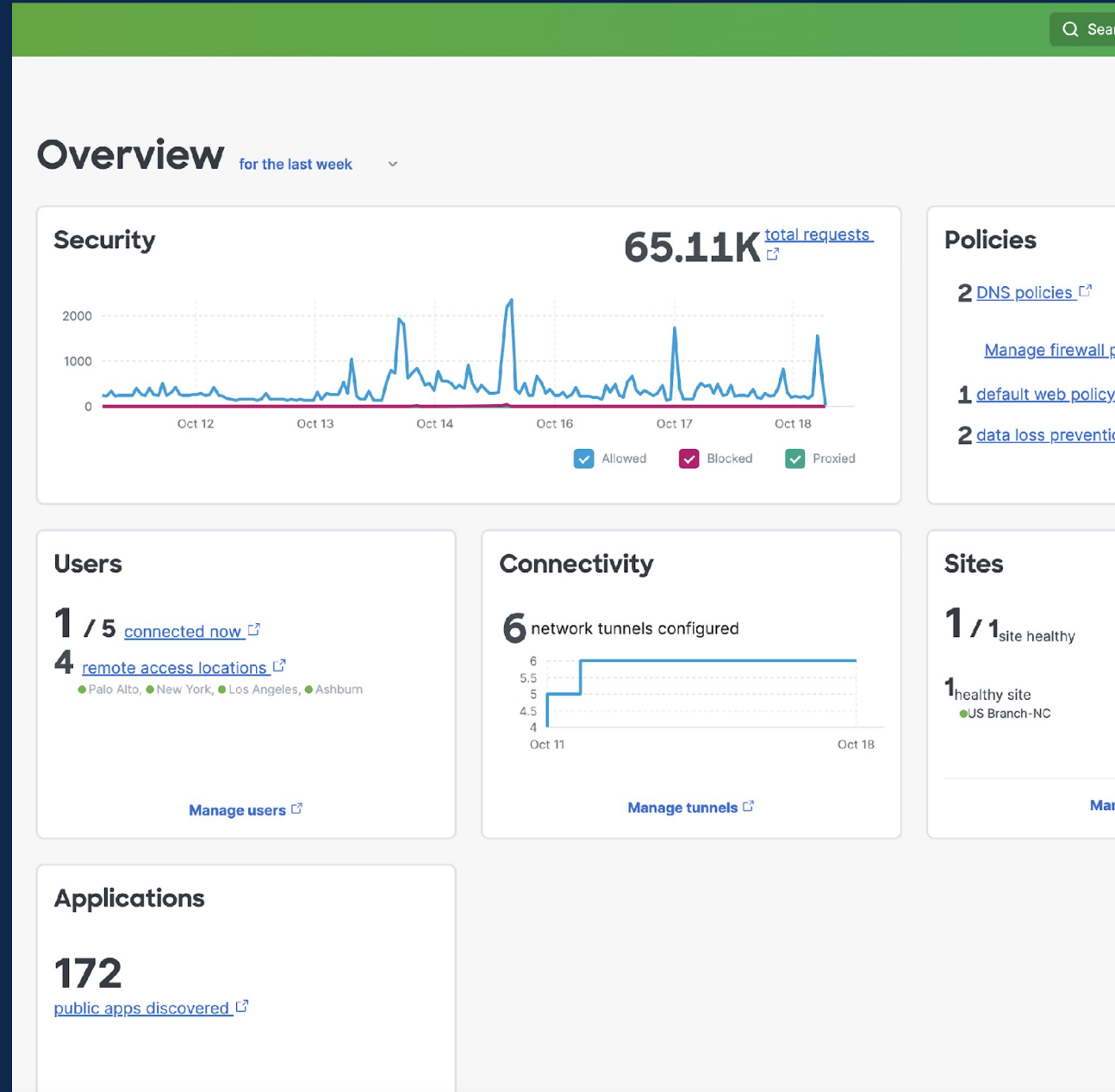
65% of enterprises plan on consolidating vendors for better risk posture

Secure Connect

Jednotné SASE riešenie

Your blueprint for SASE, made easy

Designed with simplicity, Secure Connect is a turnkey solution that creates operational consistency across premises to cloud and unlocks secure hybrid work across branch and remote, delivering greater network resiliency and seamless user experiences, everywhere.



Unifikované Cisco SASE bežiacie na Meraki platforme

Najjednoduchší a najrýchlejší spôsob ochrany vášho podniku pred najnovšími hrozbami



LARGEST CLOUD PLATFORM

12M+

nodes across hundreds of thousands of global customers



FORTUNE 500 COMPANIES

75%

trust the Meraki cloud platform to securely execute their mission



NEW THREAT PROTECTION

<10 mins

for every Meraki customer node to be protected



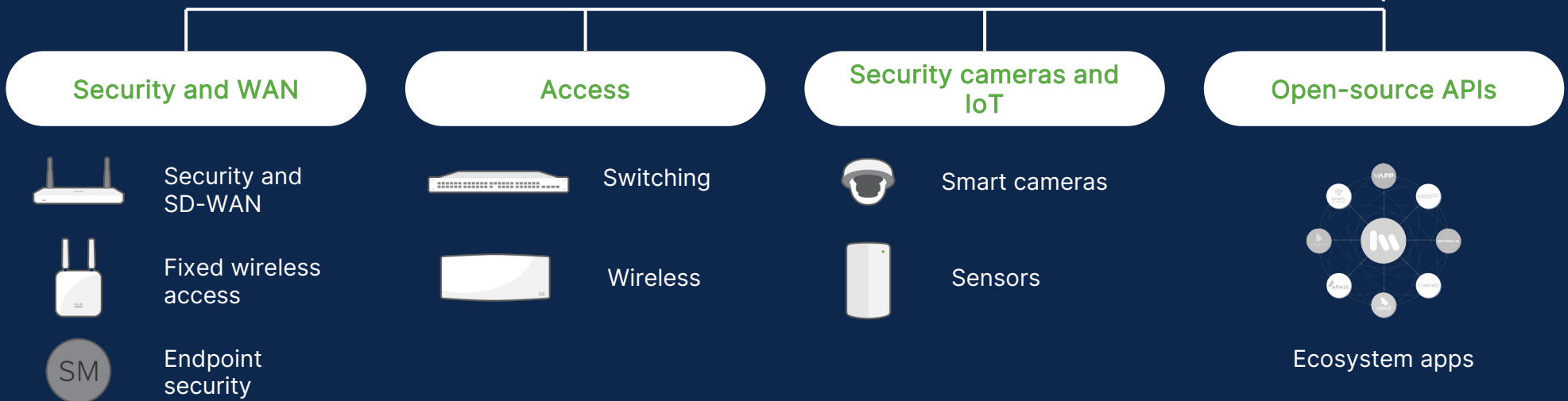
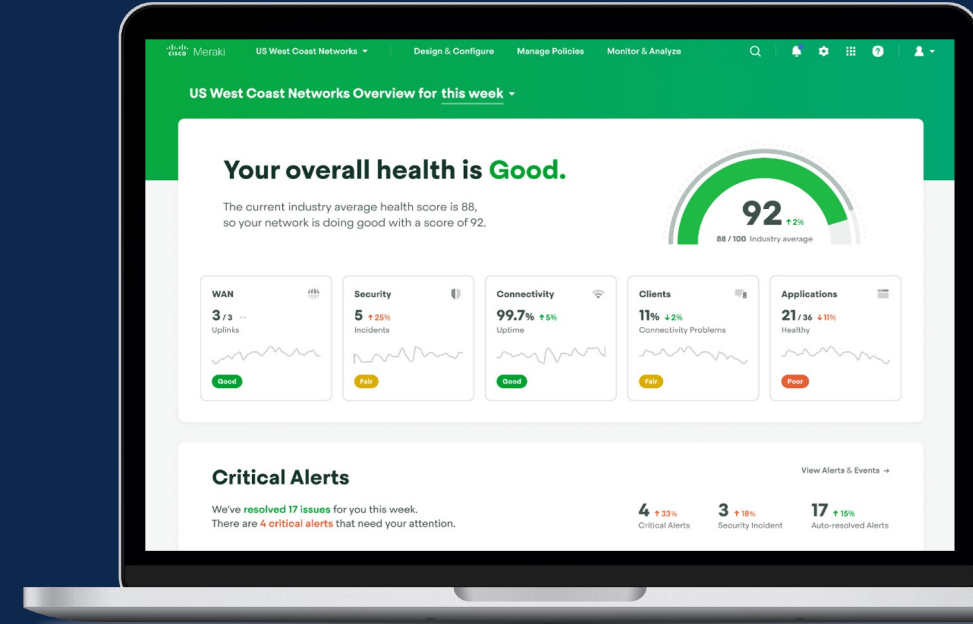
INFOSEC RESOURCES

0

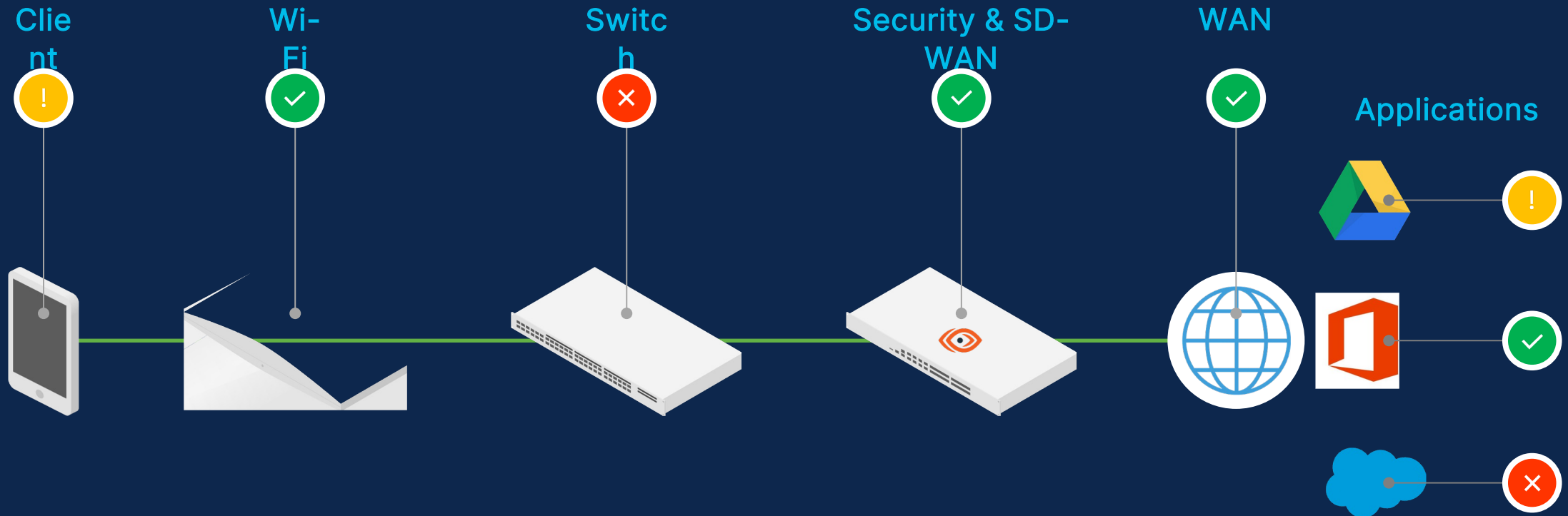
Resources needed to update infrastructure and protect against new threats

Inteligentná cloud platforma Meraki

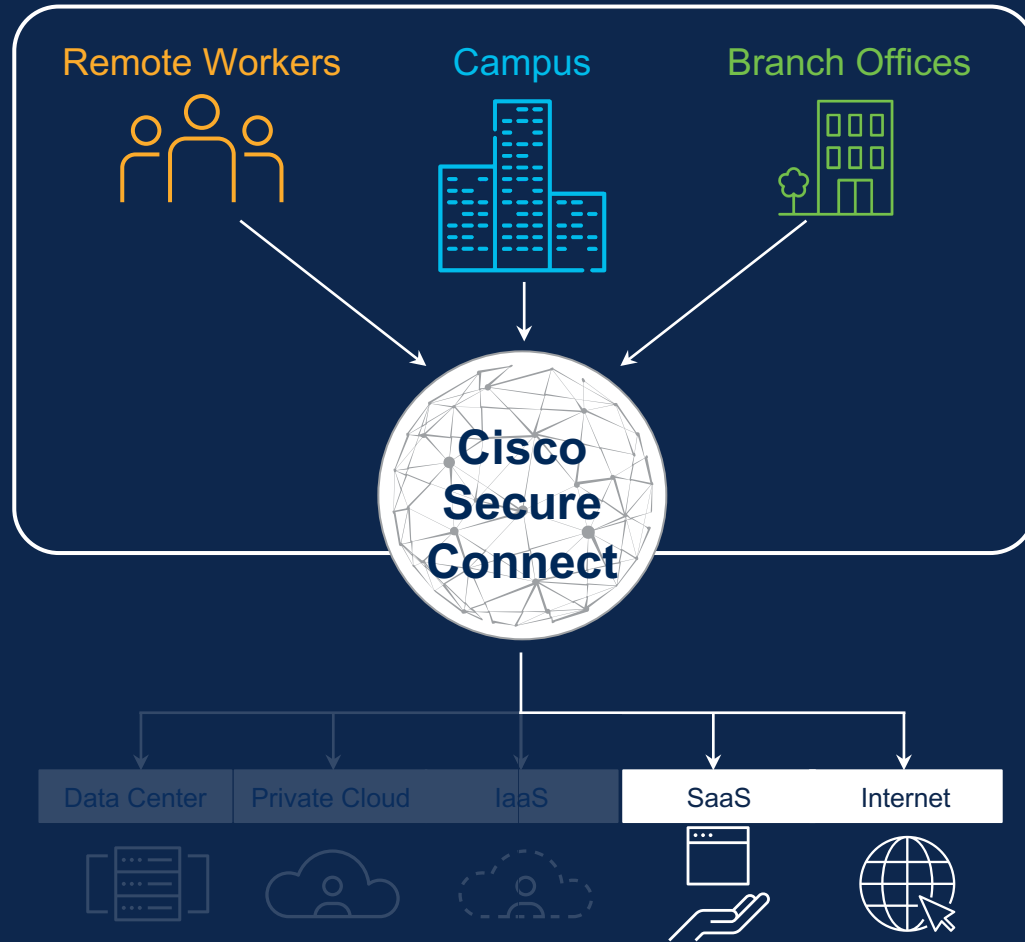
94% of customers save time with a single intuitive dashboard



Unikátny end-to-end prehľad od užívateľa k aplikáciám



Secure Internet Access



DNS Security

- The first line of defense against malware, phishing, botnets and other threats

Cloud Firewall

- Controls access at the IP address and port level to the destinations and protocols end users can access
- Blocks malware and other threats for non-web traffic

Web Security (Secure Web Gateway)

- The Secure Web Gateway inspects and controls access to web traffic to improve performance and block threats

SaaS Security (Cloud Access Security Broker)

- Provides application visibility, and controls access and data sharing with common SaaS applications

Secure Remote Access

Remote Access VPNaaS

- Provides access to private applications hosted in data centers, private clouds or IaaS using the Cisco Secure Client (Anyconnect)

ZTNA – Client / Clientless

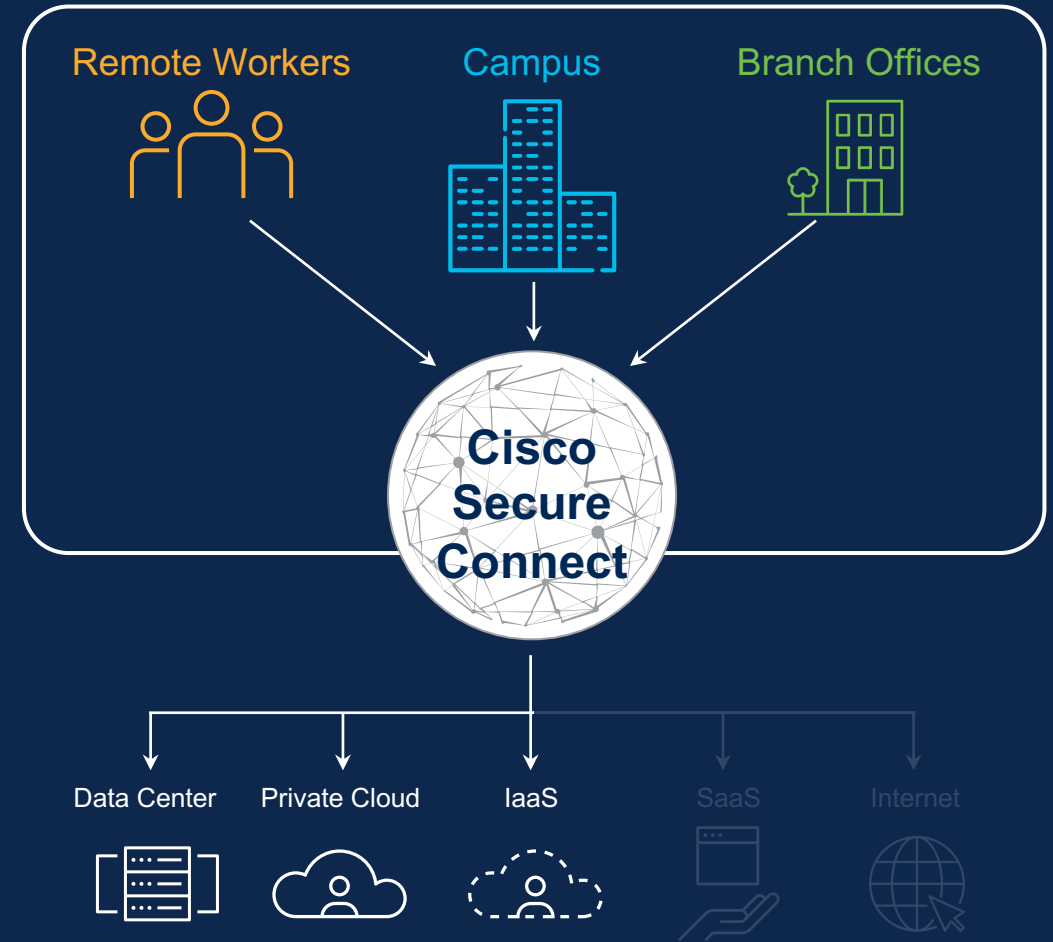
- Frictionless remote access for all applications for managed and unmanaged devices
- Clientless access to private web applications for unmanaged devices (BYOD, contractors, etc.)

Branch Connectivity

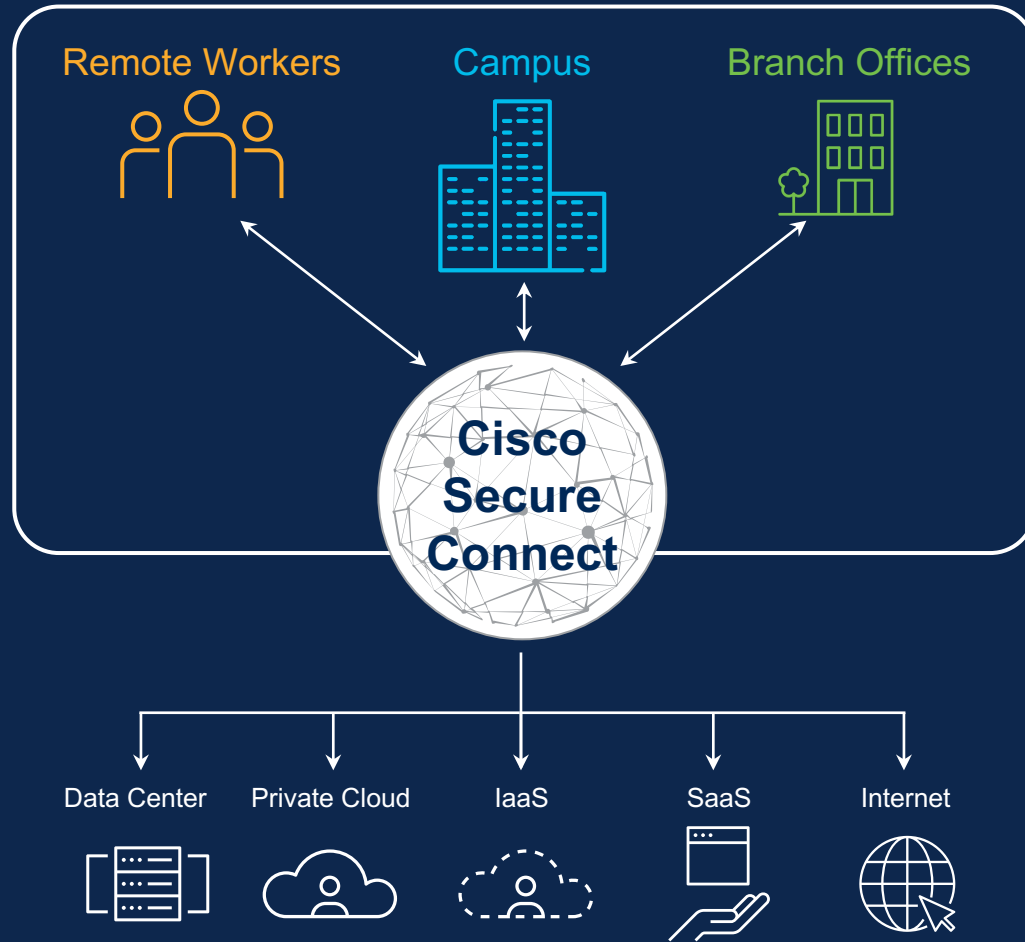
- Enables secure connect of branch offices to private resources on the network

Unified Access Policy

- Provides simple, consistent user access control policies regardless how the user is access the network



Interconnect



Centralized Management

- Configure, monitor and troubleshoot routing and security from a single dashboard

Simplified Setup

- Meraki Auto VPN simplifies setup of VPN tunnels between sites and the Secure Connect cloud
- Cloud-based network fabric simplifies routing setup for Meraki and non-Meraki devices

Network Scalability

- Cloud-based network enables the network scale up without the need to over-engineer the network to handle future expansion

Centralized Management, Distributed Enforcement



Firewall Policies – Secure Con... x

n123.meraki.com/0/A1B2C3/manage/organization/cpsc/firewall_policies

Meraki Demo Networks Search Dashboard


Organization-wide Layer 7 Firewall Policies

Organization rules apply across sites and cloud networks, allowing you to enforce security policies more efficiently. Organization rules are processed after local network rules.

[Organization-wide firewall policy documentation](#)

Rules

Search Filters 0 results + Add rule

<input type="checkbox"/>	#	Status	Rule name	Action	Protocol	Source	Src Port	Destination	Dst Port	Enforcements	
 No rules yet											

Last login about 2 hours ago from your current IP address

Current session started about 2 hours ago

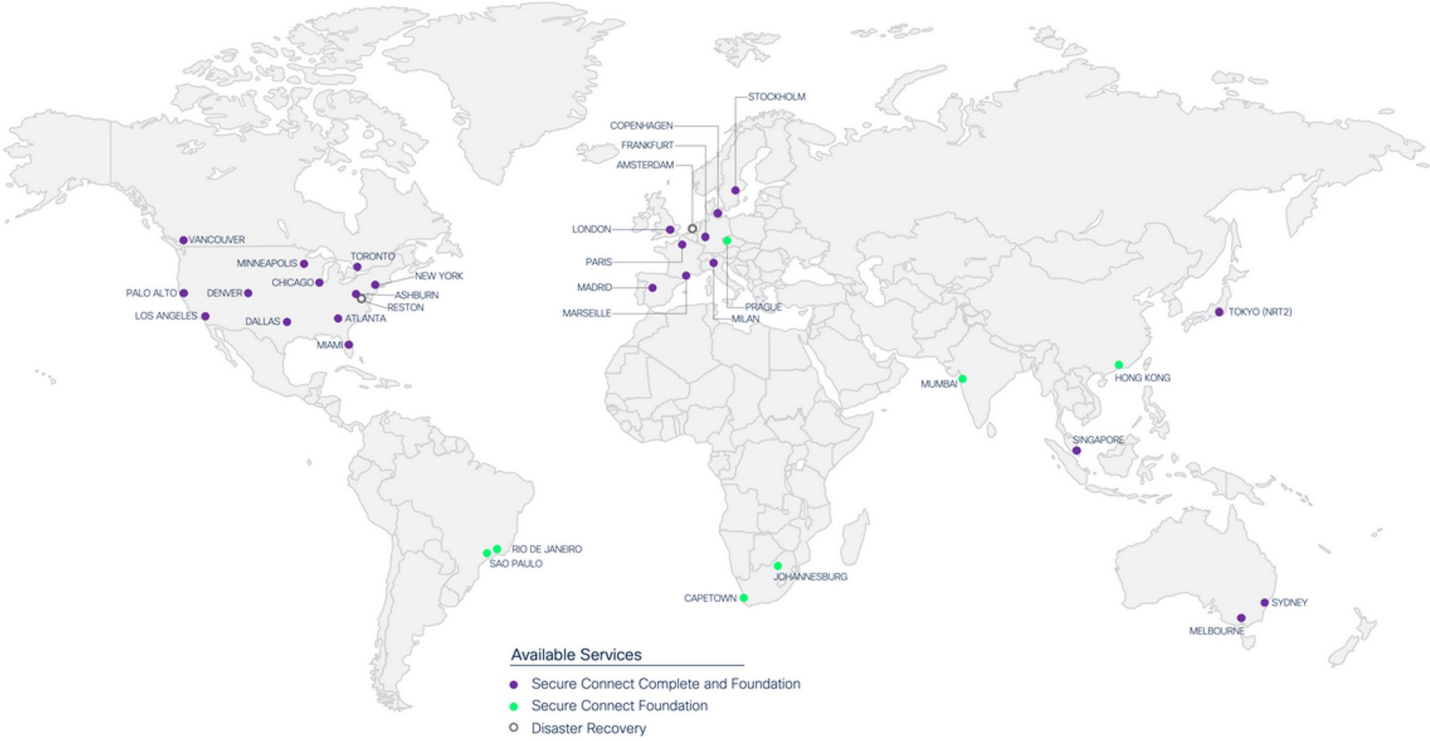
Data for this organization is hosted in North America

© 2023 Cisco Systems, Inc. [Privacy](#) - [Terms](#)

[Give your feedback](#)



Secure Connect Data Centers



Head-End Regions
Assign site directly to these regions Internet & Private App Access
US West Los Angeles/Palo Alto
US Northeast New York/Ashburn
US Central Denver/Dallas
US Southeast Atlanta/Miami
US Midwest Minneapolis/Chicago
Europe-1 London/Frankfurt
Europe-2 Paris/Marseille
Europe-3 Madrid/Milan
Europe-4 Stockholm/Copenhagen
Asia-1 Narita/Singapore
Australia-1 Melbourne/Sydney
Canada-1 Vancouver/Toronto

Cloud Hubs (SIG)
Assign site to Cloud Hub in these regions Internet Access Only Up to 22 Cloud Hubs can be deployed.
Hong Kong/Mumbai ✓
Rio de Janeiro/Sao Paulo
Johannesburg/Cape Town

[Link to updated Meraki documentation page](#)

When possible, migrate to Regions



Jednotná technická podpora naprieč riešením



NETWORK SUPPORT



SECURITY SUPPORT



**SECURE CONNECT
UNIFIED SUPPORT**

Bezpečnostná inteligencia z najväčšieho globálneho výskumného tímu pre hrozby je integrovaná do SASE platformy



DAILY THREATS
BLOCKED

20B

20x more than any
other vendor

DAILY WEB REQUESTS
ANALYZED

625B

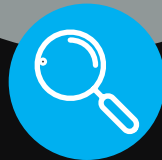
70x more than Google
searches processed
daily



GLOBAL SECURITY
PARTNERS

60+

Government and
law enforcement
partnerships



SECURITY
EXPERTS

500+

of the most sought-after
threat researchers
and scientists

TALOS



The bridge to possible