Let's go

The bridge to possible

Cisco's Vision for Security

Jeetu Patel, EVP & GM, Security & Collaboration

Tom Gillis, SVP & GM, Security

Forward-Looking Statements

This presentation may be deemed to contain projections and other forward-looking statements regarding future events or the future financial performance of Cisco, including future operating results. These projections and statements are only predictions. Actual events or results may differ materially from those in the projections or other forward-looking statements. Please see Cisco's filings with the SEC, including its most recent filings on Forms 10-K and 10-Q, for a discussion of important risk factors that could cause actual events or results to differ materially from those in the projections or other forward-looking statements.

Security TAM

Our Large and Growing Opportunity

Tailwinds

Security Cloud Platform
Eliminate Vendor Patchwork & Increase Security Resilience

Innovation
Address Customers' Biggest Needs at High Velocity

Buying Center Simplicity
Enable Land & Expand through Simplified Use Cases unique to Cisco

Source: IDC, Gartner, Dell'Oro, Synergy, 451 Research, 650 Group, Cignal AI, Exact Ventures, LightCounting & Internal Cisco Estimates. TAMs are based on limited information currently available to Cisco, which is subject to change. Actual results may differ materially due to a variety of factors listed in Cisco SEC filings, including business and economic conditions.

The scale of Cisco Security

80%
of the world's internet traffic

300K
customers worldwide

400B
security events observed daily

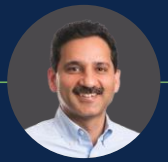
2.0M
new malware samples daily

400+
third-party integrations

Security executive team

TOM GILLIS
SVP/GM SECURITY

PRODUCT & ENGINEERING



RAJ CHOPRA
SVP PRODUCT MANAGEMENT & DESIGN

SHAILA SHANKAR
SVP/GM ENGINEERING

CRAIG CONNORS
VP, SECURITY INNOVATION

OPS & SHARED SERVICES

CHRIS MINUNNI
CHIEF OF STAFF

MEGAN FURMAN
SR DIR, TRANSFORMATION & PLANNING

GINNY LEE
LEGAL

MARK LINGENBRINK
PEOPLE & COMMUNITIES

STEPHAN TREMBLAY
FINANCE

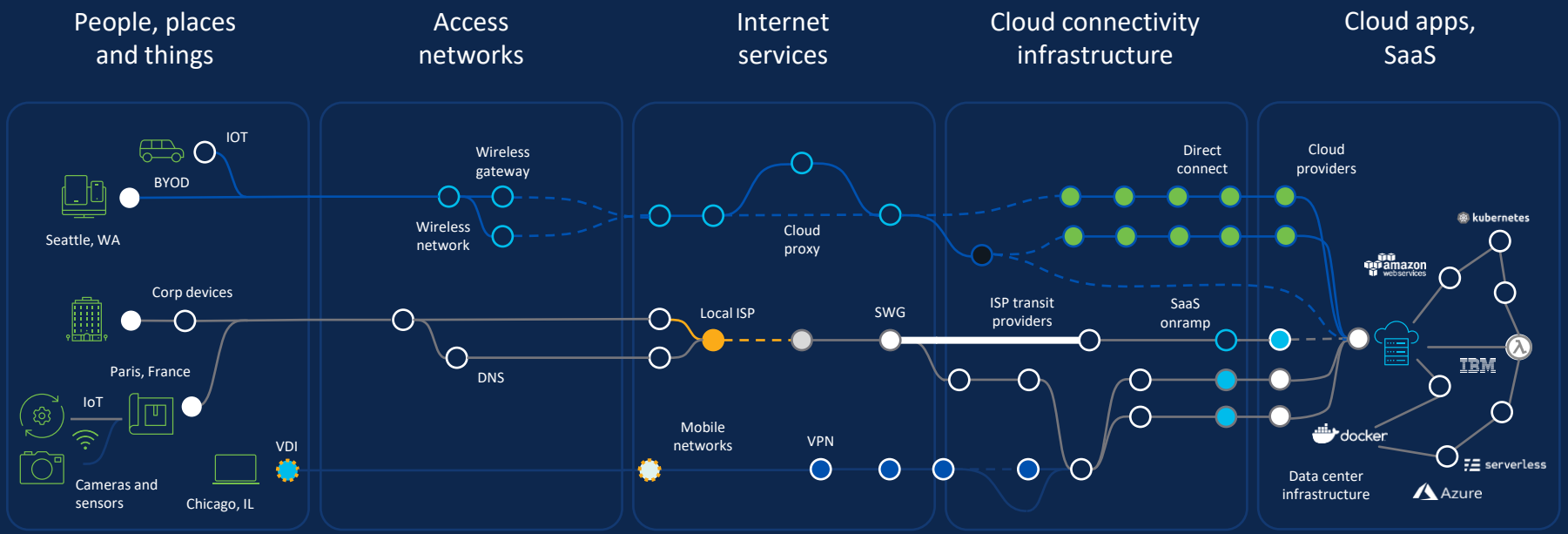
GO-TO-MARKET

EMMA CARPENTER
GLOBAL SALES

AMBIKA GADRE
SVP MARKETING

CHRISTEN GENTILE
DIR COMMUNICATIONS

Fast and reliable connections are complex



Securing those connections compounds this complexity

People, places and things

Access networks

Internet services

Cloud connectivity infrastructure

Cloud apps, SaaS

Security innovation is patchwork

Exfiltration

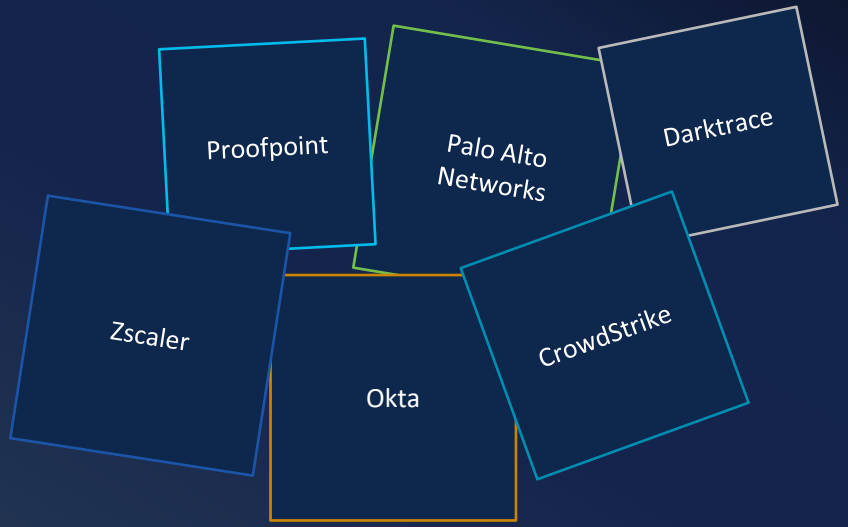
Ransomware

Lateral movement

Web threats

Stolen credentials

Spam



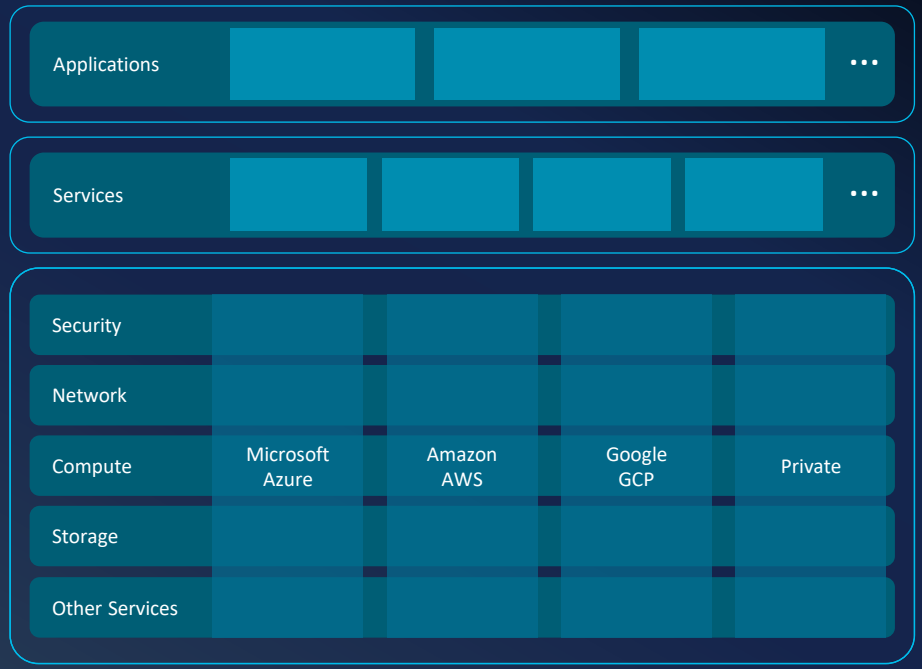
New threats spawn new vendors, putting the burden on customers

Hybrid multicloud future

Software as a Service

Platform as a Service

Infrastructure as a Service



Expect a different patchwork of security tech in a multicloud world

Cisco Security Cloud

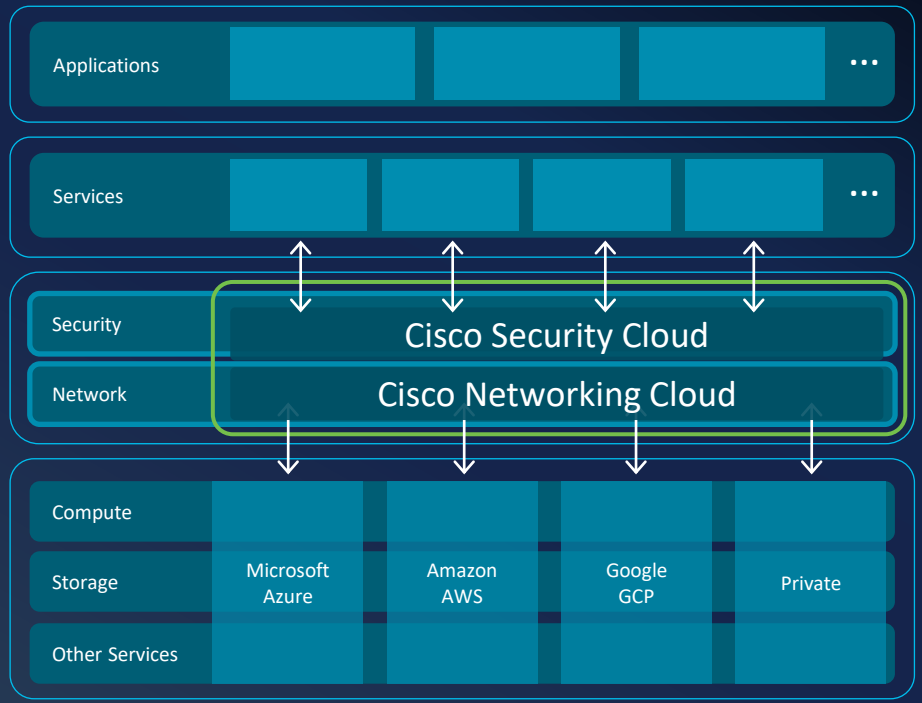
Software as a Service

Platform as a Service

Security & Networking as a Service

Optimizes performance & security of every connection

Infrastructure as a Service



Cisco Security Cloud

Integrated AI-powered security platform

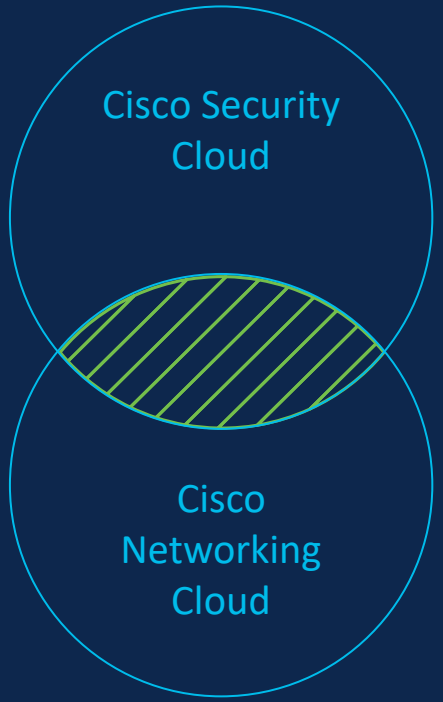
User protection

Cloud protection

Application protection

Breach protection

Shared networking and security platform advantage



Unified User Experience

Common Policy

Shared Telemetry

Open APIs

Cisco Security Cloud benefits

Users

Seamless and fast connections and continuous granting of trust

IT

Centralized policy and advanced security enforcement

Developers + DevSecOps

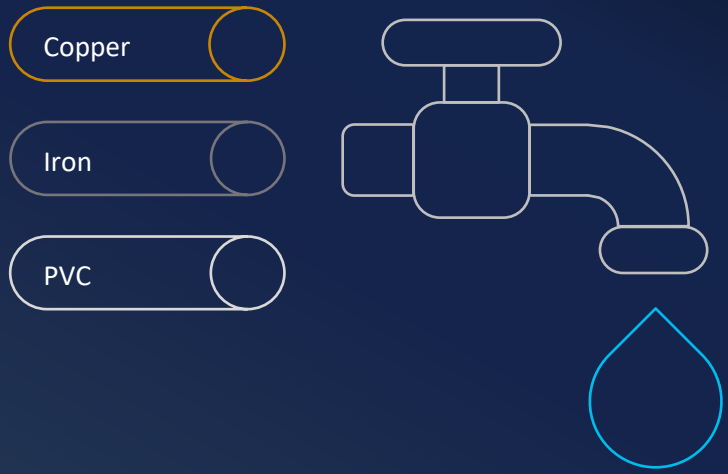
Are free to focus on business logic not security functions

Security Operations Center

A unique end-to-end view that stops advanced threats like ransomware

Eliminate unnecessary decisions

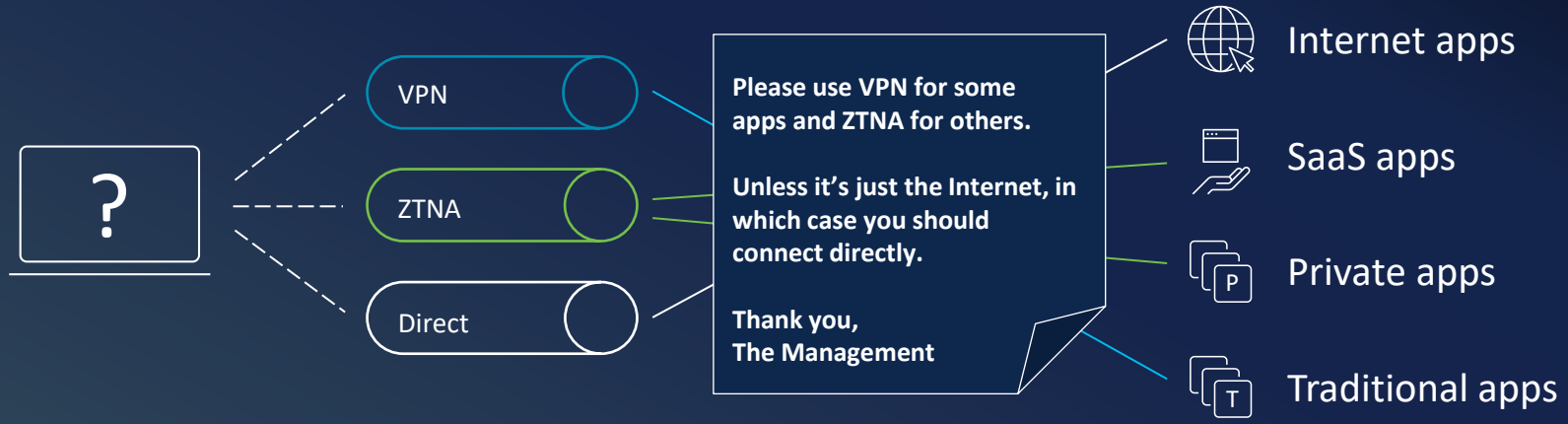
How would you like your water delivered?



Users

Eliminate unnecessary decisions

How would you like to connect to your applications?



Users

Cisco delivers a better way to connect

INTRODUCING

Cisco Secure Access

- One click access to any application or data
- Intelligently connects using the best protocol
- Un-matched ease of use for your workforce

Cisco makes the connections needed

1 Connect to a network

2 Get to work

Internet apps
Protected by Umbrella

SaaS apps
Protected by CASB

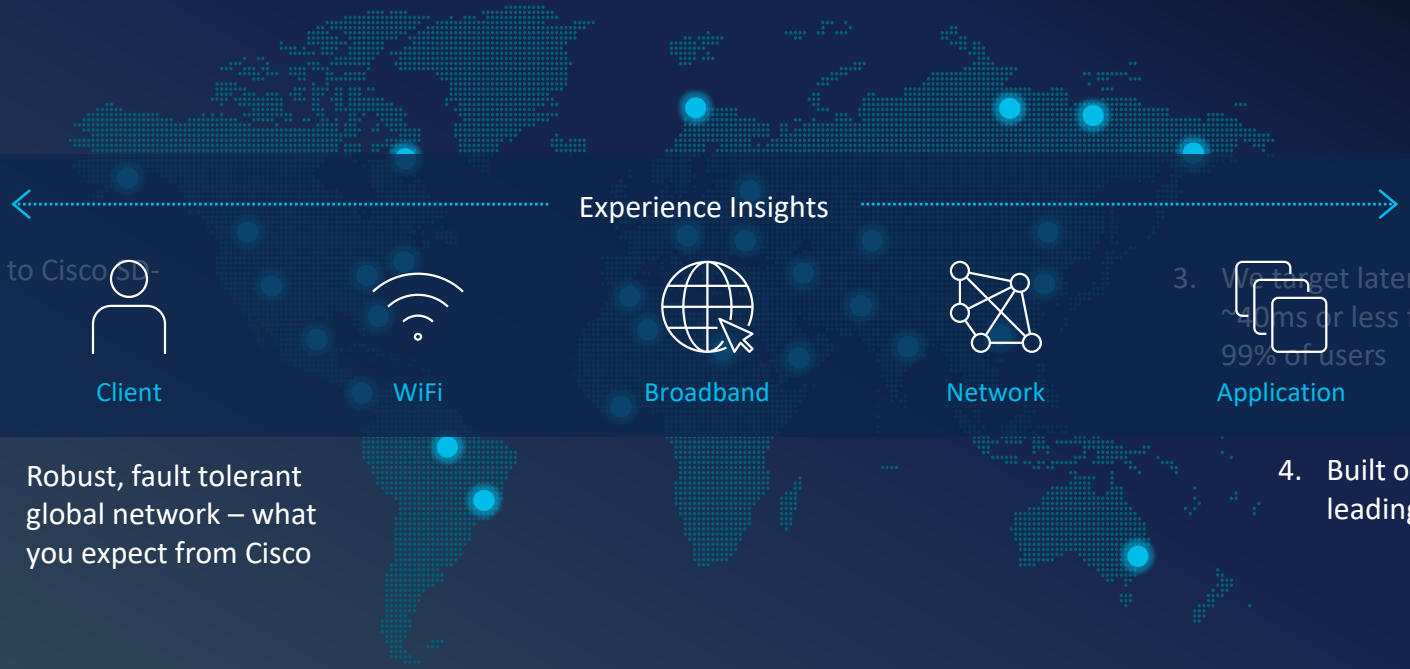
Private apps
ZTNA gives controlled access to selected applications

Traditional apps
VPN gives network access for existing applications

Note: Supports both client and clientless connectivity

Users

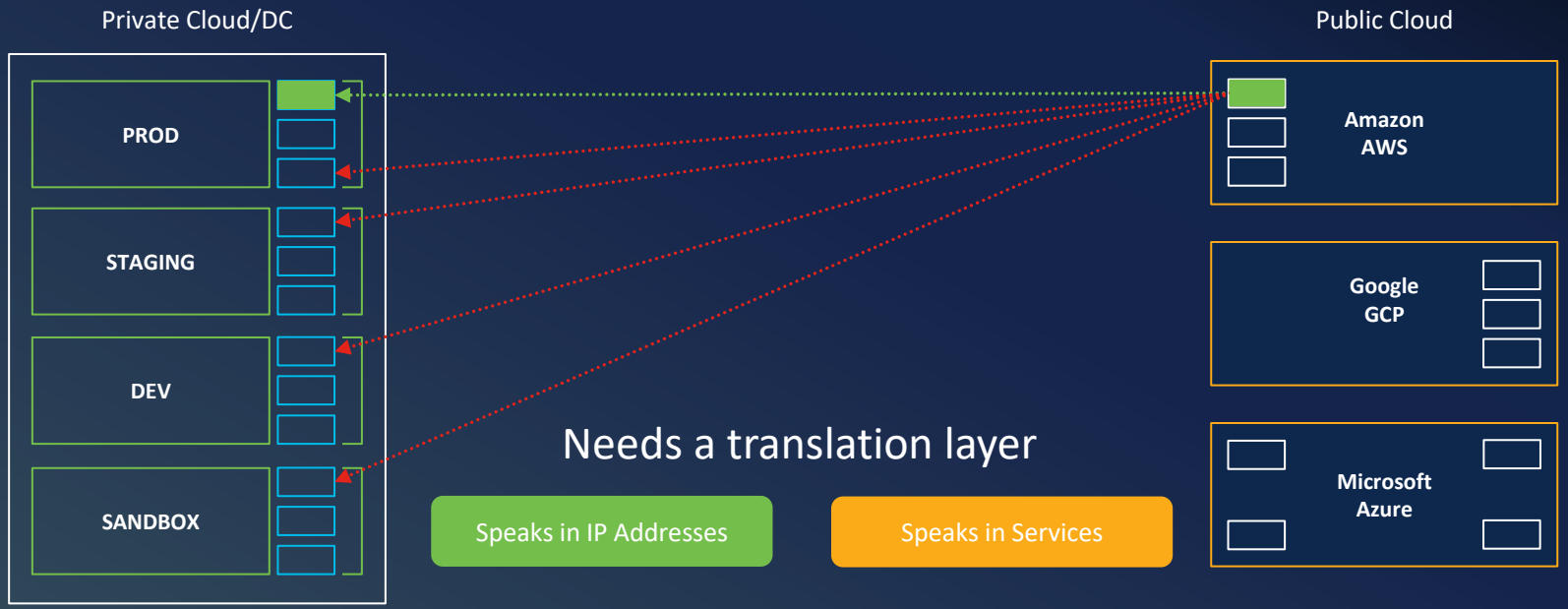
Cisco provides a great user experience



1. Built-in to Cisco SD-WAN
2. Robust, fault tolerant global network – what you expect from Cisco
3. We target latency of ~40ms or less for 99% of users
4. Built on industry leading QUIC protocol

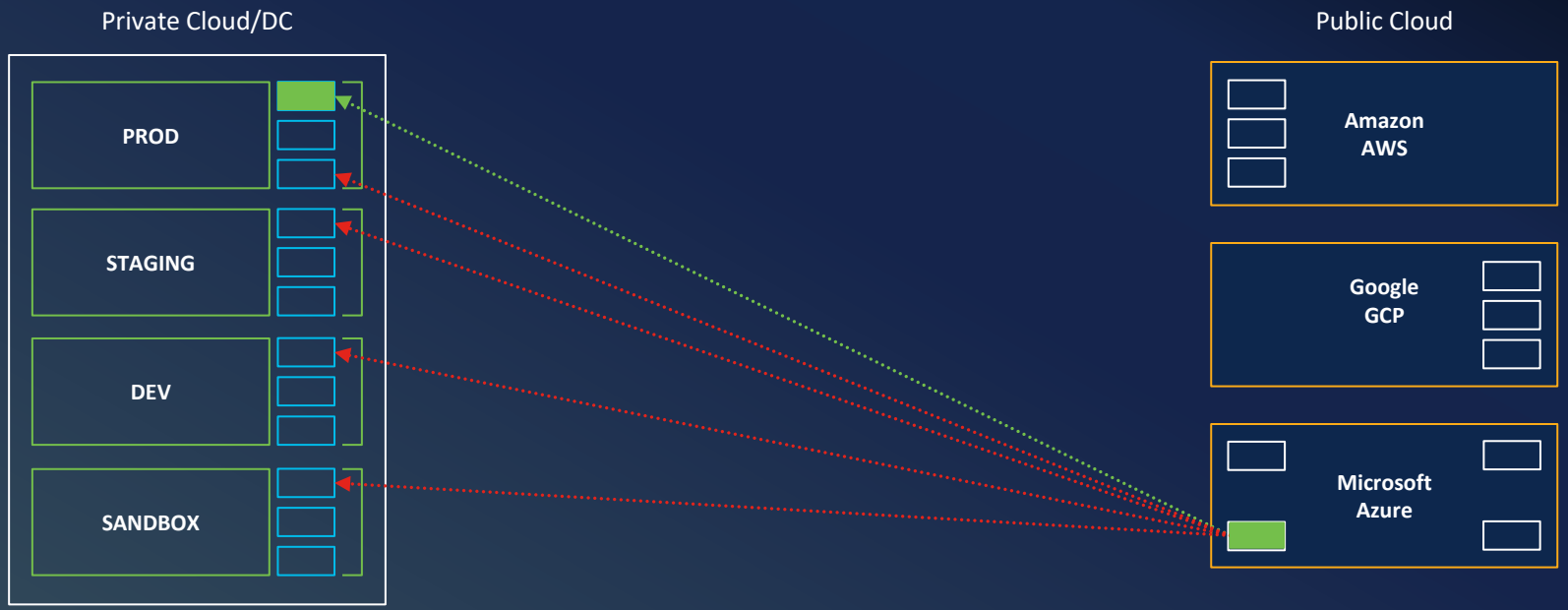
IT

Modern applications are not monolithic



IT

Modern applications are not monolithic



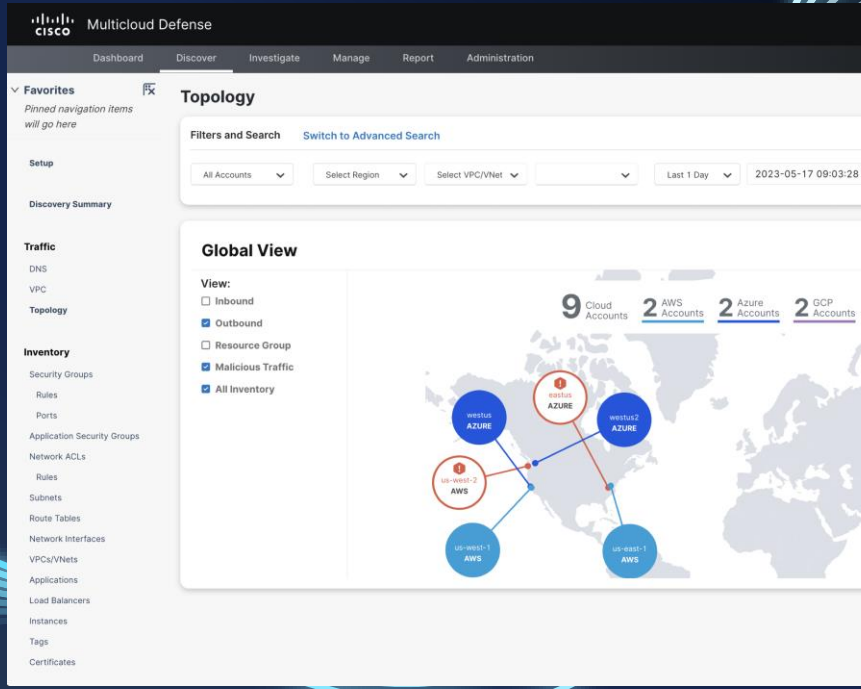
IT

Cisco simplifies multicloud security

INTRODUCING

Cisco Multicloud Defense

- Understands hybrid multicloud fabric
- Ensures privileged communications
- Protects from threats
- Unifies security controls across clouds & applications



IT

Cisco simplifies operations

INTRODUCING

Cisco Secure Firewall 4200 & 7.4OS

- Simplified branch routing features
- Zero Trust application access
- Encrypted visibility engine 2.0

4200 Series

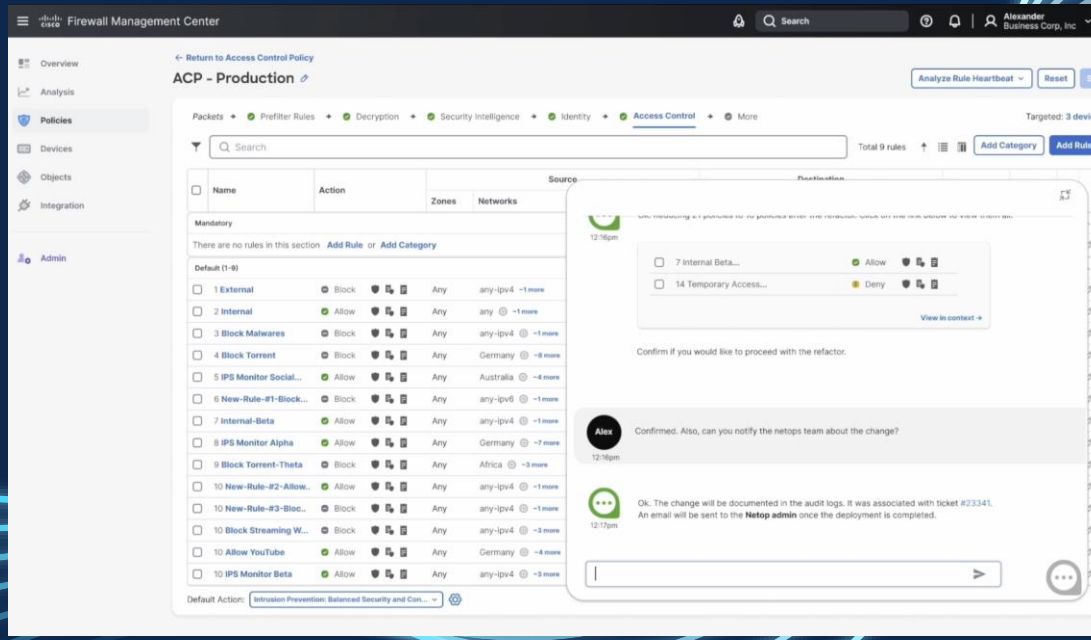
Great performance. Great Price.

- **2x** throughput and a wide range of throughput interfaces (up to 200 Gbps)
- Smaller footprint with **1RU** form factor
- Encrypt and decrypt traffic faster with **high performance**
- Future-proof your investment with **16x** node cluster
- **2x SSD** for event storage and malware analysis

Eliminating policy complexity

INTRODUCING THE ALL NEW

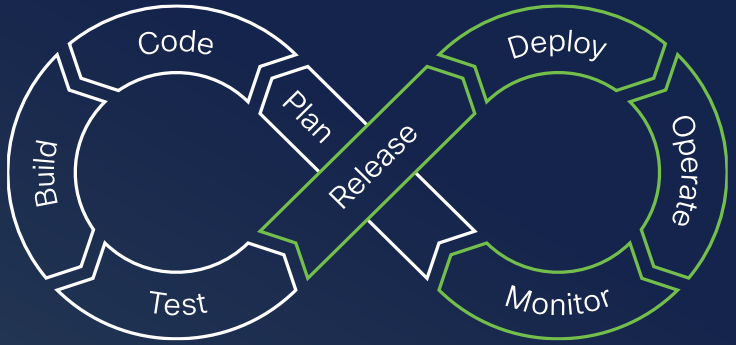
Policy Assistant



DevOps

Security built-in from the start

Application Development (CI/CD)



Policy as code

Embed security policies into the application during development

Microsegmentation

Stop threats from spreading to protect the applications across any environment

Business Risk Observability

Prioritize application vulnerabilities according to business risk

Cisco XDR has the broadest native telemetry

One central data warehouse, analytics, and management in the Security Cloud

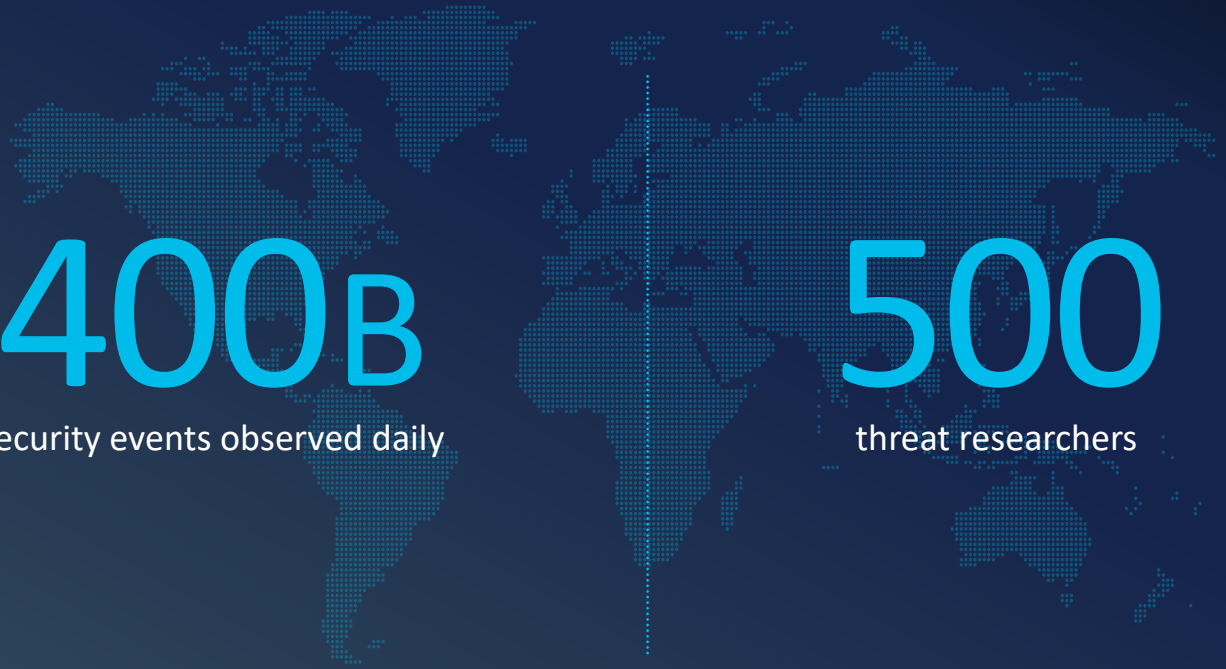
We see every email, even forwarded emails, to spot phishing

We see more web requests than anyone (600B per day) to spot fast-changing malicious sites

We uniquely track every process that makes a connection

We see more network traffic, in more detail, than anyone

Talos powers the Cisco portfolio with intelligence



400B

security events observed daily

500

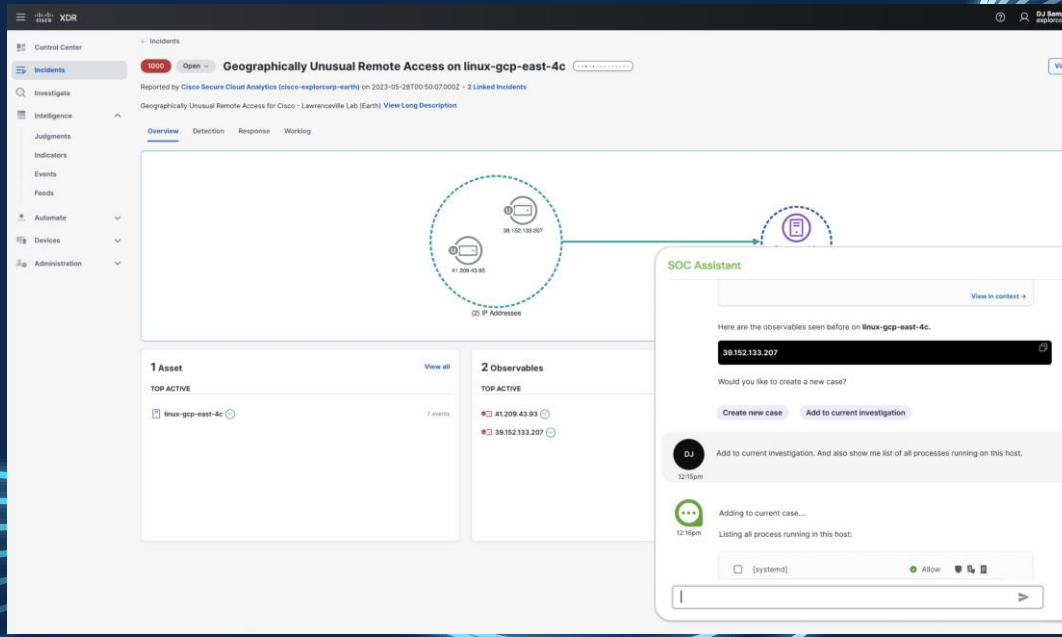
threat researchers

Empowering SOC analysts

INTRODUCING THE ALL NEW

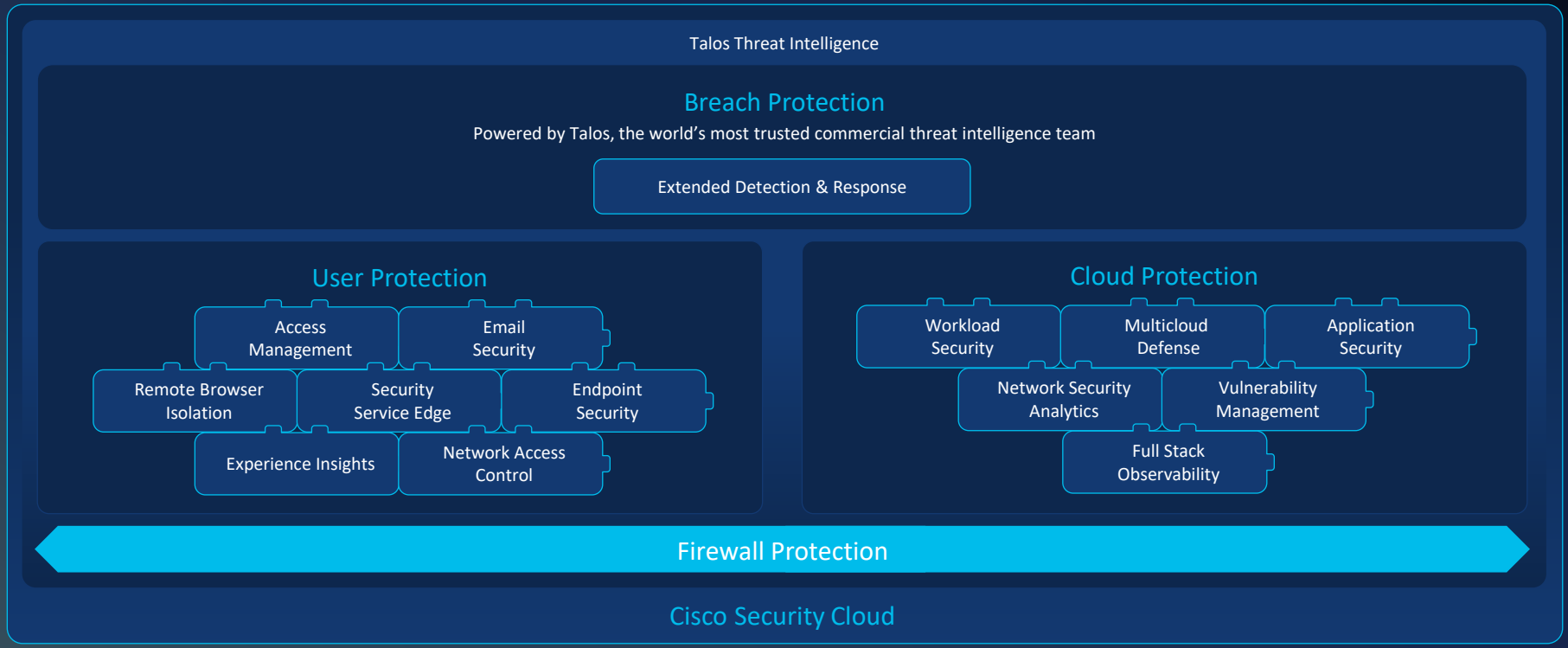
SOC Assistant

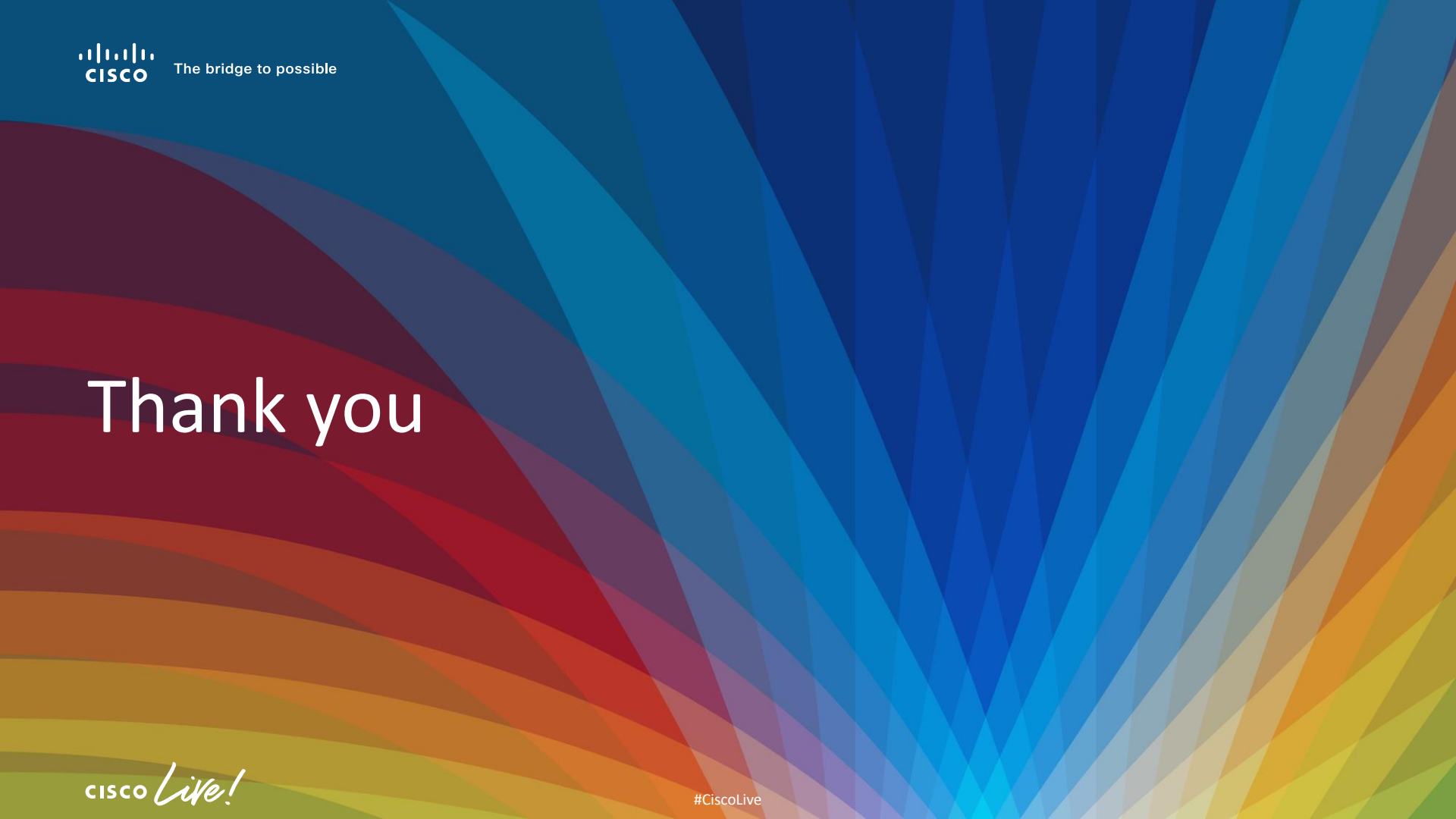
- Summarizes incidents across domains
- Optimized remediation tactics



Cisco Security Cloud

Simplified selling motion




cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLive

FORWARD-LOOKING STATEMENTS

This presentation contains forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. These forward-looking statements include, among other things, statements regarding future events (such as statements regarding our product plans and growth and strategy) and the future financial performance of Cisco that involve risks and uncertainties. Readers are cautioned that these forward-looking statements are only predictions and may differ materially from actual future events or results due to a variety of factors, including: the impact of the COVID-19 pandemic and related public health measures; business and economic conditions and growth trends in the networking industry, our customer markets and various geographic regions; global economic conditions and uncertainties in the geopolitical environment; overall information technology spending; the growth and evolution of the Internet and levels of capital spending on Internet-based systems; variations in customer demand for products and services, including sales to the service provider market and other customer markets; the return on our investments in certain priorities, key growth areas, and in certain geographical locations, as well as maintaining leadership in Secure, Agile Networks and services; the timing of orders and manufacturing and customer lead times; significant supply constraints; changes in customer order patterns or customer mix; insufficient, excess or obsolete inventory; variability of component costs; variations in sales channels, product costs or mix of products sold; our ability to successfully acquire businesses and technologies and to successfully integrate and operate these acquired businesses and technologies; our ability to achieve expected benefits of our partnerships; increased competition in our product and service markets, including the data center market; dependence on the introduction and market acceptance of new product offerings and standards; rapid technological and market change; manufacturing and sourcing risks; product defects and returns; litigation involving patents, other intellectual property, antitrust, stockholder and other matters, and governmental investigations; our ability to achieve the benefits of restructurings and possible changes in the size and timing of related charges; cyber-attacks, data breaches or malware; vulnerabilities and critical security defects; terrorism; natural catastrophic events (including as a result of global climate change); any other pandemic or epidemic; our ability to achieve the benefits anticipated from our investments in sales, engineering, service, marketing and manufacturing activities; our ability to recruit and retain key personnel; our ability to manage financial risk, and to manage expenses during economic downturns; risks related to the global nature of our operations, including our operations in emerging markets; currency fluctuations and other international factors; changes in provision for income taxes, including changes in tax laws and regulations or adverse outcomes resulting from examinations of our income tax returns; potential volatility in operating results; and other factors listed in Cisco's most recent reports on Forms 10-Q and 10-K filed with the SEC. Any forward-looking statements in this presentation are based on limited information currently available to Cisco, which is subject to change. Although any such forward-looking statements and the factors influencing them will likely change, Cisco will not necessarily update the information. Such information speaks only as of the date of this presentation.