Efficient Protection from Cyberattacks

Challenges and Solutions

Aleksandar Pavlović, Cisco
Cybersecurity Solutions RSM for CEE

Infosec Conference, Budva, September 26th, 2024

In a hybrid, multi-vendor, multi-vector universe

Everyone is an insider

+30%

of all incidents involved stolen credentials or malicious insiders

Attacks start from anywhere

45%

of breaches occurred in the cloud, and 19% due to a compromise at a business partner

Alert fatigue is worse

37%

of IT and SecOps pros say swelling alert volume, complexity increases job difficulty

Expanding attack surface

22%

increase in the average cost of a data breach where hybrid work was a factor

According to “2024 Cybersecurity Readiness Index”

- Only 3% of companies are ready to tackle today’s threats
- Despite the lack of readiness, 80% of companies feel moderately to very confident in their ability to stay resilient in this evolving cybersecurity landscape
- The industries that ranked the highest in cybersecurity readiness are Financial Services, Technology Services, Media and Communications, and Manufacturing

Source: “2024 Cybersecurity Readiness Index” Cisco survey, August 2024

According to “2024 Cybersecurity Readiness Index”

- Over half of the companies plan to significantly upgrade their IT infrastructure in the next 12-24 months (an increase from 2023 when just one-third said they planned an upgrade)
- In response to the heightened cybersecurity risk, 97% expect to increase their cybersecurity budgets in the next 12 months
- The talent gap persists with nearly 50% of companies having more than 10 open cybersecurity roles
- 11% of companies see AI-related cyber threats among the top three risks in the year ahead

Source: “2024 Cybersecurity Readiness Index” Cisco survey, August 2024

Tactics, Techniques and Procedures (TTPs) that once only impacted nation-states are now being used by every-day attackers

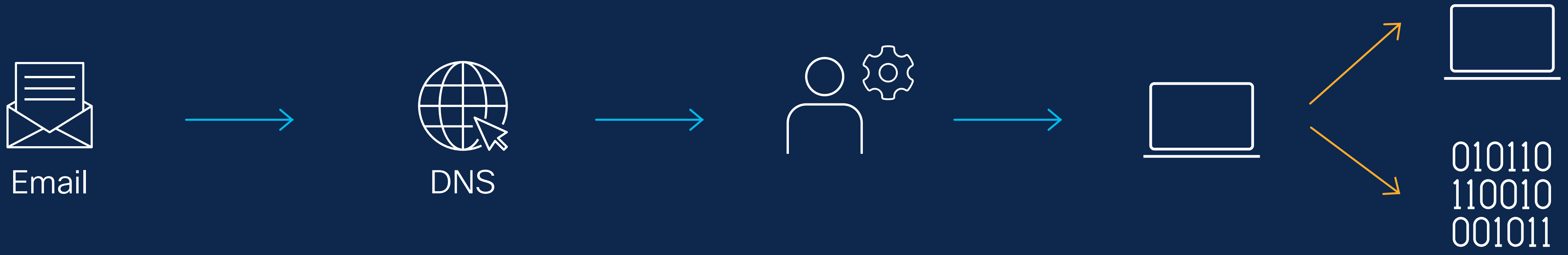
Are everyone's problem now

To address the threats of tomorrow, we need to change how we look at detection and response today

Security Operations Simplified - XDR

Stop advanced threats like ransomware

Most attacks use a sequence like this…



A well-tailored and personalized email causes a user to click…

Which goes to a questionable web site…

Which leads to a strange process being created locally on the user's device…

That process will connect to another machine or directly to their data

T1055: Process Injection

T1566: Spear phishing

T1189: Drive-by Compromise

T1570: Lateral Tool Transfer

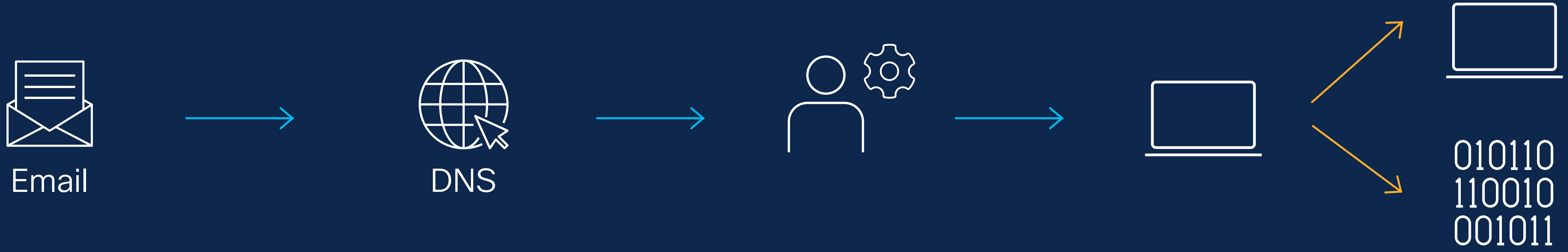
T1087: Account Discovery: Domain Account

T1048: System Network Connections Discovery

Vendor A	Vendor C	Vendor E	Vendor G	Vendor D

Anatomy of a real attack

Most attacks use a sequence like this...



You need a solution that sees deeply across the entire attack chain

Cisco XDR

Built on the Cisco Security Cloud platform

SECURE

The XDR promise

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

Only an effective XDR solution can adapt to the changing nature of the threat

Security tools need to focus on the attacker

Turn potential false positives into validated incidents

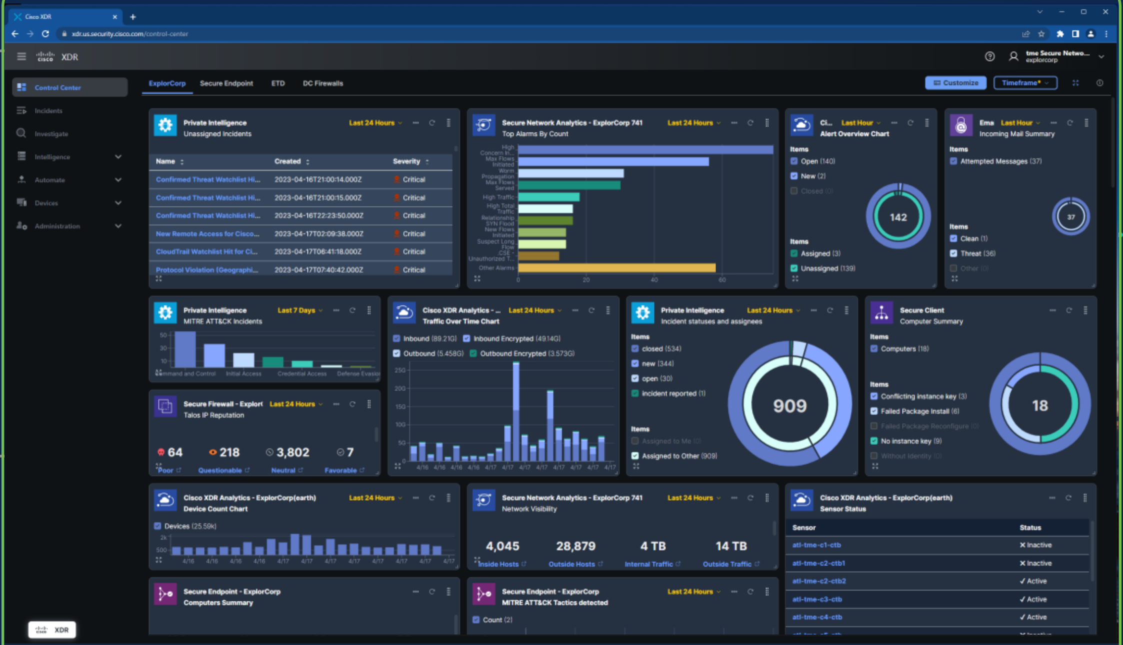
Focus on initial compromise, lateral movement, privilege escalation and data exfiltration

Simplify with Cisco XDR

Cisco

Network | Endpoint | Email

Cloud | Applications | Identity



Private Intelligence
Unassigned Incidents
Last 24 Hours

Name	Created	Severity
Confirmed Threat Watchlist Hi...	2023-04-16T21:00:14.000Z	Critical
Confirmed Threat Watchlist Hi...	2023-04-16T21:00:15.000Z	Critical
Confirmed Threat Watchlist Hi...	2023-04-16T22:23:50.000Z	Critical
New Remote Access for Cisco...	2023-04-17T02:09:38.000Z	Critical
CloudTrail Watchlist Hit for Ci...	2023-04-17T06:41:18.000Z	Critical
Protocol Violation (Geographi...	2023-04-17T07:40:42.000Z	Critical

Cisco XDR Analytics - ExplorCorp(earth)
Sensor Status

Sensor	Status
atl-tme-c1-ctb	✗ Inactive
atl-tme-c2-ctb1	✗ Inactive
atl-tme-c2-ctb2	✓ Active
atl-tme-c3-ctb	✓ Active
atl-tme-c4-ctb	✓ Active

Built on the Cisco security platform

Open and extensible | Clear prioritization | Automation and response guidance | Streamlined investigations

Your Infrastructure

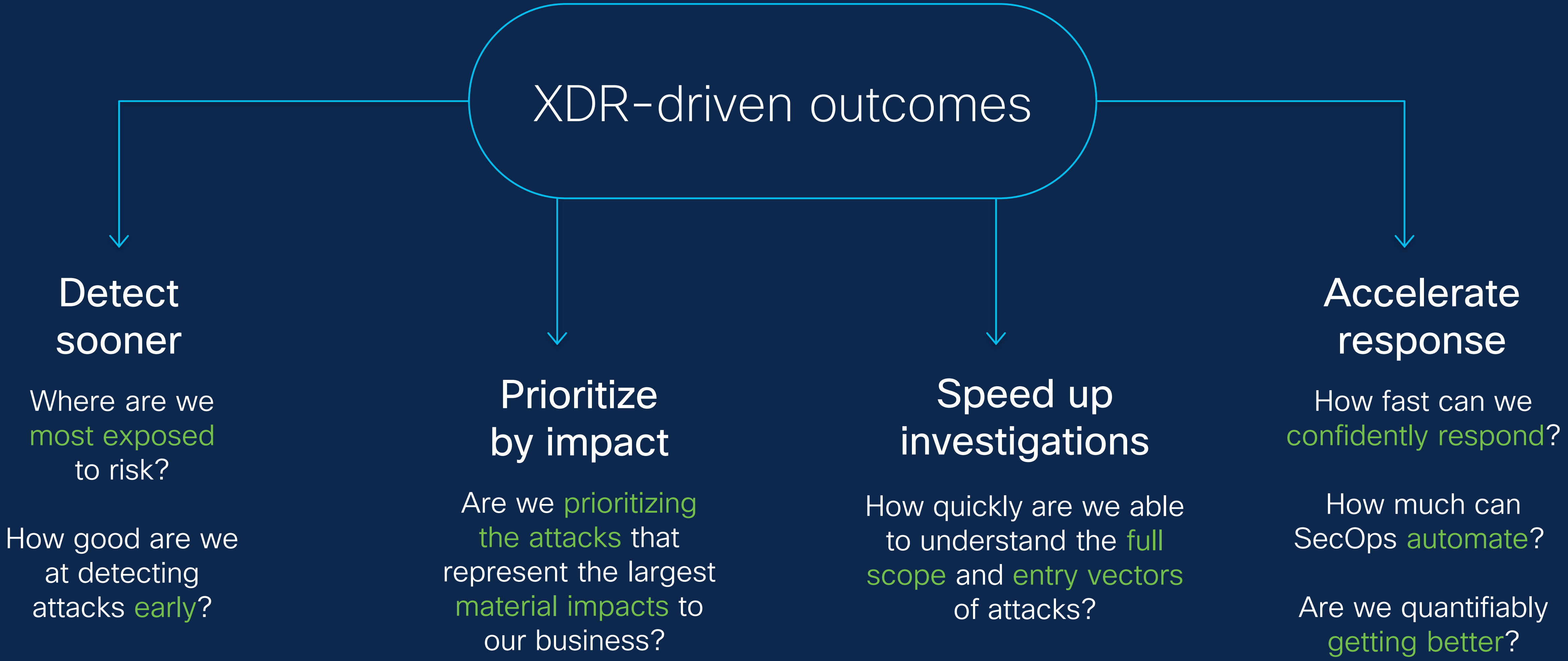
3rd party tools | Intelligence

010110
110010
001011
Others | SIEM/SOAR

Your SOC

SecOps Analyst | CISO | Incident responder

Shift the focus to outcomes



XDR-driven outcomes

Detect sooner

Where are we most exposed to risk?

How good are we at detecting attacks early?

Prioritize by impact

Are we prioritizing the attacks that represent the largest material impacts to our business?

Speed up investigations

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

Accelerate response

How fast can we confidently respond?

How much can SecOps automate?

Are we quantifiably getting better?

CISCO SECURE

Key XDR use cases

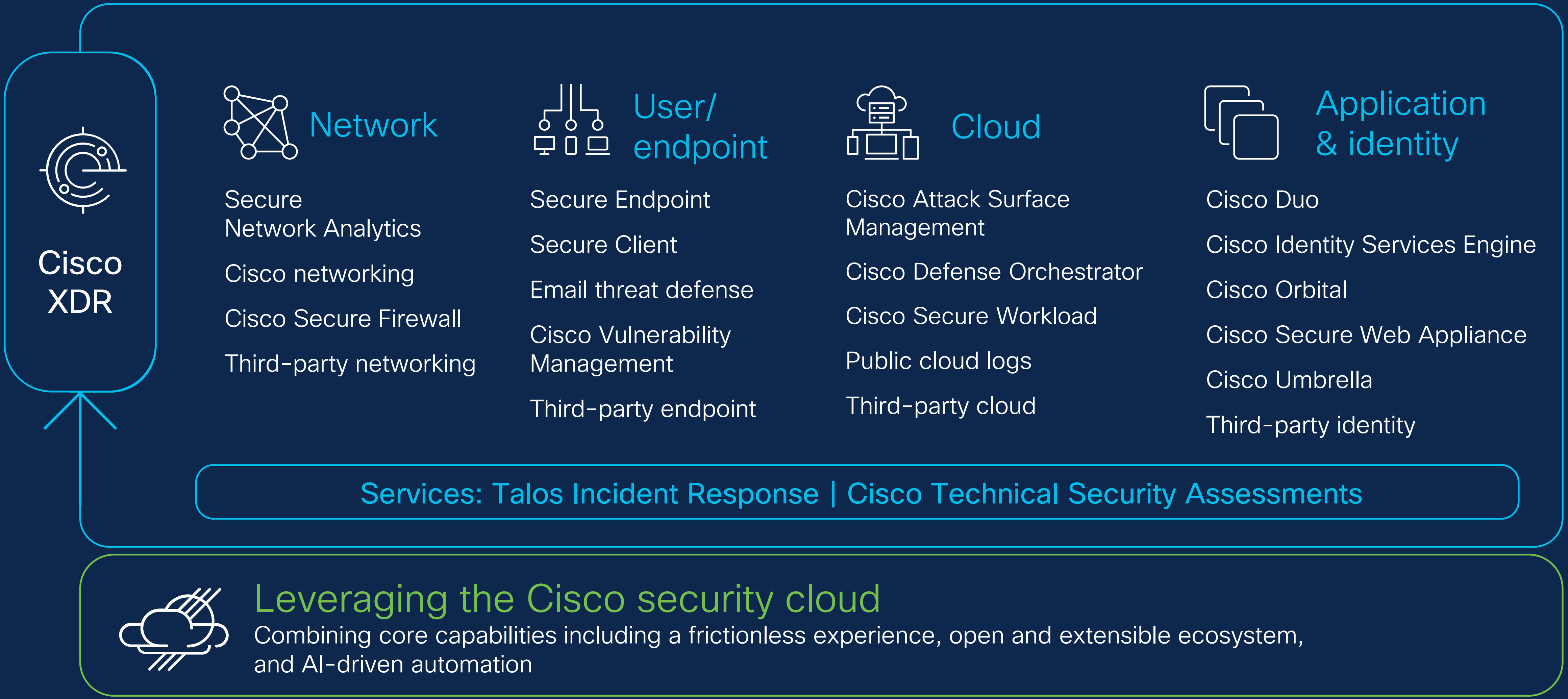
Focus on the most critical security events for immediate attention

Prioritized incident response

Reduce the time between intrusion and discovery of attackers

On-demand threat hunting

Delivering XDR to meet you where you are



Cisco XDR

Network

- Secure Network Analytics
- Cisco networking
- Cisco Secure Firewall
- Third-party networking

User/ endpoint

- Secure Endpoint
- Secure Client
- Email threat defense
- Cisco Vulnerability Management
- Third-party endpoint

Cloud

- Cisco Attack Surface Management
- Cisco Defense Orchestrator
- Cisco Secure Workload
- Public cloud logs
- Third-party cloud

Application & identity

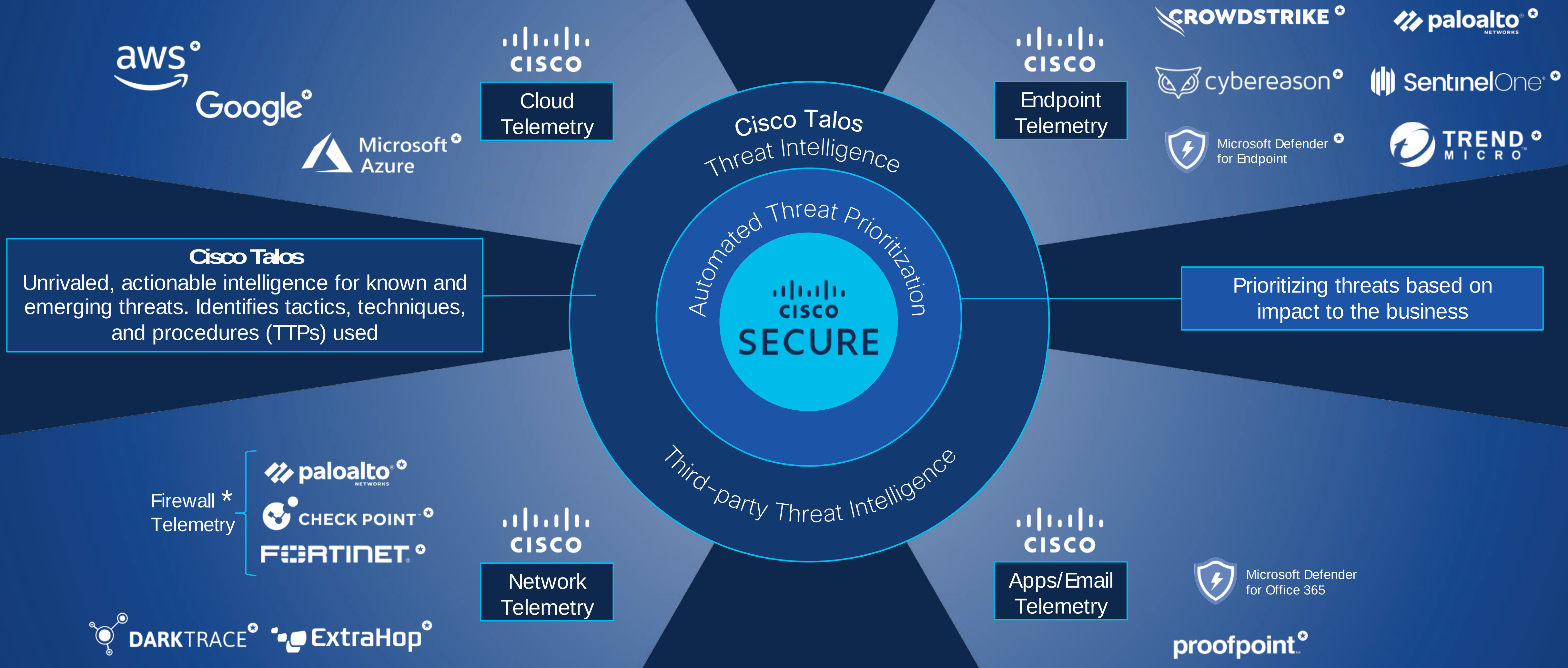
- Cisco Duo
- Cisco Identity Services Engine
- Cisco Orbital
- Cisco Secure Web Appliance
- Cisco Umbrella
- Third-party identity

Services: Talos Incident Response | Cisco Technical Security Assessments

Leveraging the Cisco security cloud

Combining core capabilities including a frictionless experience, open and extensible ecosystem, and AI-driven automation

Strategic integrations to deliver customer outcomes



Cisco Talos
Unrivaled, actionable intelligence for known and emerging threats. Identifies tactics, techniques, and procedures (TTPs) used

Prioritizing threats based on impact to the business

✪ Coming soon

Easy to buy tiers for Cisco XDR

Cisco XDR Essentials

Full featured XDR

Native integration of the Cisco security portfolio enabling analysts to detect and respond to the most sophisticated threats, plus a repository for data ingest and retention

Cisco XDR Advantage

Full featured XDR

+

Commercially supported and curated integrations with select third-party security solutions

Cisco XDR Premier

Full featured XDR

+

Third-party integrations

+

Cisco Secure Managed Detection and Response

+

Cisco Talos Incident Response

+

Cisco Technical Security Assessment

The Cisco approach to XDR

Detect more, act faster, elevate productivity, build resilience

Detect the most sophisticated threats

- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimized for multi-vendor environments

Act on what **truly** matters, faster

- Prioritize threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations

Elevate productivity

- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks

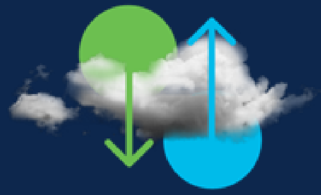
Build resilience

- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, everyday with continuous, quantifiable improvement

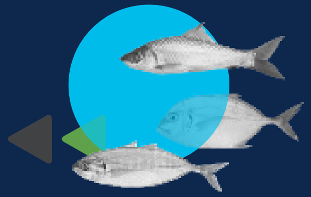
Increasing demands on Security Teams

Business evolution

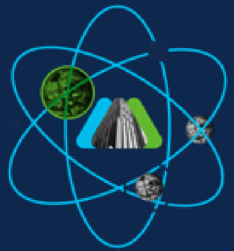
Unlimited devices



Transition to the cloud

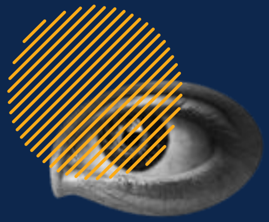


Distributed workforces



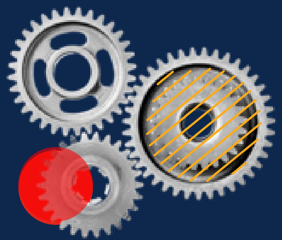
Digital transformation

Security pressures



Too little visibility

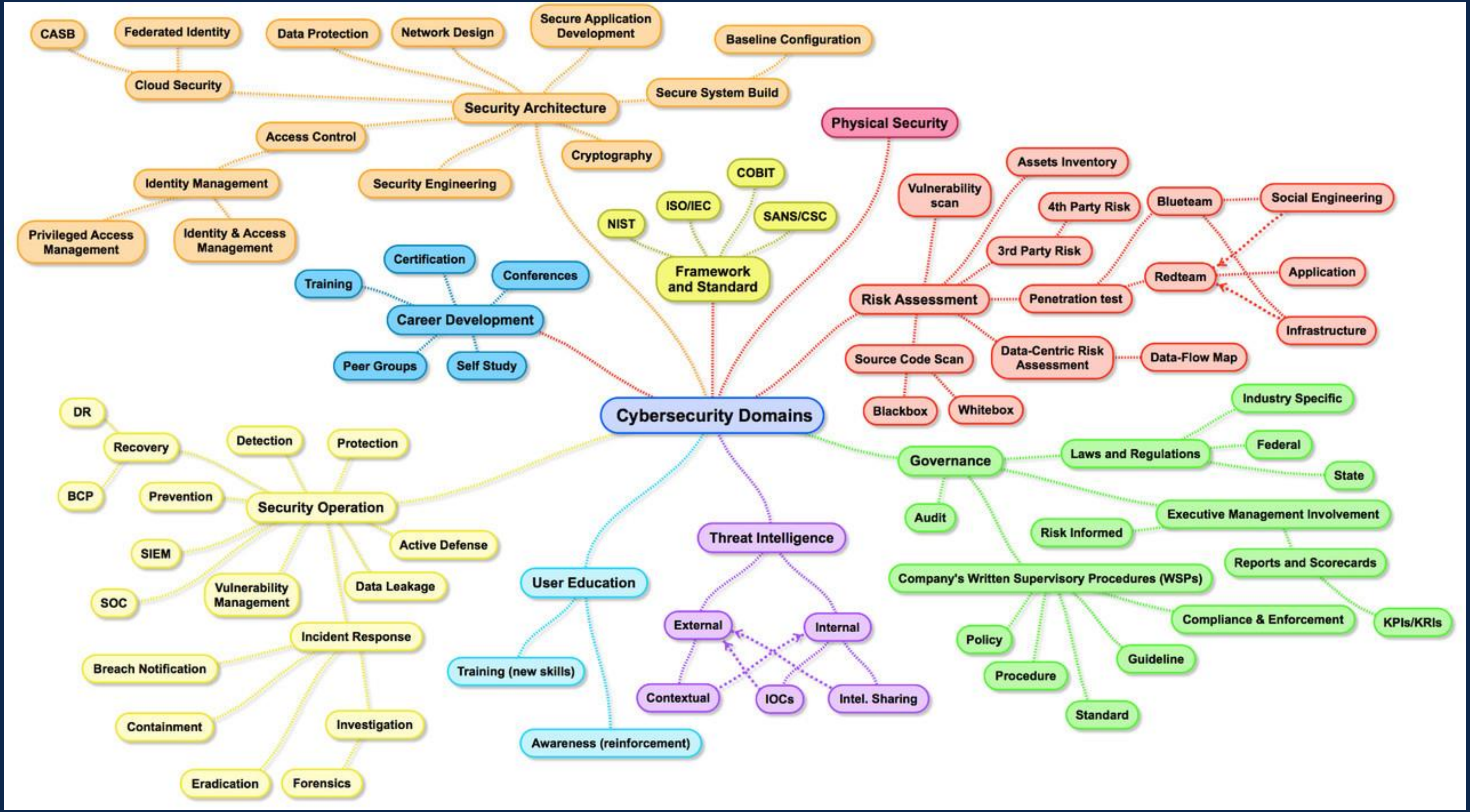
Too few experts



Too little integration

Too much exposure

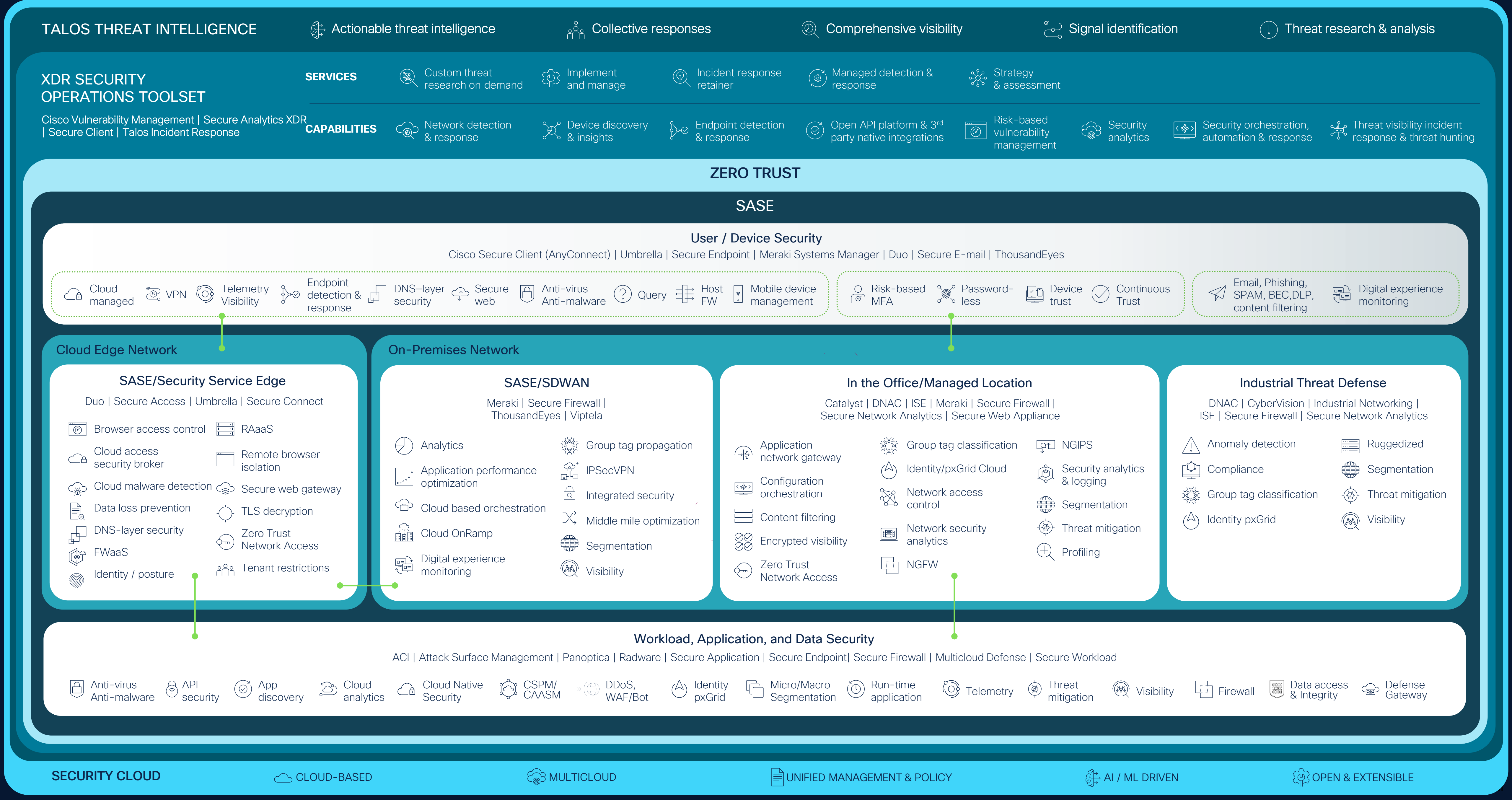
Cybersecurity Domains



- Cybersecurity Domains
  - Security Architecture
    - Cloud Security
      - CASB
      - Federated Identity
    - Data Protection
    - Network Design
    - Secure Application Development
    - Secure System Build
      - Baseline Configuration
    - Access Control
      - Identity Management
        - Privileged Access Management
        - Identity & Access Management
    - Security Engineering
    - Cryptography
  - Physical Security
  - Framework and Standard
    - NIST
    - ISO/IEC
    - COBIT
    - SANS/CSC
  - Risk Assessment
    - Vulnerability scan
    - Assets Inventory
    - 3rd Party Risk
      - 4th Party Risk
    - Penetration test
      - Blueteam
      - Redteam
        - Social Engineering
        - Application
        - Infrastructure
    - Source Code Scan
      - Blackbox
      - Whitebox
    - Data-Centric Risk Assessment
      - Data-Flow Map
  - Career Development
    - Training
    - Certification
    - Conferences
    - Peer Groups
    - Self Study
  - Security Operation
    - Recovery
      - DR
      - BCP
    - Detection
    - Protection
    - Prevention
    - Active Defense
    - SIEM
    - SOC
    - Vulnerability Management
    - Data Leakage
    - Incident Response
      - Breach Notification
      - Containment
      - Eradication
      - Forensics
      - Investigation
  - User Education
    - Training (new skills)
    - Awareness (reinforcement)
  - Threat Intelligence
    - External
    - Internal
    - Contextual
    - IOCs
    - Intel. Sharing
  - Governance
    - Laws and Regulations
      - Industry Specific
      - Federal
      - State
    - Audit
    - Executive Management Involvement
      - Risk Informed
      - Reports and Scorecards
        - KPIs/KRIs
    - Company's Written Supervisory Procedures (WSPs)
      - Policy
      - Procedure
      - Standard
      - Guideline
      - Compliance & Enforcement

Security Reference Architecture

cisco.com/go/sra



TALOS THREAT INTELLIGENCE

Actionable threat intelligence | Collective responses | Comprehensive visibility | Signal identification | Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management | Secure Analytics XDR | Secure Client | Talos Incident Response

SERVICES

- Custom threat research on demand
- Implement and manage
- Incident response retainer
- Managed detection & response
- Strategy & assessment

CAPABILITIES

- Network detection & response
- Device discovery & insights
- Endpoint detection & response
- Open API platform & 3rd party native integrations
- Risk-based vulnerability management
- Security analytics
- Security orchestration, automation & response
- Threat visibility incident response & threat hunting

ZERO TRUST

SASE

User / Device Security

Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes

- Cloud managed
- VPN
- Telemetry Visibility
- Endpoint detection & response
- DNS–layer security
- Secure web
- Anti-virus Anti-malware
- Query
- Host FW
- Mobile device management

- Risk-based MFA
- Password-less
- Device trust
- Continuous Trust

- Email, Phishing, SPAM, BEC,DLP, content filtering
- Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect

- Browser access control
- Cloud access security broker
- Cloud malware detection
- Data loss prevention
- DNS-layer security
- FWaaS
- Identity / posture
- RAaaS
- Remote browser isolation
- Secure web gateway
- TLS decryption
- Zero Trust Network Access
- Tenant restrictions

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Viptela

- Analytics
- Application performance optimization
- Cloud based orchestration
- Cloud OnRamp
- Digital experience monitoring
- Group tag propagation
- IPSecVPN
- Integrated security
- Middle mile optimization
- Segmentation
- Visibility

In the Office/Managed Location

Catalyst | DNAC | ISE | Meraki | Secure Firewall | Secure Network Analytics | Secure Web Appliance

- Application network gateway
- Configuration orchestration
- Content filtering
- Encrypted visibility
- Zero Trust Network Access
- Group tag classification
- Identity/pxGrid Cloud
- Network access control
- Network security analytics
- NGFW
- NGIPS
- Security analytics & logging
- Segmentation
- Threat mitigation
- Profiling

Industrial Threat Defense

DNAC | CyberVision | Industrial Networking | ISE | Secure Firewall | Secure Network Analytics

- Anomaly detection
- Compliance
- Group tag classification
- Identity pxGrid
- Ruggedized
- Segmentation
- Threat mitigation
- Visibility

Workload, Application, and Data Security

ACI | Attack Surface Management | Panoptica | Radware | Secure Application | Secure Endpoint| Secure Firewall | Multicloud Defense | Secure Workload

- Anti-virus Anti-malware
- API security
- App discovery
- Cloud analytics
- Cloud Native Security
- CSPM/ CAASM
- DDoS, WAF/Bot
- Identity pxGrid
- Micro/Macro Segmentation
- Run-time application
- Telemetry
- Threat mitigation
- Visibility
- Firewall
- Data access & Integrity
- Defense Gateway

SECURITY CLOUD

CLOUD-BASED | MULTICLOUD | UNIFIED MANAGEMENT & POLICY | AI / ML DRIVEN | OPEN & EXTENSIBLE

Security innovation
is a
Lookout
COALFIRE
red canary
McAfee
passbase
clearswift
CHECK POINT
FusionAuth
proofpoint
okta
Ping Identity
sophos
solarwind
deepwatch
KnowBe4
U410
CROWDSTRIKE
paloalto
hackerone
FORCEPOINT
axio
GoGuardian
NowSecure
VARONIS
HUNTRESS
DARKTRACE
RAPID7
zscaler
SecureAuth

Security Innovation is a Patchwork

New threats spawn new vendors, putting the burden on customers.

Result

3.500+ cyber security vendors in the market

76 security tools used per enterprise today on average

Source: CyberDB

A Modern Approach to Business Resilience and Employee Satisfaction: Secure Access

Current patchwork approach exacerbates the problem

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*

SECURE

*Source: “Keys to Successful SSE”, ESG global survey. June 2023

Customer top priorities address the challenges

Boost Productivity

Empower users to
do their best work

Optimize Costs

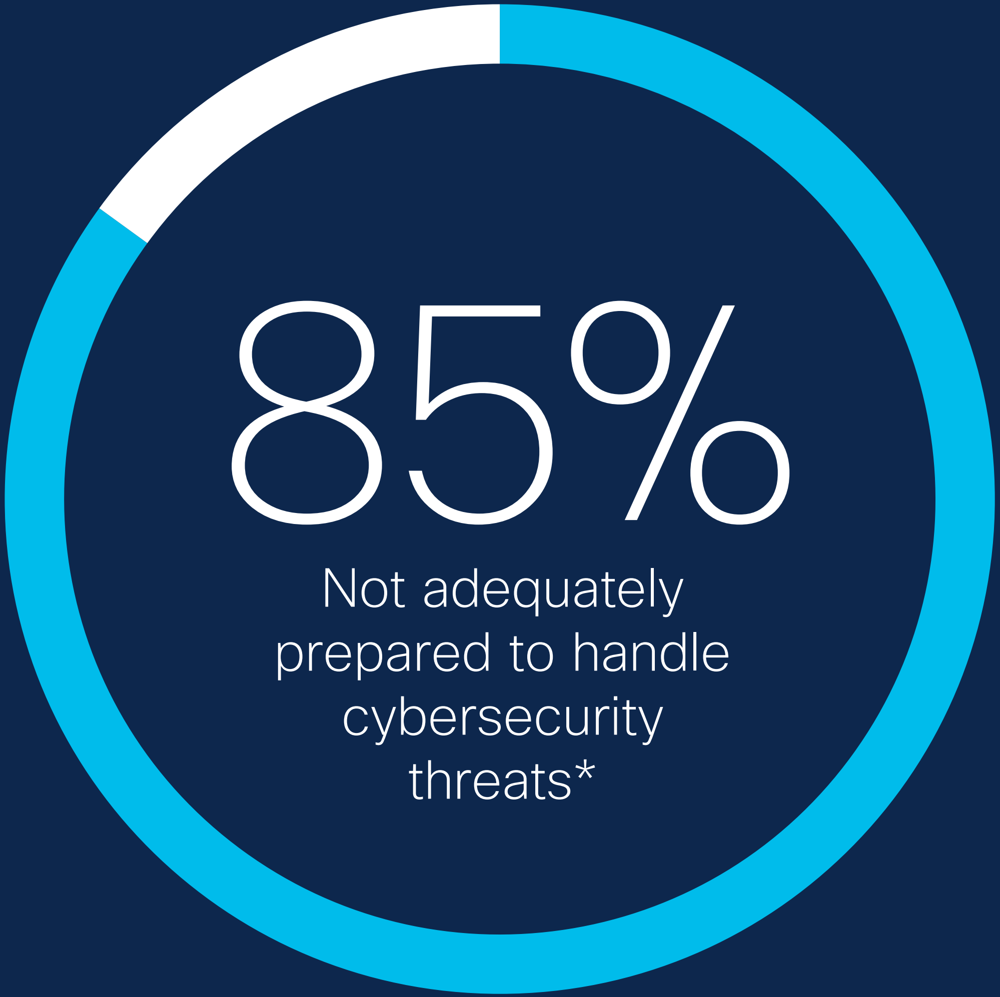
Address inefficiencies

Minimize Risk

Secure your organization

Hybrid work era creates unmanageable risk

Highly distributed environments make secure connectivity hard



85%

Not adequately prepared to handle cybersecurity threats*

*Source: Cybersecurity Readiness Index – Cisco: March, 2023

According to “2024 Cybersecurity Readiness Index”

Employees are working and accessing data from anywhere, on multiple devices, and leveraging an array of applications from secured and unsecured networks.

- 85% of companies say their employees access company platforms from unmanaged devices
- 43% of those spend 20% of their time logged onto company networks from unmanaged devices
- 29% reported their employees hop between at least six networks throughout a week

Source: “2024 Cybersecurity Readiness Index” Cisco survey, August 2024

According to “2024 Cybersecurity Readiness Index”

- Hyperconnectivity is creating vulnerabilities. Readiness is critical, as 73% said a cybersecurity incident will likely disrupt their business in the next 12 to 24 months
- The cost can be substantial, as 54% said they experienced a cybersecurity incident in the last 12 months, and 52% of those affected said it cost them at least US$300,000
- Threats ranging from malware and phishing to ransomware, supply chain, and social engineering cyber attacks

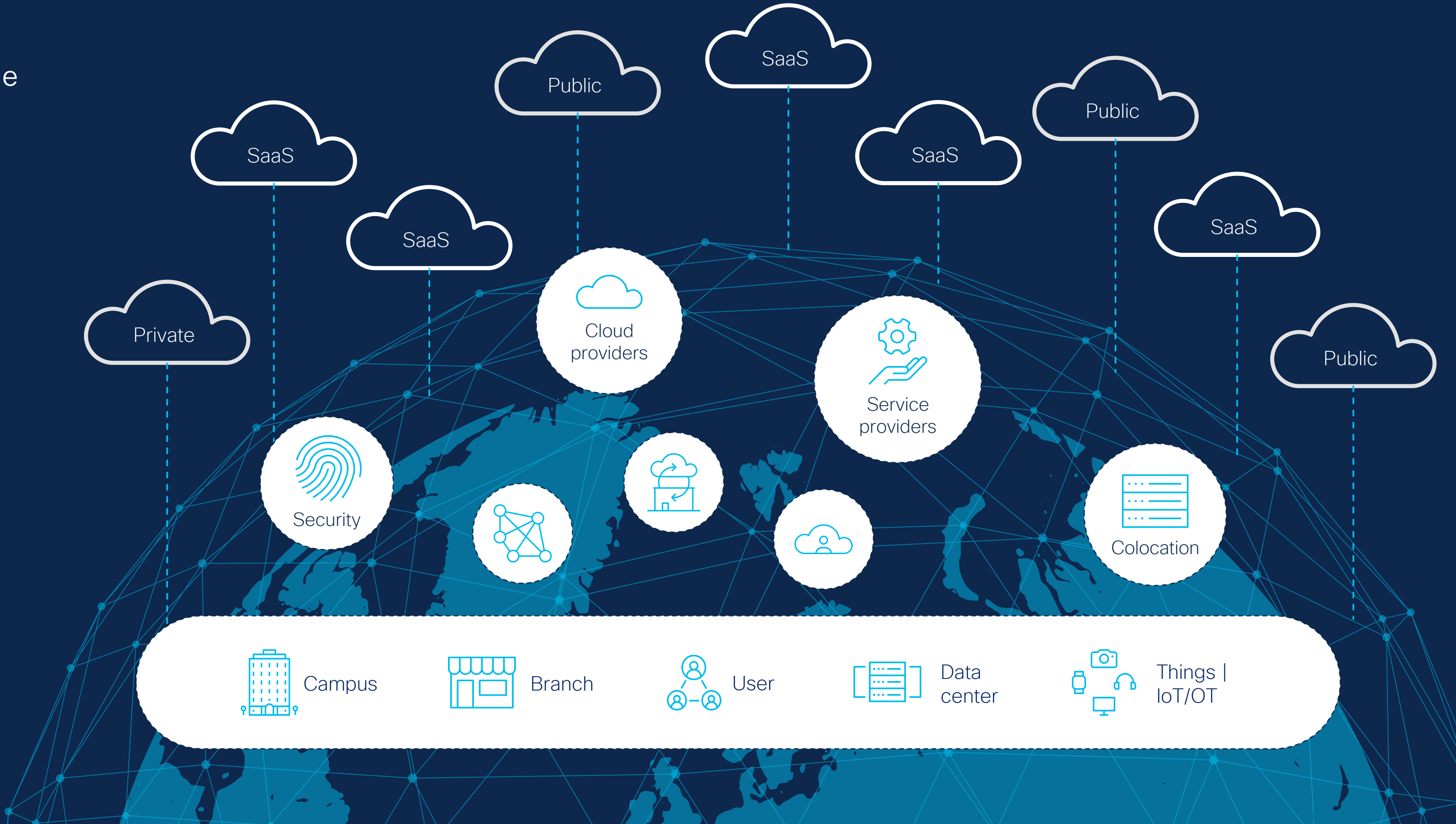
Source: “2024 Cybersecurity Readiness Index” Cisco survey, August 2024

Highly distributed and diverse IT landscape makes secure connectivity hard

41% Say securing user access to cloud-based applications and mobile devices or cloud-based solutions is their biggest obstacle

86% See having a consistent operational model across on-prem, private cloud, public cloud, and SaaS as important

85% Say they value simplicity when it comes to technology management



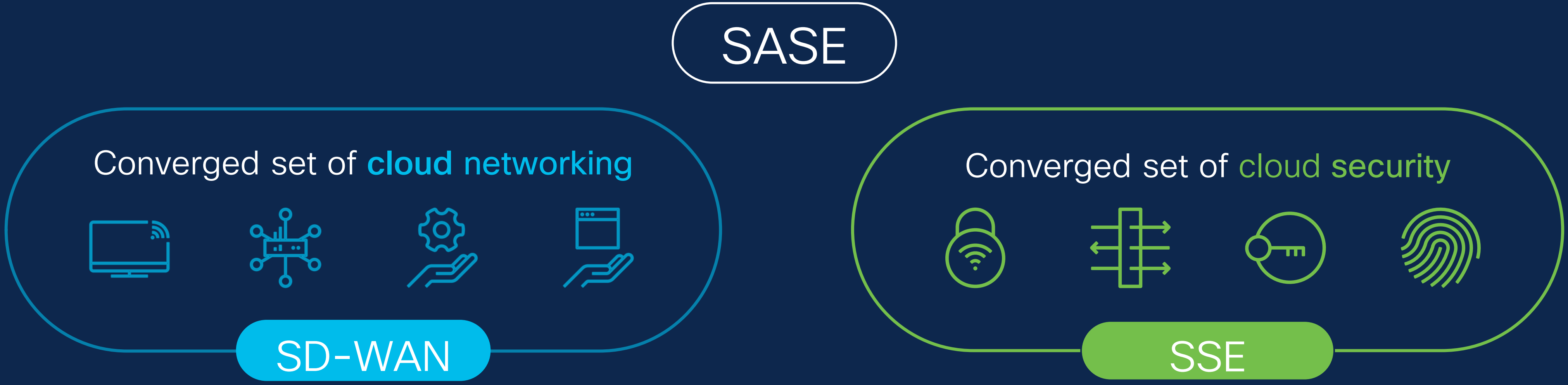
Source: 2023 Global Networking Trends Report, Cisco

SASE/SSE approach is the technology foundation

Fundamental to your security strategy for a hyper-distributed world

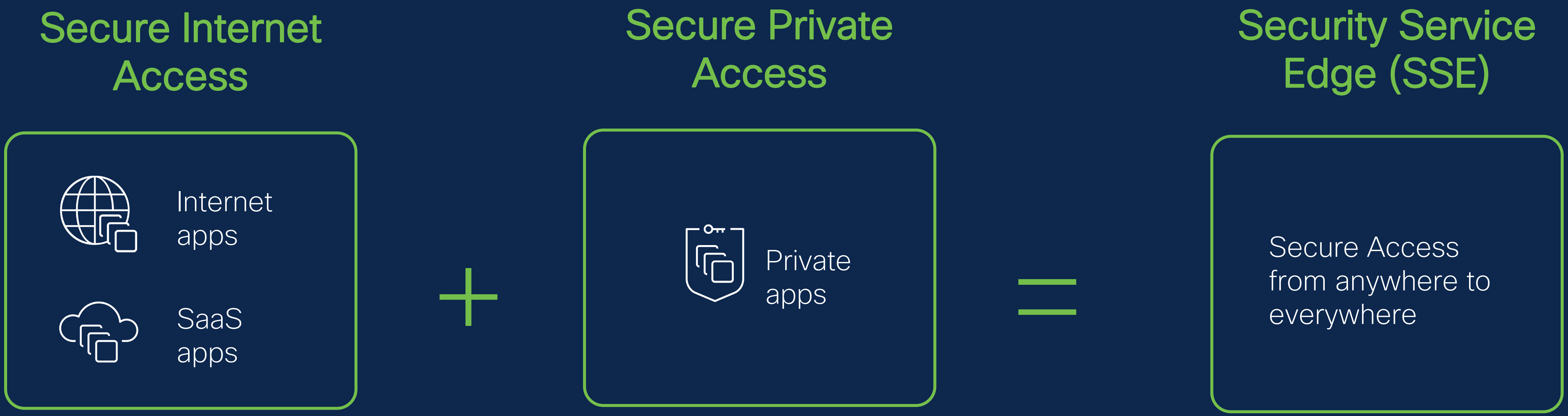
SASE brings networking & security capabilities into a single-service, cloud-native model to address today's challenges.

65% plan on adopting SSE in next 2 years



SASE
Converged set of **cloud networking**
SD-WAN
Converged set of cloud **security**
SSE

Customer priority use cases



Secure Internet Access

Internet apps

SaaS apps

+

Secure Private Access

Private apps

=

Security Service Edge (SSE)

Secure Access from anywhere to everywhere

Introducing an innovative new solution: Cisco Secure Access

Better for users, easier for IT, and safer for everyone

cisco SECURE

Introducing Cisco Secure Access

Proven cloud-native security converged into one service

Umbrella DNS
>12 years

Umbrella SWG
>5 years

DUO Posture
>4 years

Umbrella CASB
>5 years

RBI
>5 years

ZTNA
>4 years

Secure Client
>3 years

VPN Termination
>10 years

Cloud Firewall
>5 years

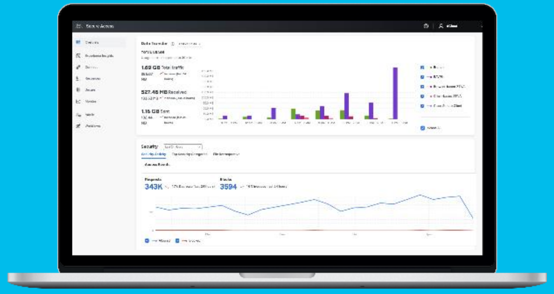
Umbrella DLP
>5 years

Umbrella Advanced Malware Protection
>7 years

Experience Insights/DEM (ThousandEyes)
>3 years

Protecting 70,000+ customers | More than 220M endpoints

Cisco Secure Access



- Single Console
- Single Client
- Unified Policies

Cisco Secure Access

Modernize your defense with converged cloud security grounded in zero trust

Better for Users

Empower their best work with a frictionless user experience

Easier for IT

Lower cost and increase efficiencies

Safer for Everyone

Reduce risk and improve business resilience

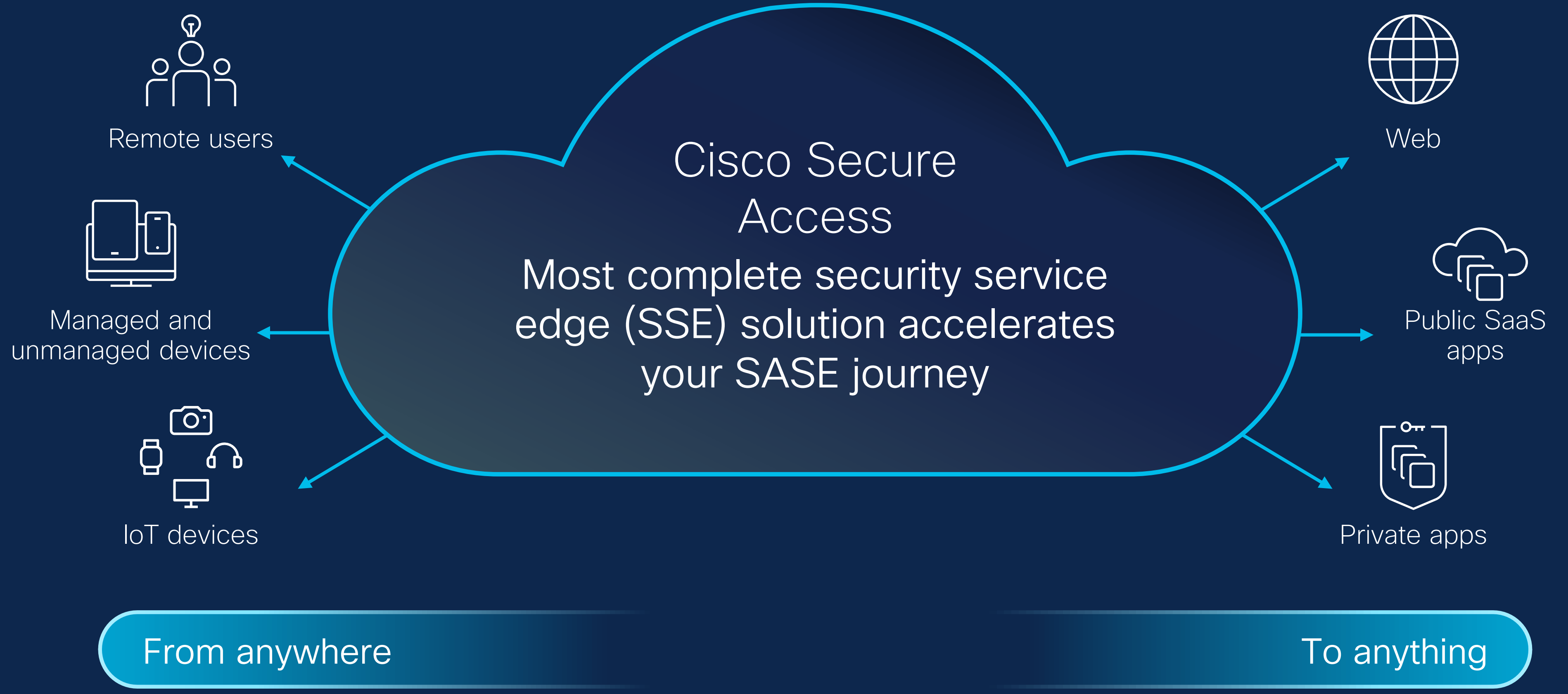
Imagine cybersecurity that's

safer and easier for everyone

CISCO SECURE

Introducing Cisco Secure Access

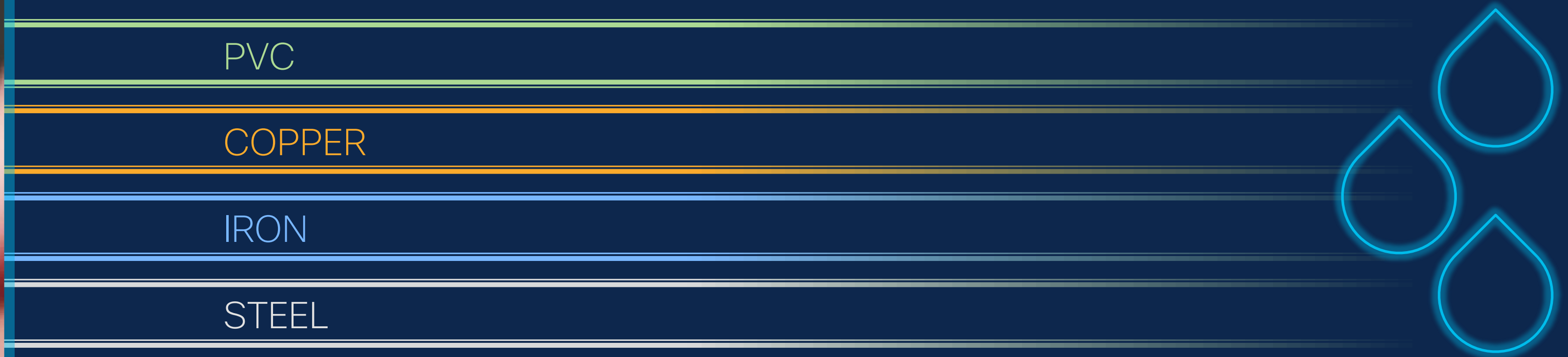
Modernize your defense with converged cloud security grounded in zero trust



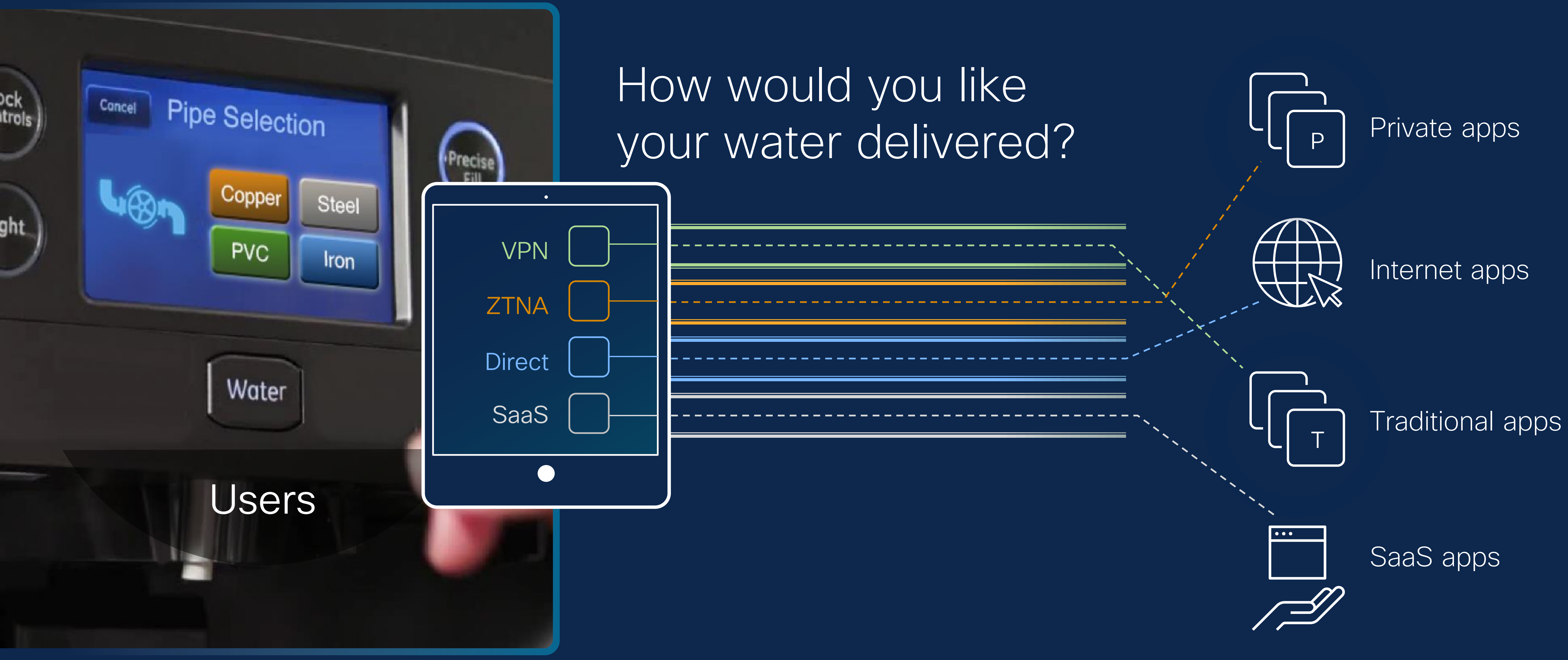
Cisco Secure Access

Most complete security service edge (SSE) solution accelerates your SASE journey

ock
ntrols
Cancel
Pipe Selection
Copper
Steel
PVC
Iron
Precise Fill
Hot Water
ght
Water

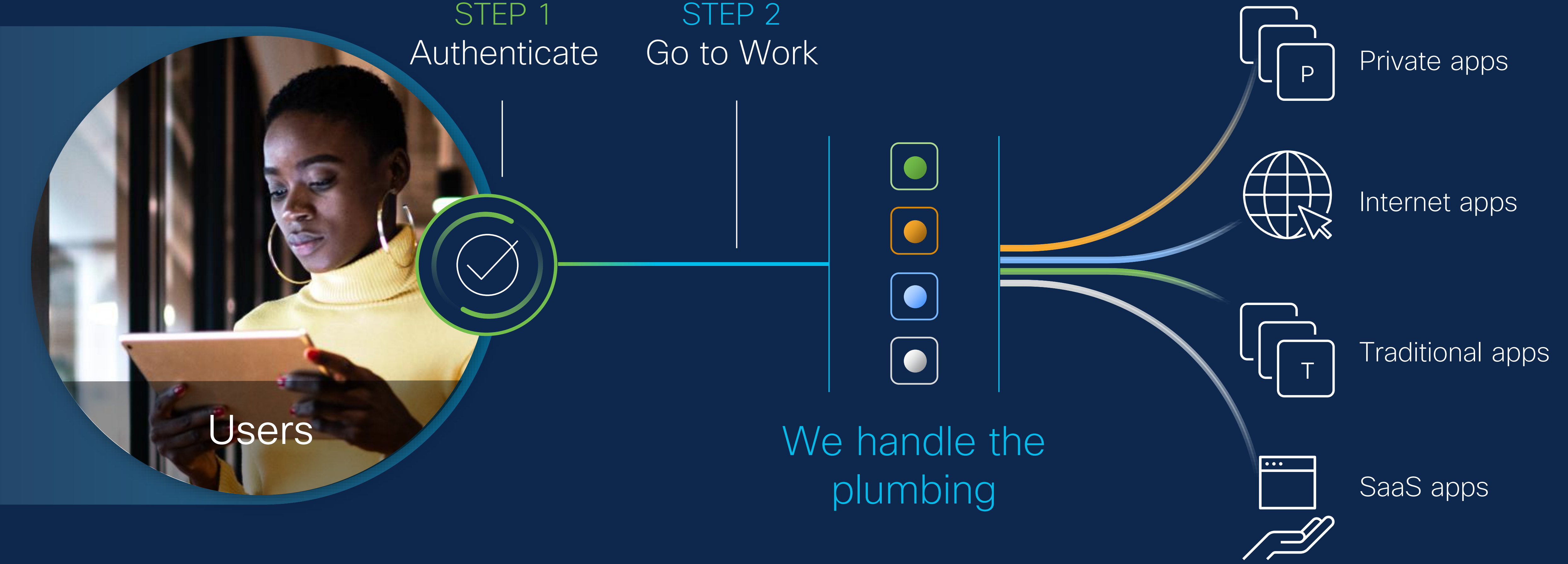

PVC
COPPER
IRON
STEEL

Eliminate unnecessary decisions



How would you like your water delivered?

Seamless user to app Zero Trust

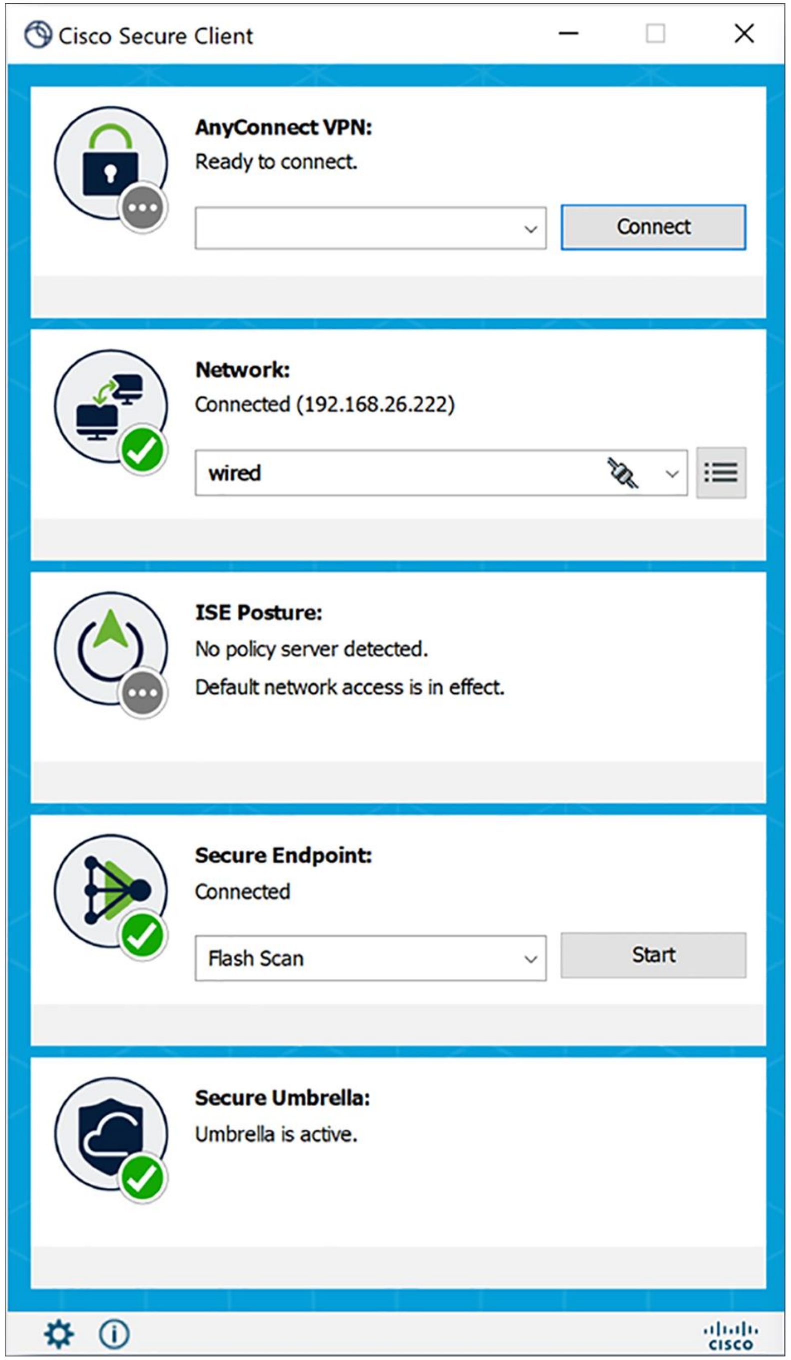


Cisco Secure Client

Unify your stack by consolidating agents

Simplifies security with **ONE agent** across **SASE, XDR** and **Zero Trust**

- ONE agent driving operational efficiency
  - Unifies deployment, updates and management
- ONE agent radically reducing agent fatigue
  - Single agent for Secure Endpoint, Umbrella, AnyConnect
- ONE platform
  - Cloud-native, cloud-managed
  - Unmatched customer value as it comes included with:
    - Device Insights for deep visibility of all your endpoints, apps and more
    - Indicator of device compromise for easy and fast disposition lookup
    - Fast response actions and remediation



Cisco Secure Client

AnyConnect VPN:
Ready to connect.

Network:
Connected (192.168.26.222)

wired

ISE Posture:
No policy server detected.
Default network access is in effect.

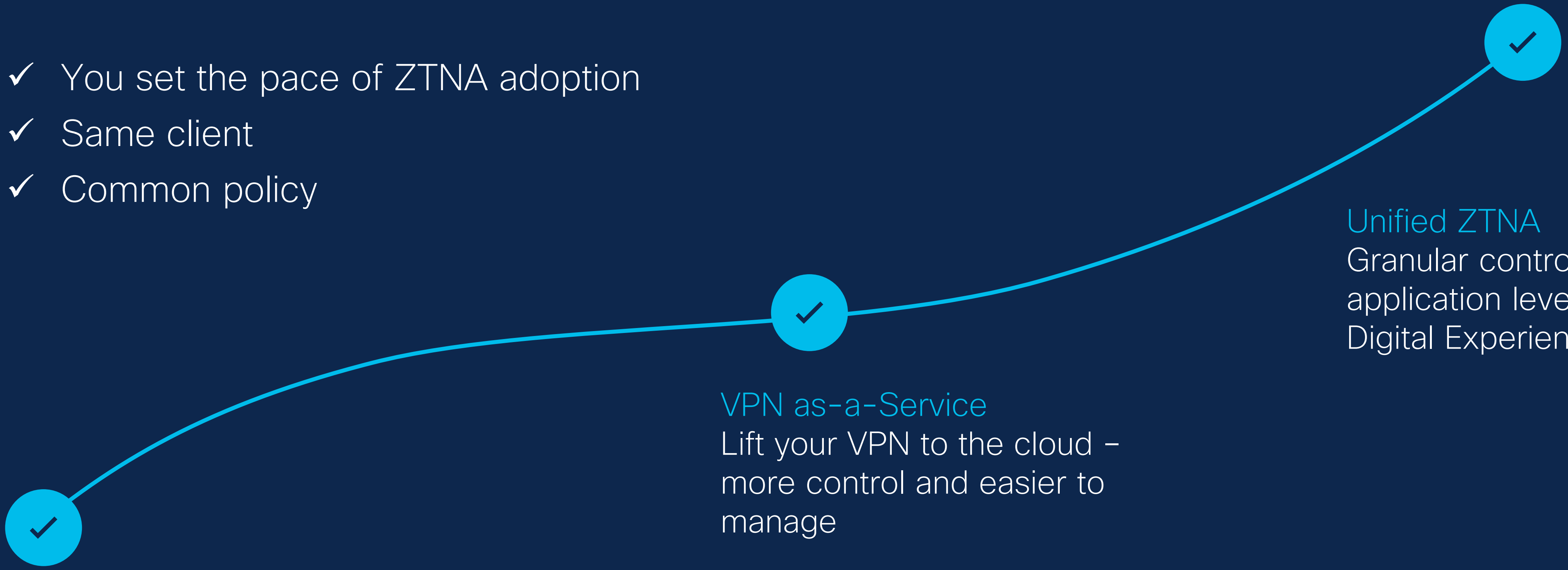
Secure Endpoint:
Connected

Flash Scan

Secure Umbrella:
Umbrella is active.

Easy migration to Zero Trust Access

- ✓ You set the pace of ZTNA adoption
- ✓ Same client
- ✓ Common policy

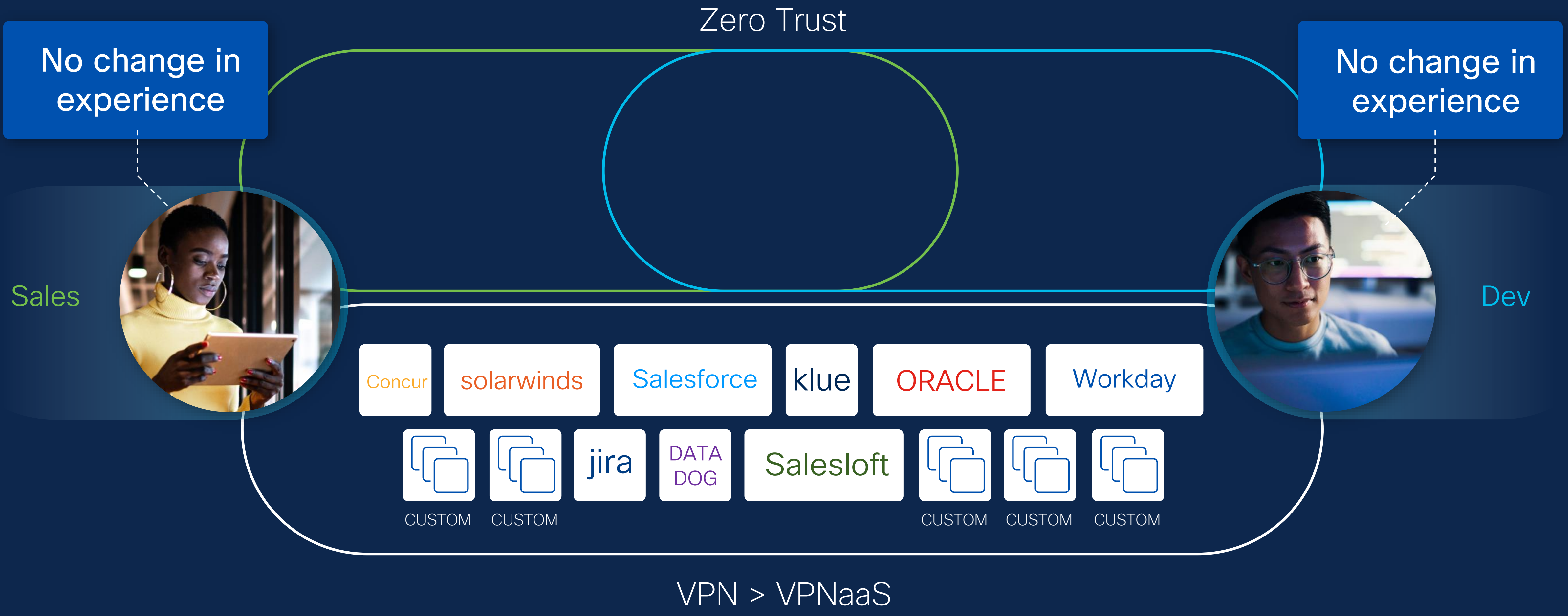


Traditional VPN
Network level access – cannot control at app level

VPN as-a-Service
Lift your VPN to the cloud – more control and easier to manage

Unified ZTNA
Granular controls at the application level + VPNaaS and Digital Experience Monitoring

Simplifying the journey to zero trust



Zero Trust

No change in experience

No change in experience

Sales

Dev

Concur

solarwinds

Salesforce

klue

ORACLE

Workday

CUSTOM

CUSTOM

jira

DATA DOG

Salesloft

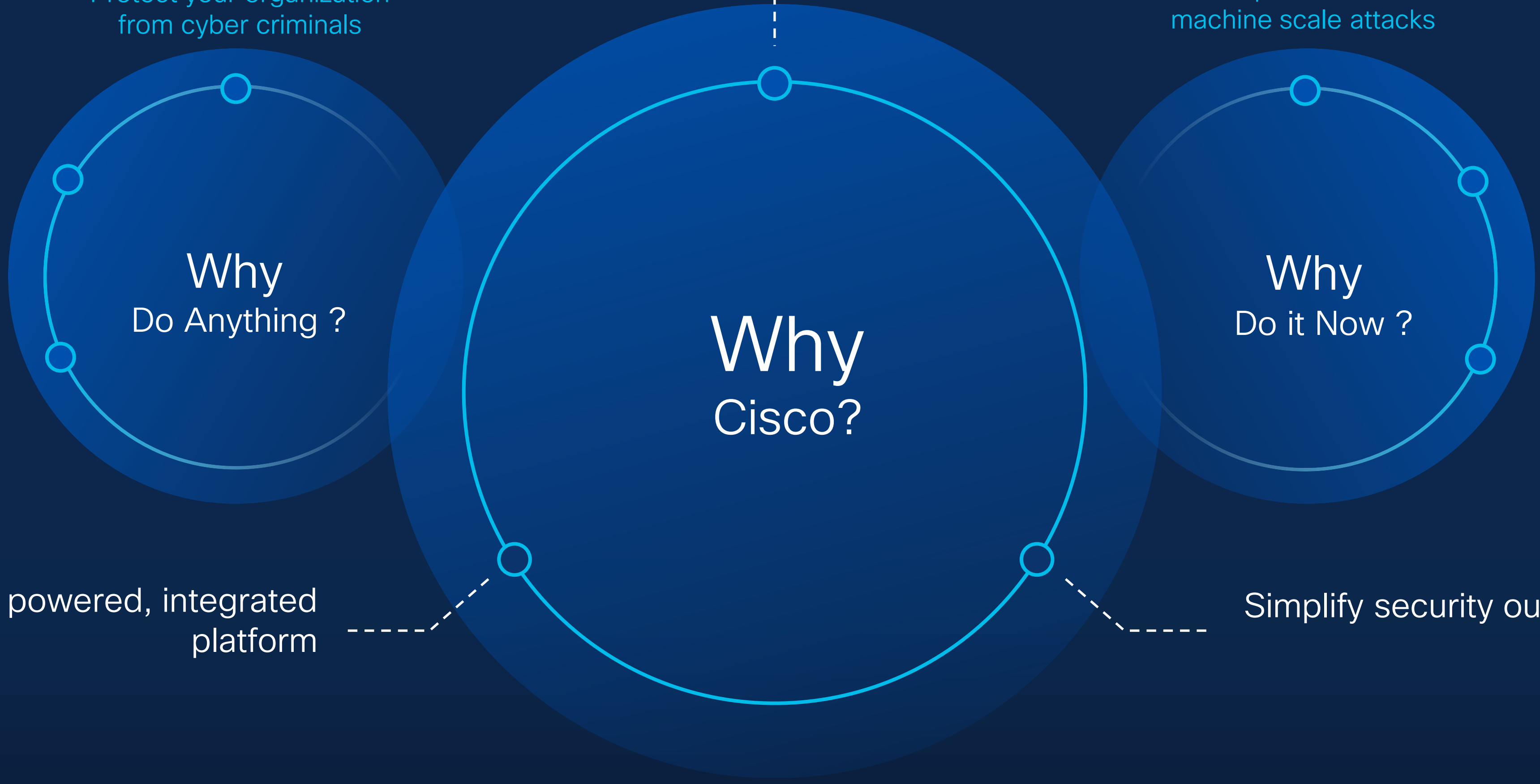
CUSTOM

CUSTOM

CUSTOM

VPN > VPNaaS

The Why?



TALOS

World’s best Threat Intelligence.
500 threat researchers + AI powered algorithms

Protect your organization
from cyber criminals

Risk
Mitigation

Attacks are trending
upwards & more and more
organizations are targeted

Why
Do Anything ?

Why
Cisco?

AI powered, integrated
platform

Simplify security outcomes

Sophisticated
machine scale attacks

Nation-state
sponsored attacks

SaaS, Cloud
transformation,
Remote / Hybrid work

Why
Do it Now ?

Why Cisco?

SECURE

Talos powers Secure Access with intelligence

Analyze

Rapid speed of correlation and detection

Collect

Enormous scale and reach for inputs

Defend

Global distribution and protection

We see more and automate more, so you can block more and respond faster to threats.

2.1M+ malware samples processed daily

625B web requests resolved daily

200+ new vulnerabilities discovered yearly

- Backed by robust expert team of full-time researchers and data scientists
- Machine learning and automation intelligence

550 B security events observed daily

Talos Powers The Cisco Portfolio With Intelligence

TALOS

500
threat researchers

AI
powered algorithms

550B
security events observed daily

Go beyond core Security Service Edge (SSE)

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

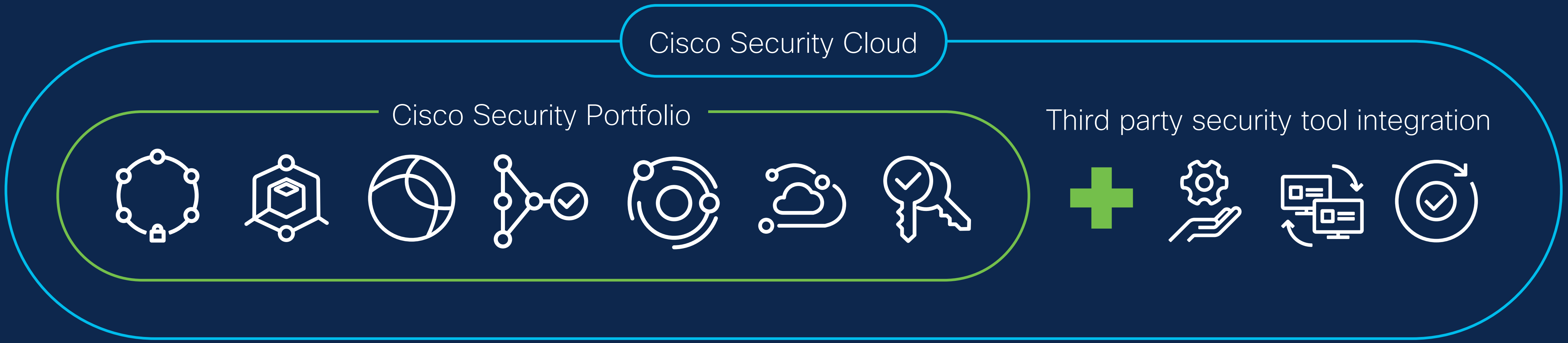
Add-on solutions

- SD-WAN
- XDR
- Duo MFA/ SSO
- CSPM

*Global general availability coming soon

Cisco Secure Access

Built on the Cisco Security Cloud platform to avoid patchwork IT dilemma



Cisco Security Cloud

Cisco Security Portfolio

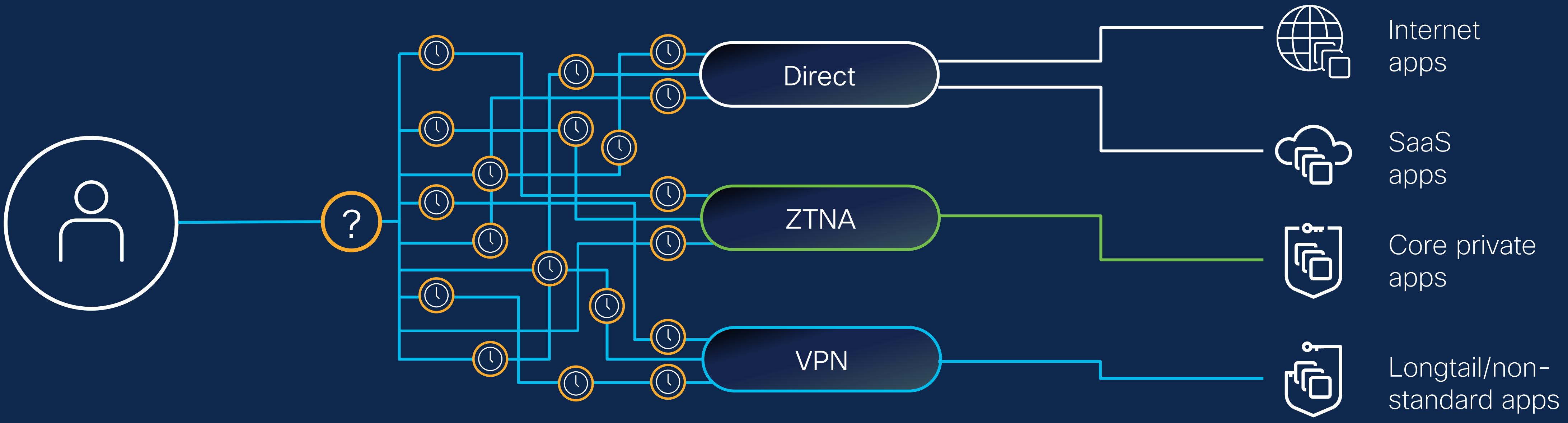
Third party security tool integration

A common platform makes it easier to extend and manage your IT environment with better integration across the Cisco security portfolio and major 3rd-party solutions.

Better for users

Facilitate frictionless workforce experience for better productivity

Users experience fatigue, friction, repetition

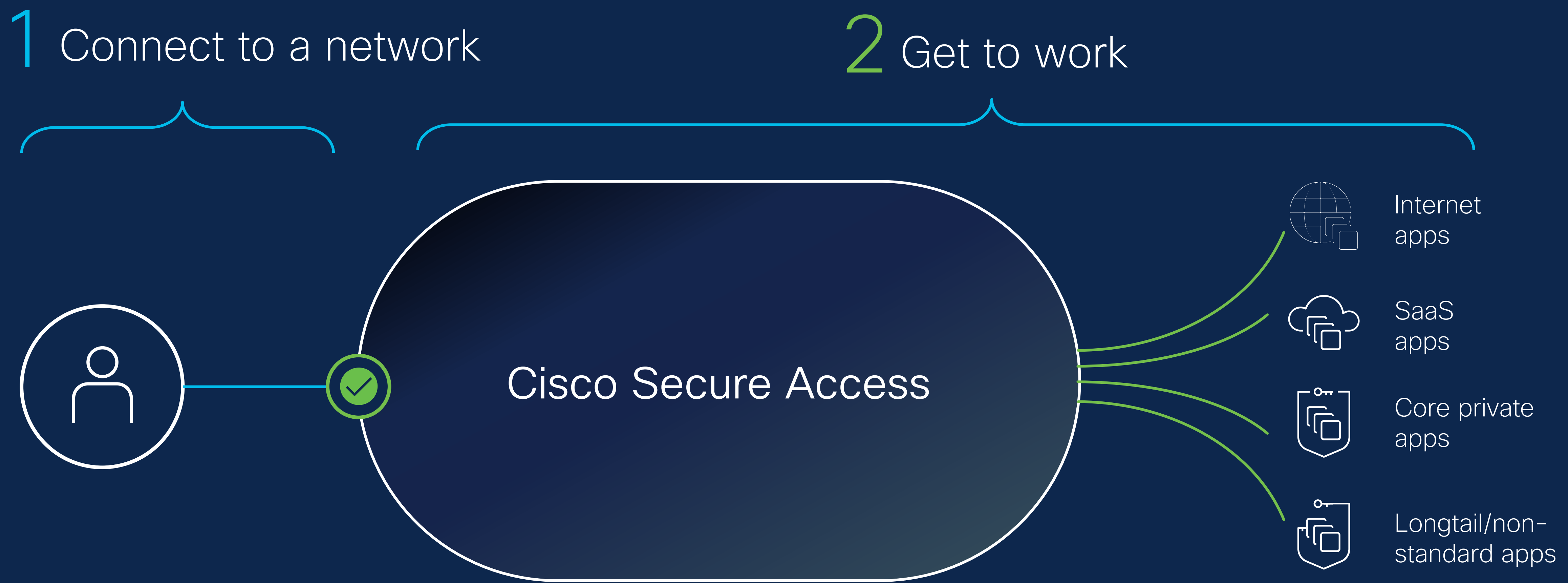


- Many connection decisions
- Various processes
- Multiple steps
- Repetitive authentication tasks

49% Employees frustrated with tech

26% Employees leaving job because of tech experience

Easy, frictionless user experience

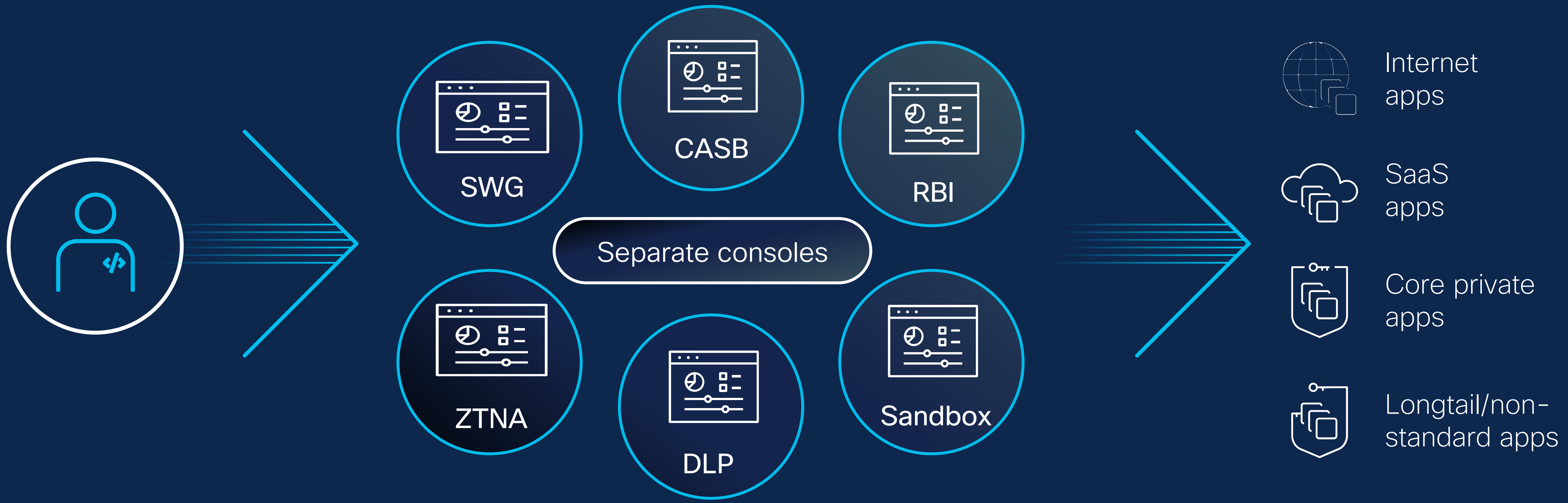


Note: Supports both client and clientless ZTNA connectivity

Easier for IT

Lower costs and improve efficiencies

The multi-vendor approach is problematic



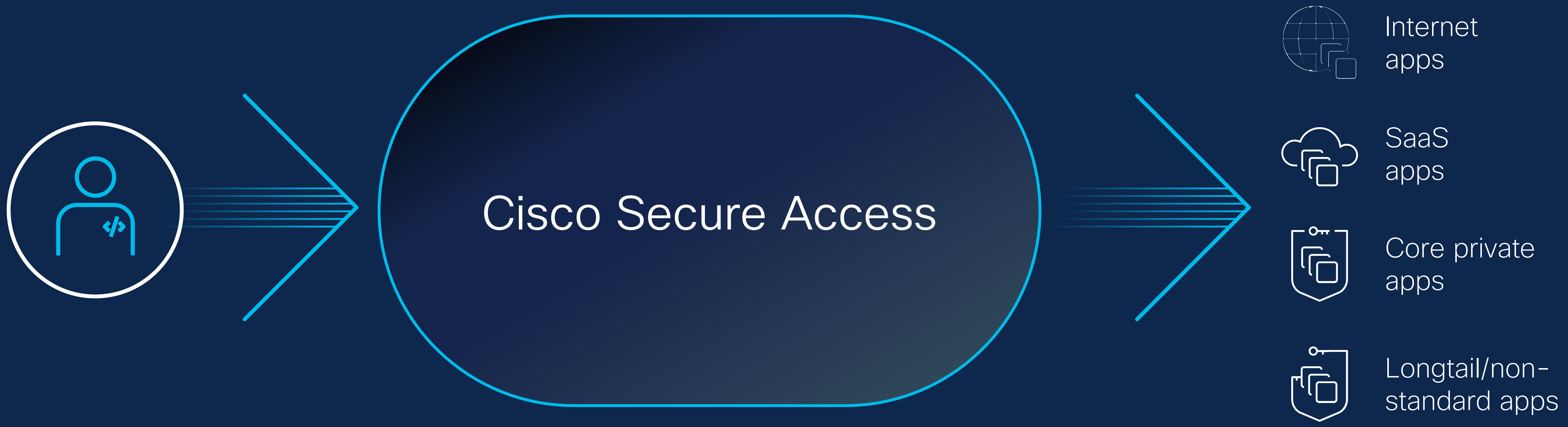
Multiple products increase cost and inefficiencies

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

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

Easier for IT

Simplification with fewer consoles



Cisco Secure Access

Internet apps

SaaS apps

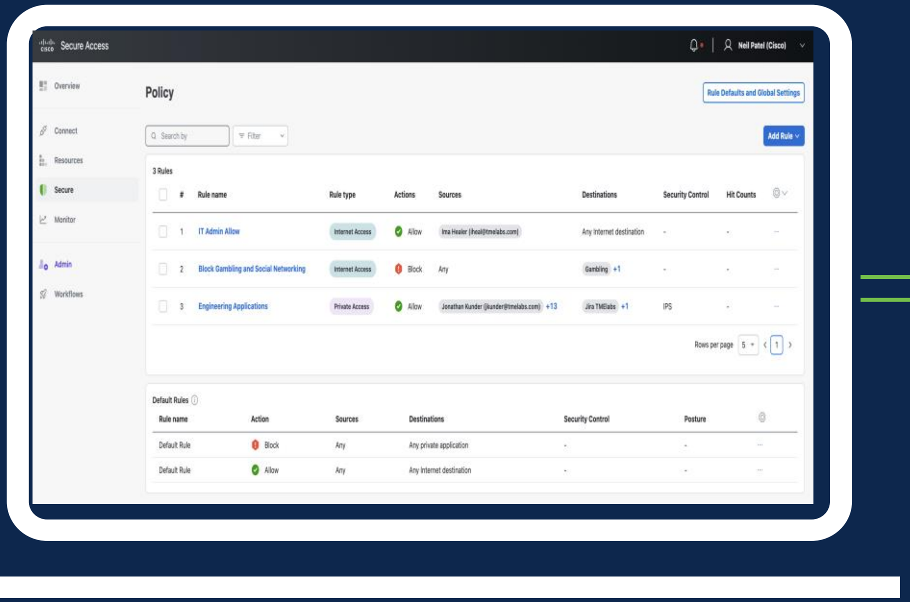
Core private apps

Longtail/non-standard apps

Secure Access converges multiple consoles into one

Easier for IT

Converged cloud security for lower cost and improved efficiencies



Policy

3 Rules

#	Rule name	Rule type	Actions	Sources	Destinations	Security Control	Hit Counts
1	IT Admin Allow	Internet Access	Allow	Ima Healer (iheal@tmelabs.com)	Any Internet destination	-	-
2	Block Gambling and Social Networking	Internet Access	Block	Any	Gambling +1	-	-
3	Engineering Applications	Private Access	Allow	Jonathan Kunder (jkunder@tmelabs.com) +13	Jira TMElabs +1	IPS	-

Rows per page 5 ‹ 1 ›

Default Rules

Rule name	Action	Sources	Destinations	Security Control	Posture
Default Rule	Block	Any	Any private application	-	-
Default Rule	Allow	Any	Any Internet destination	-	-

Higher efficiency

- *Single* agent, console, identity and posture, policy management
- Digital Experience Monitoring (DEM)*
- Single SLA

Lower costs

- Consolidated licensing
- Less hardware
- Ecosystem

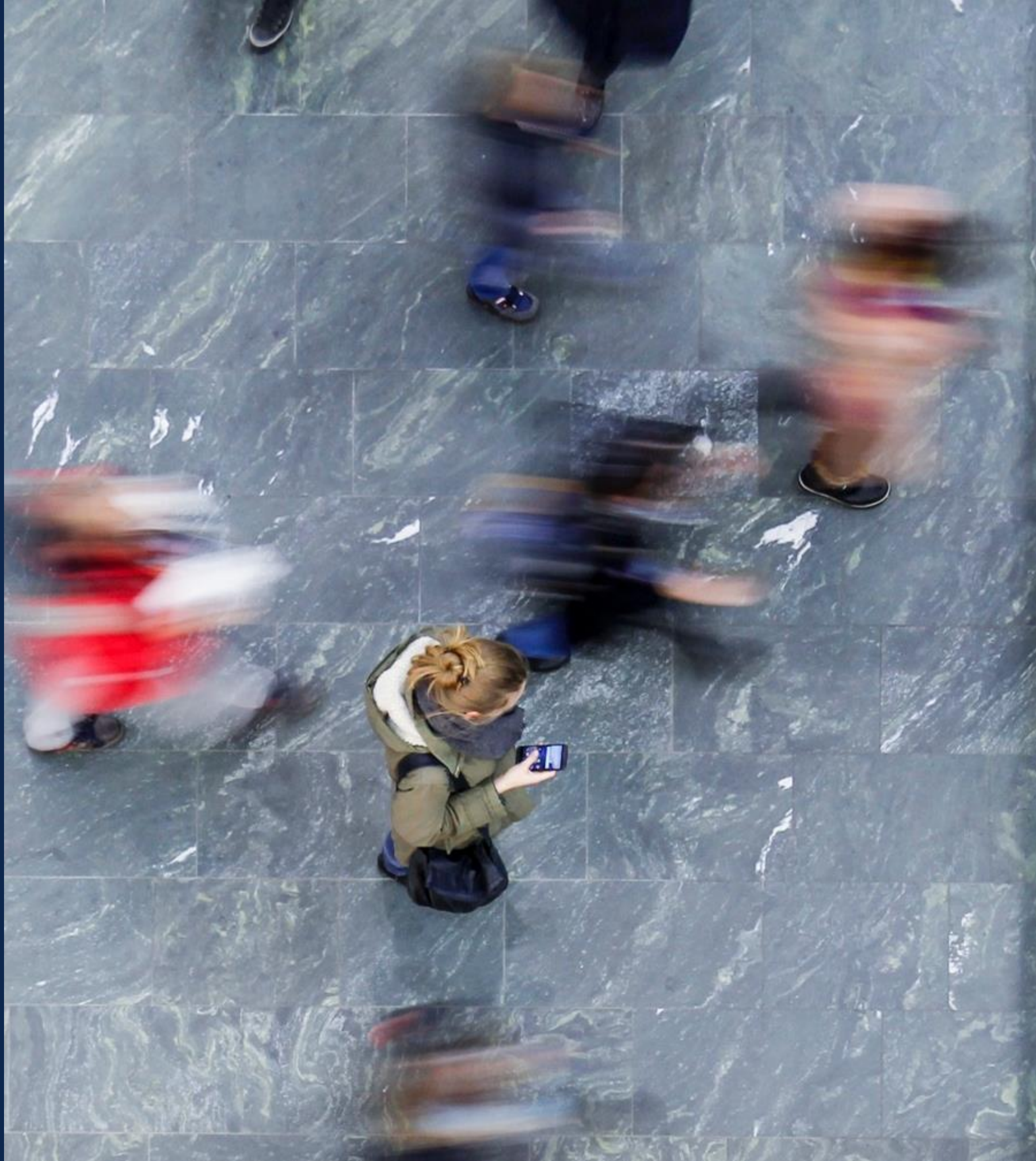
One place to see traffic, set policies, and analyze risk.

SECURE

*Global general availability coming soon

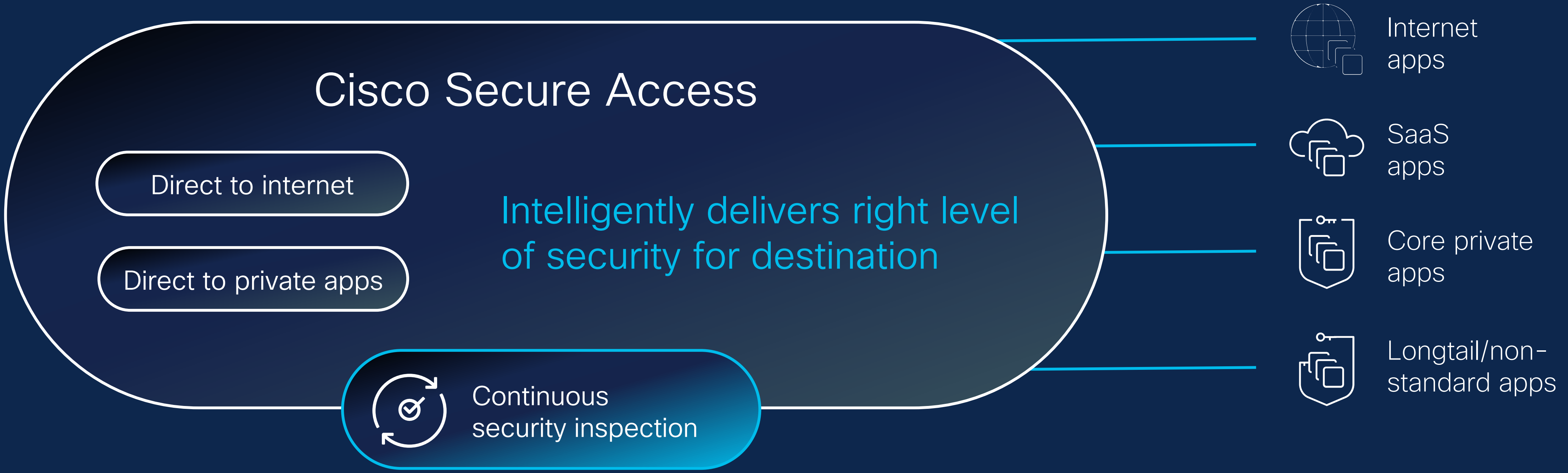
Safer for everyone

Reduce risk and improve business resilience



Advanced cybersecurity benefits

Block more, investigate faster, and remediate fully



Cisco Secure Access

Direct to internet

Direct to private apps

Intelligently delivers right level of security for destination

Continuous security inspection

Internet apps

SaaS apps

Core private apps

Longtail/non-standard apps

Improved security efficacy

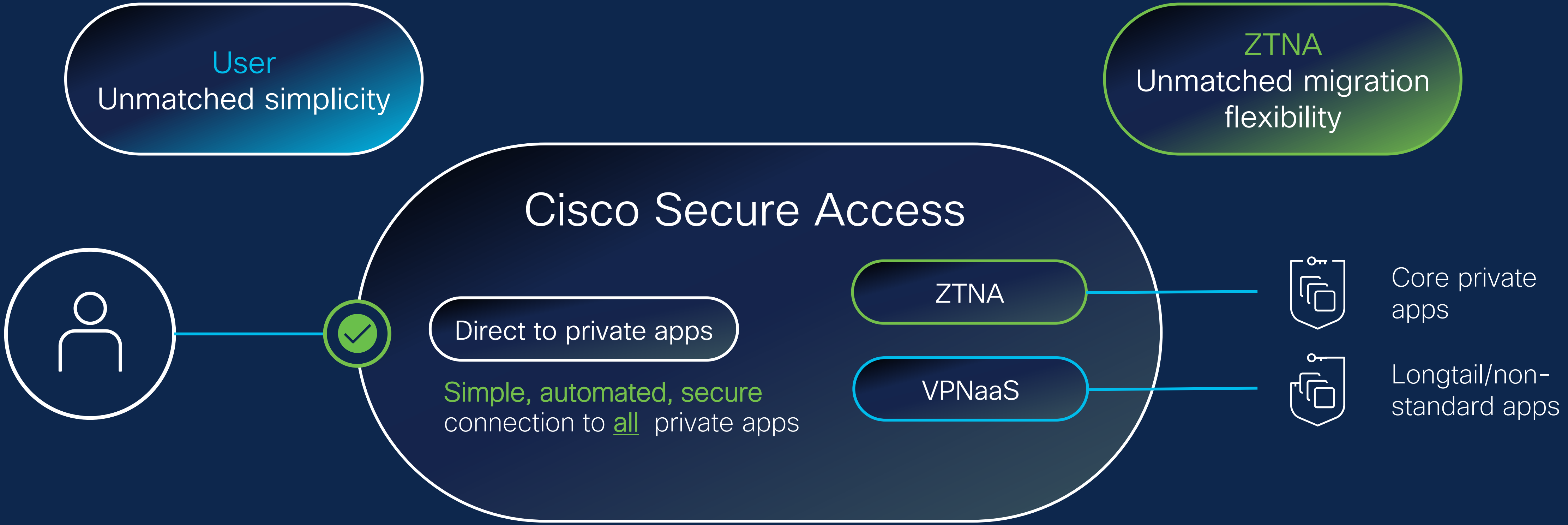
- Deeper visibility and insights
- Reduced alert volume
- Stronger threat correlation
- Faster detection

- High analyst effectiveness
- Least privileged app access
- Reduced exposure

Reduction in successful attacks

Zero Trust Network Access (ZTNA) journey

Intelligent private application access from anywhere


User
Unmatched simplicity
ZTNA
Unmatched migration flexibility
Cisco Secure Access
Direct to private apps
Simple, automated, secure connection to all private apps
ZTNA
VPNaaS
Core private apps
Longtail/non-standard apps

Benefits

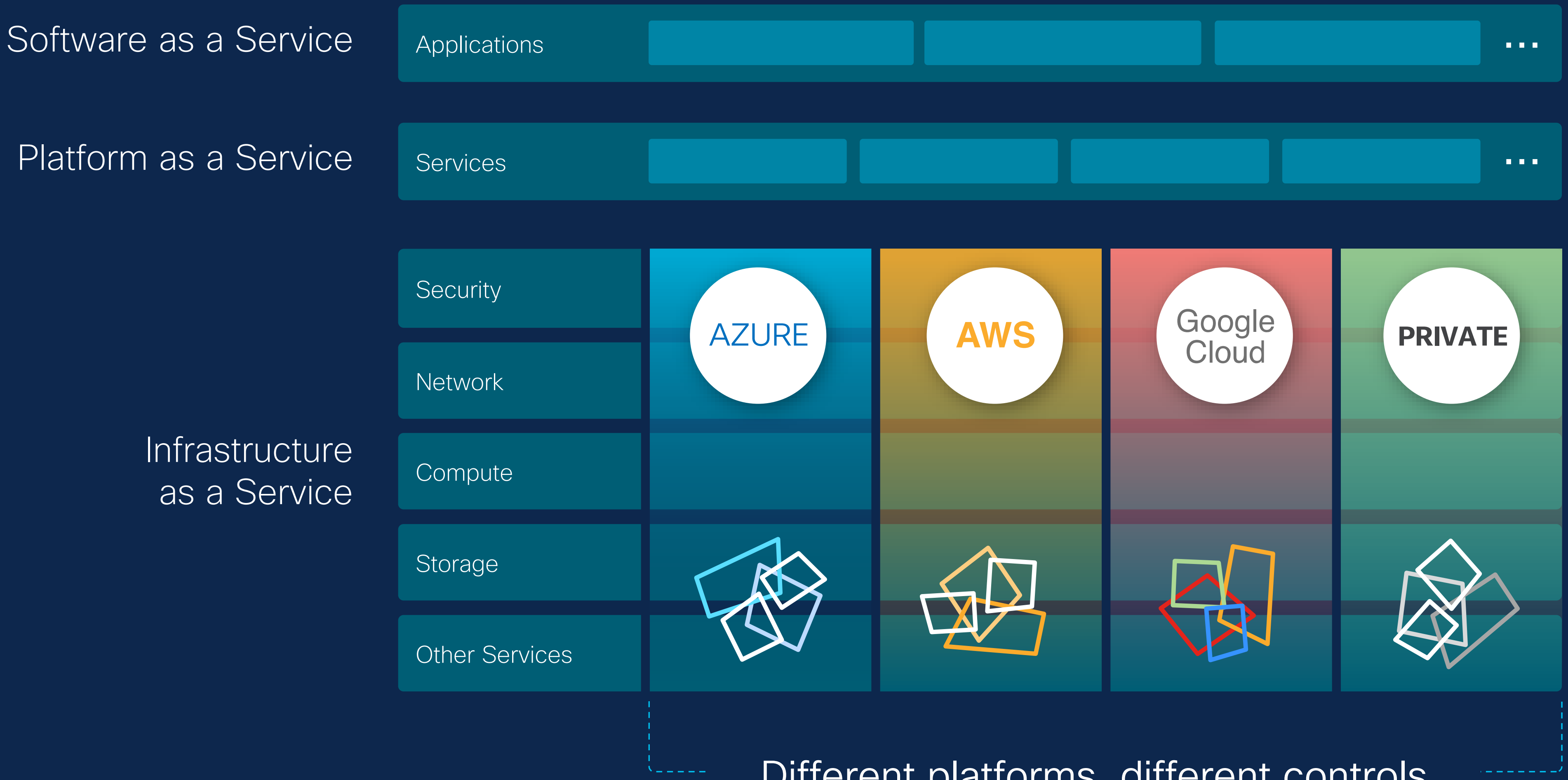
- App-specific access
- Undiscoverable IP address
- Least privileged user access
- Reduced threat surface
- Automated selection of ZTNA or VPNaaS
- Posture verification
- Access segmentation

If it’s connected,
it’s protected.

The Next Step:

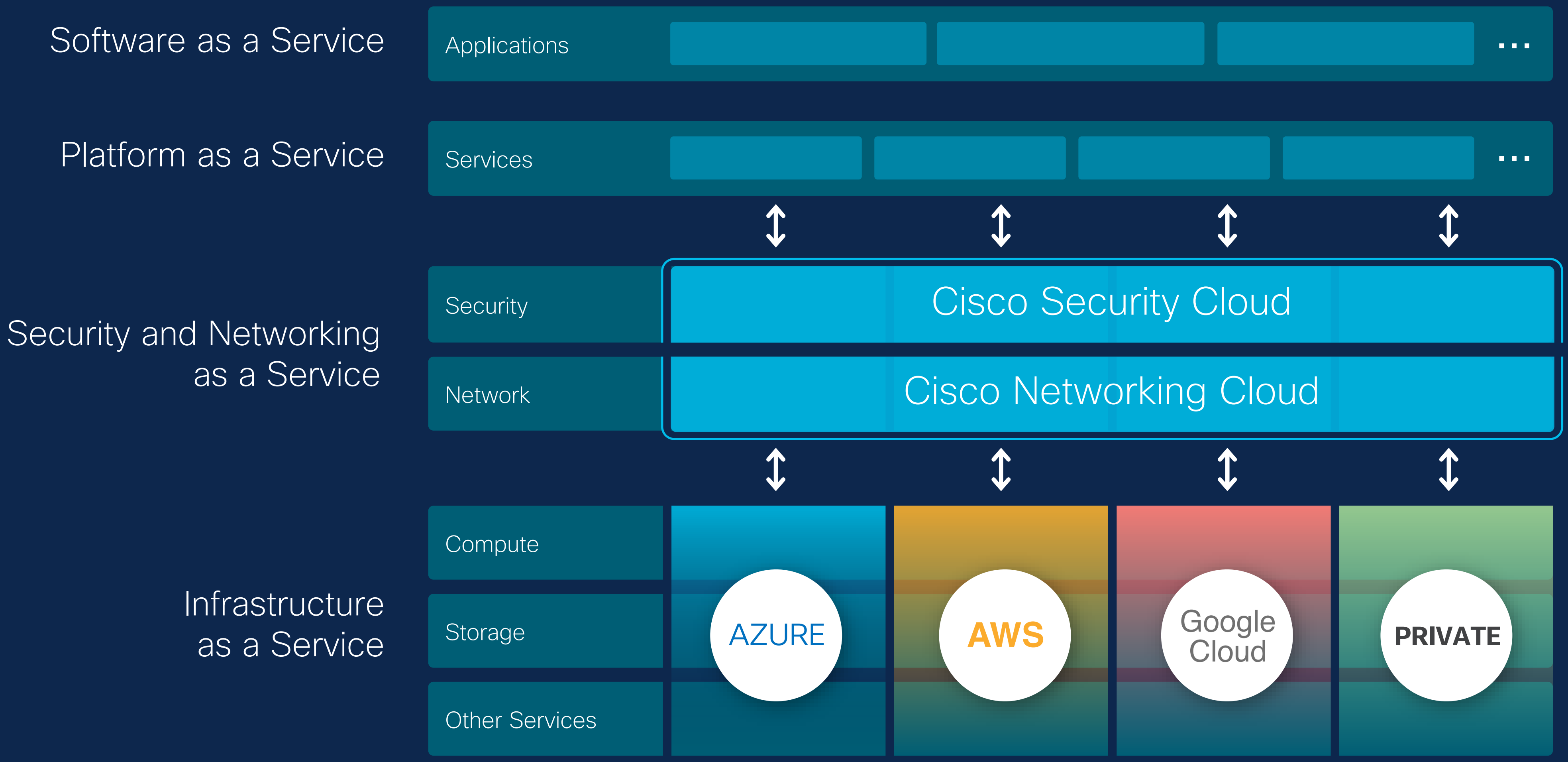
Cisco Multicloud Defense

Multiple clouds makes tool sprawl worse



Different platforms, different controls

Introducing Cisco Security Cloud



cisco SECURE