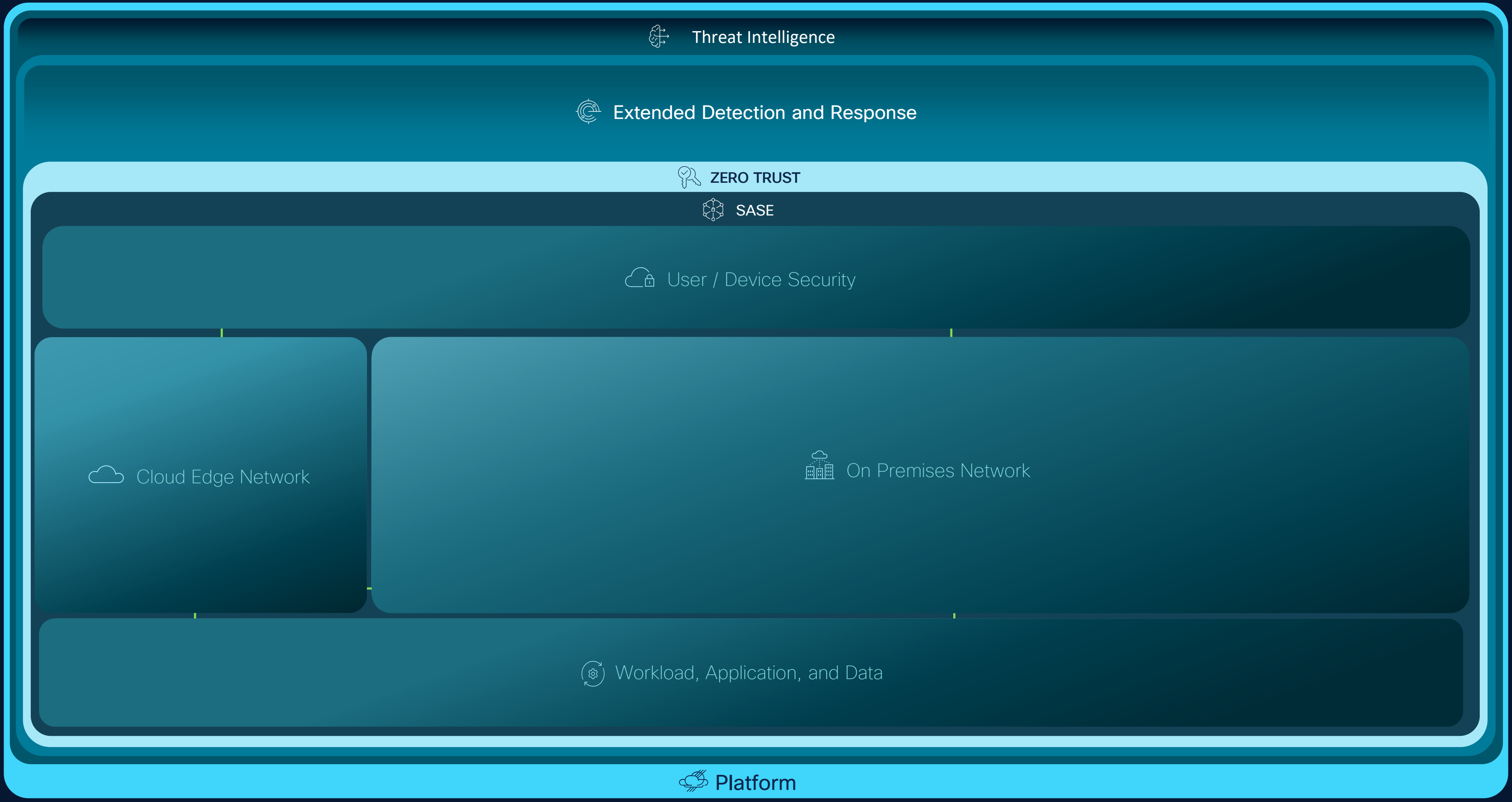
Cisco Security Reference Architecture

Architecture overview and use cases

Global Security Architecture Team

May 2024



Threat Intelligence

Extended Detection and Response

ZERO TRUST

SASE

User / Device Security

Cloud Edge Network

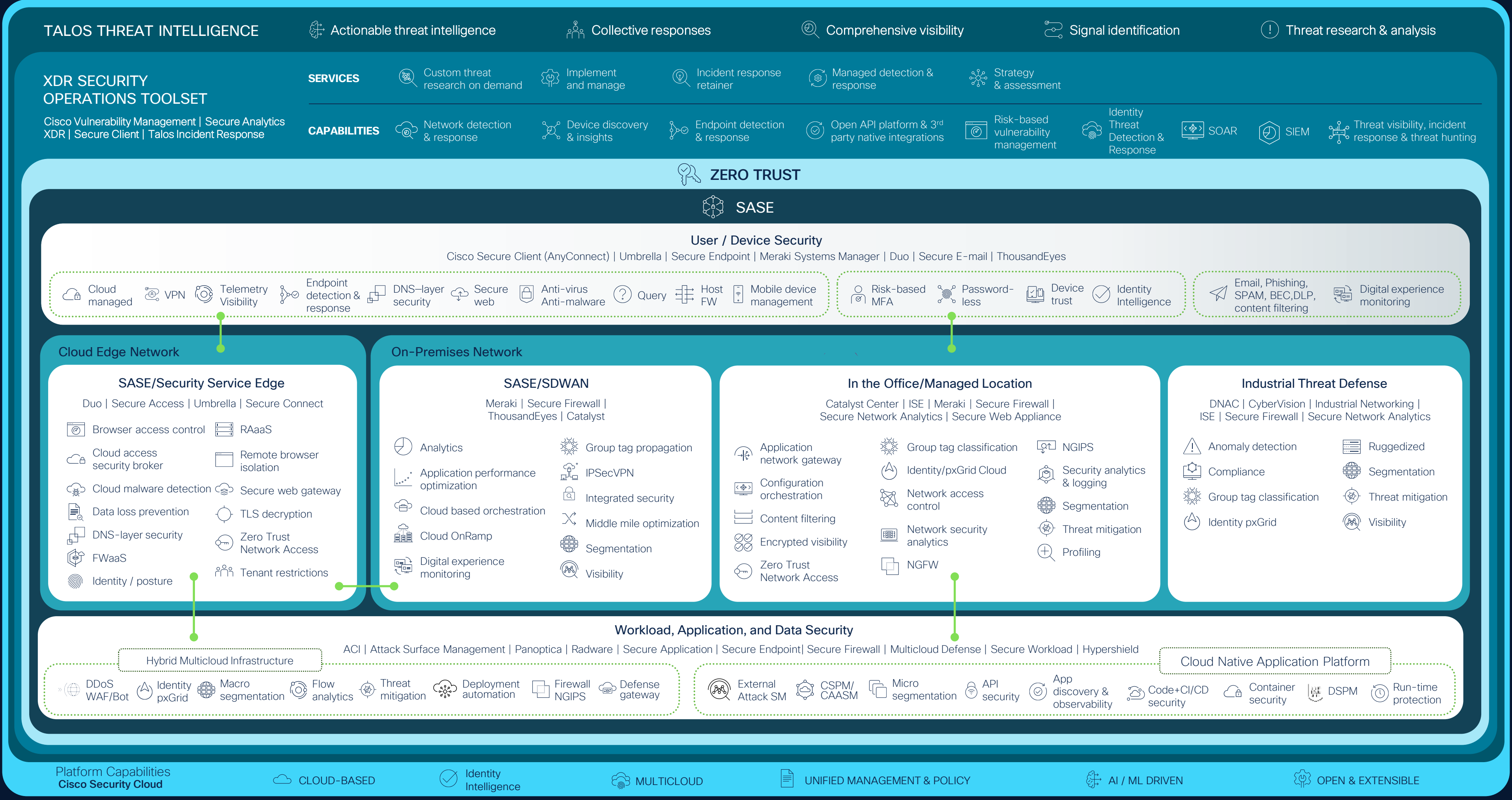
On Premises Network

Workload, Application, and Data

Platform

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 | Identity Threat Detection & Response | SOAR | SIEM | 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 | Identity Intelligence

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

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall |
ThousandEyes | Catalyst

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

In the Office/Managed Location

Catalyst Center | 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 | Hypershield

Hybrid Multicloud Infrastructure

DDoS WAF/Bot | Identity pxGrid | Macro segmentation | Flow analytics | Threat mitigation | Deployment automation | Firewall NGIPS | Defense gateway

Cloud Native Application Platform

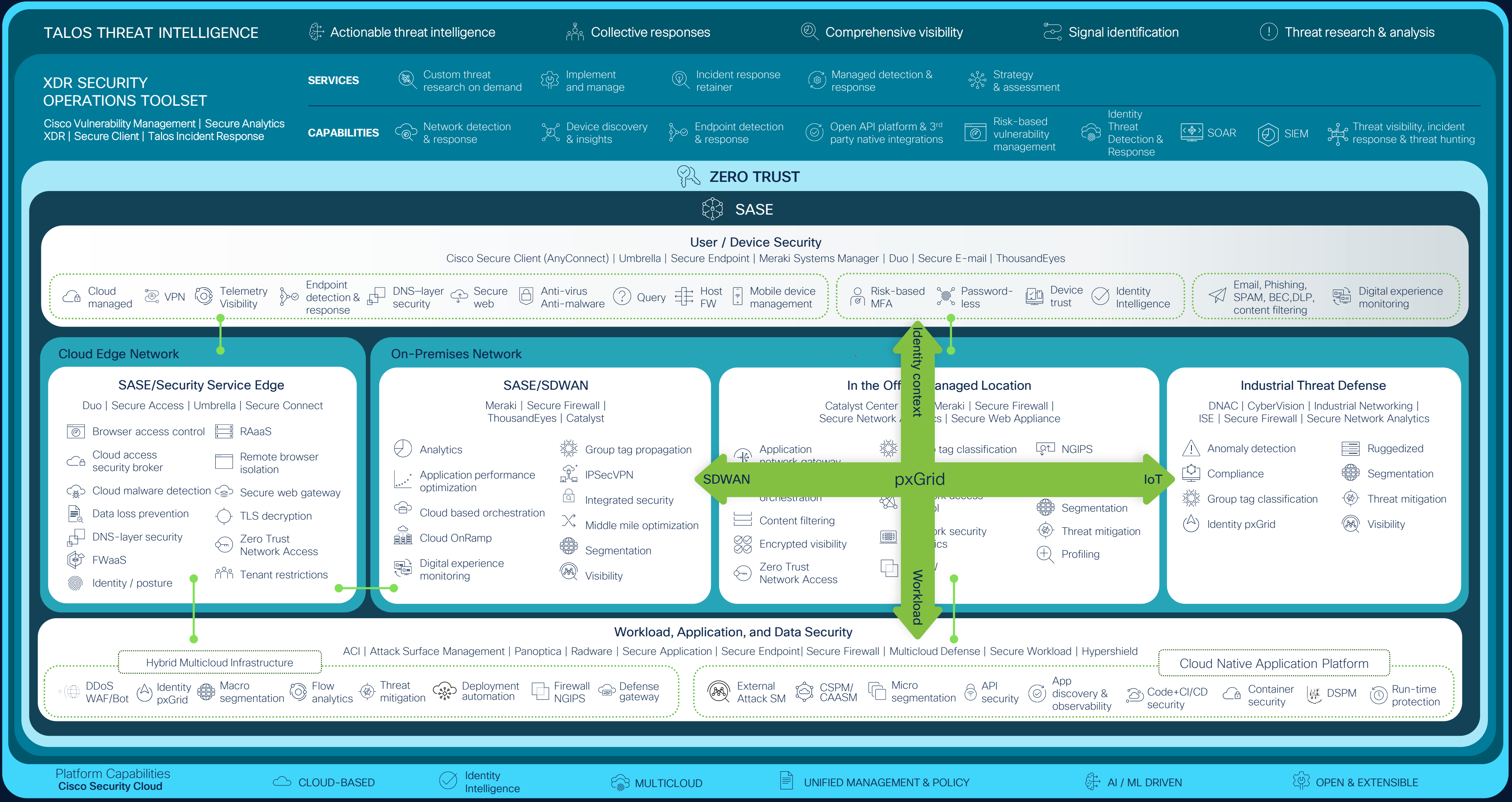
External Attack SM | CSPM/ CAASM | Micro segmentation | API security | App discovery & observability | Code+CI/CD security | Container security | DSPM | Run-time protection

Platform Capabilities
Cisco Security Cloud

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

Common Identity

Security Reference Architecture



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
- Identity Threat Detection & Response
- SOAR
- SIEM
- 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
- Identity Intelligence

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

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall |
ThousandEyes | Catalyst

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

In the Off anaged Location

Catalyst Center Meraki | Secure Firewall |
Secure Network / cs | Secure Web Appliance

- Application network gateway
- tag classification
- NGIPS
- orchestration
- ork access
- l
- Segmentation
- Content filtering
- ork security
- ics
- Threat mitigation
- Encrypted visibility
- Profiling
- Zero Trust Network Access
- /

Industrial Threat Defense

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

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

Workload, Application, and Data Security

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

Hybrid Multicloud Infrastructure

- DDoS WAF/Bot
- Identity pxGrid
- Macro segmentation
- Flow analytics
- Threat mitigation
- Deployment automation
- Firewall NGIPS
- Defense gateway

Cloud Native Application Platform

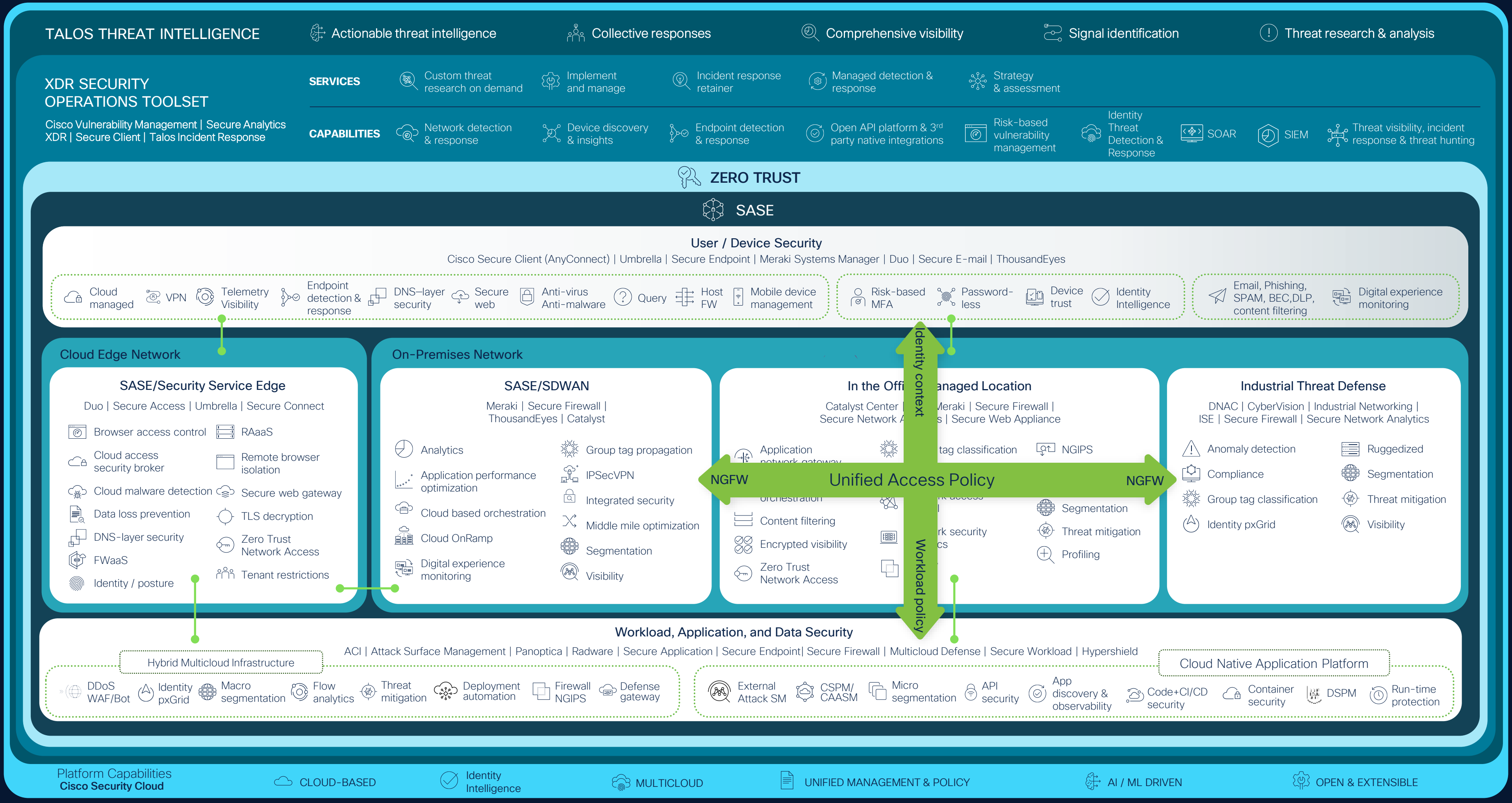
- External Attack SM
- CSPM/ CAASM
- Micro segmentation
- API security
- App discovery & observability
- Code+CI/CD security
- Container security
- DSPM
- Run-time protection

Platform Capabilities
Cisco Security Cloud

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

Converged Multicloud Policy

Security Reference Architecture



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; Identity Threat Detection & Response; SOAR; SIEM; 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; Identity Intelligence

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

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Catalyst

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

In the Offi anaged Location

Catalyst Center | eraki | Secure Firewall | Secure Network A s | Secure Web Appliance

Application network gateway; tag classification; NGIPS; orchestration; k access; l; Segmentation; Content filtering; rk security; cs; Threat mitigation; Encrypted visibility; Profiling; Zero Trust Network Access

Identity context

NGFW | Unified Access Policy | NGFW

Workload policy

Industrial Threat Defense

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

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

Workload, Application, and Data Security

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

Hybrid Multicloud Infrastructure: DDoS WAF/Bot; Identity pxGrid; Macro segmentation; Flow analytics; Threat mitigation; Deployment automation; Firewall NGIPS; Defense gateway

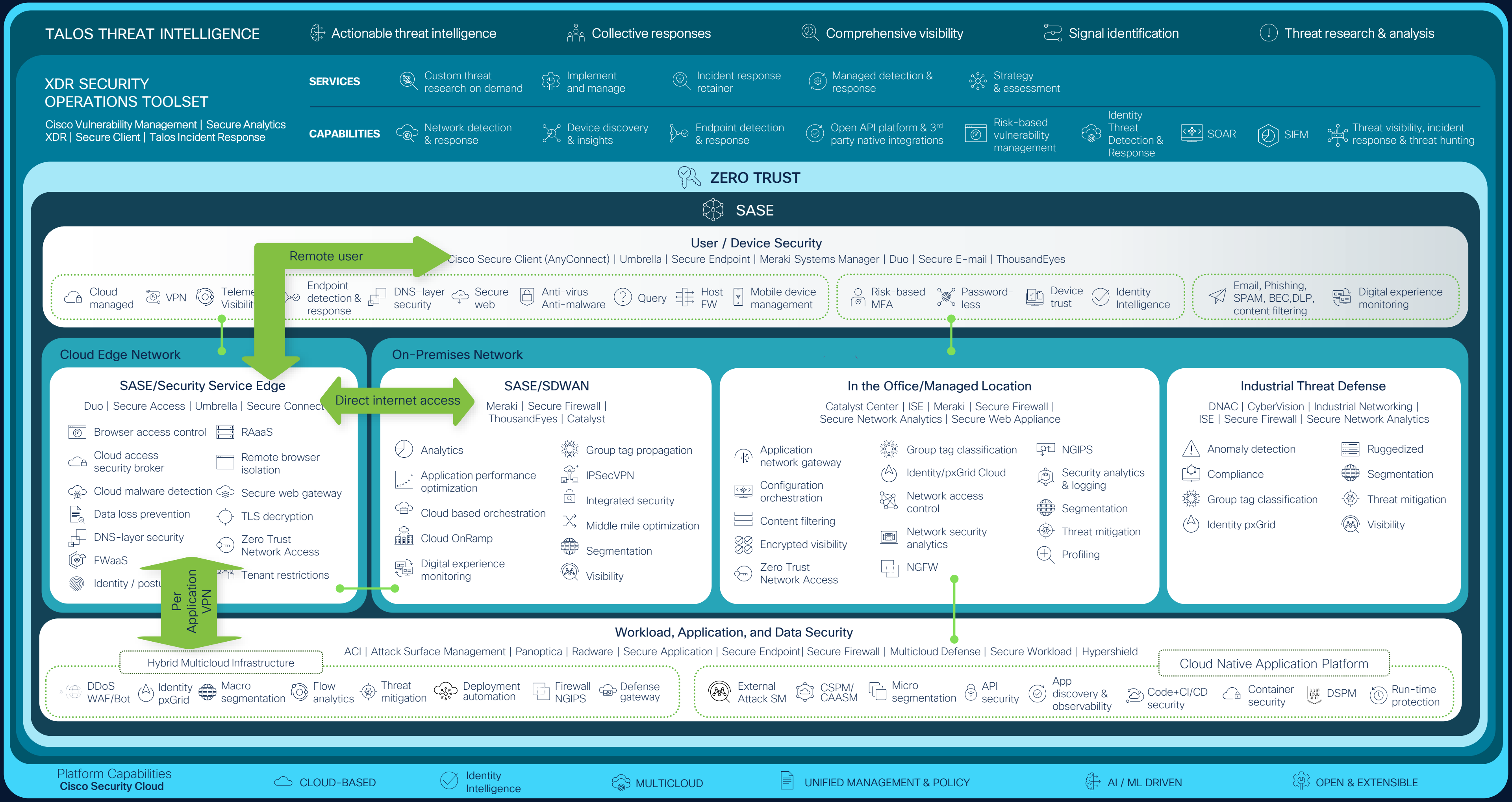
Cloud Native Application Platform: External Attack SM; CSPM/ CAASM; Micro segmentation; API security; App discovery & observability; Code+CI/CD security; Container security; DSPM; Run-time protection

Platform Capabilities
Cisco Security Cloud

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

SSE/SASE

Security Reference Architecture



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
- Identity Threat Detection & Response
- SOAR
- SIEM
- 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
- Teleme… Visibilit…
- 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
- Identity Intelligence
- Email, Phishing, SPAM, BEC,DLP, content filtering
- Digital experience monitoring

Remote user

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect

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

Direct internet access

Per Application VPN

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Catalyst

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

In the Office/Managed Location

Catalyst Center | 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
- Ruggedized
- Compliance
- Segmentation
- Group tag classification
- Threat mitigation
- Identity pxGrid
- Visibility

Workload, Application, and Data Security

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

Hybrid Multicloud Infrastructure

- DDoS WAF/Bot
- Identity pxGrid
- Macro segmentation
- Flow analytics
- Threat mitigation
- Deployment automation
- Firewall NGIPS
- Defense gateway

Cloud Native Application Platform

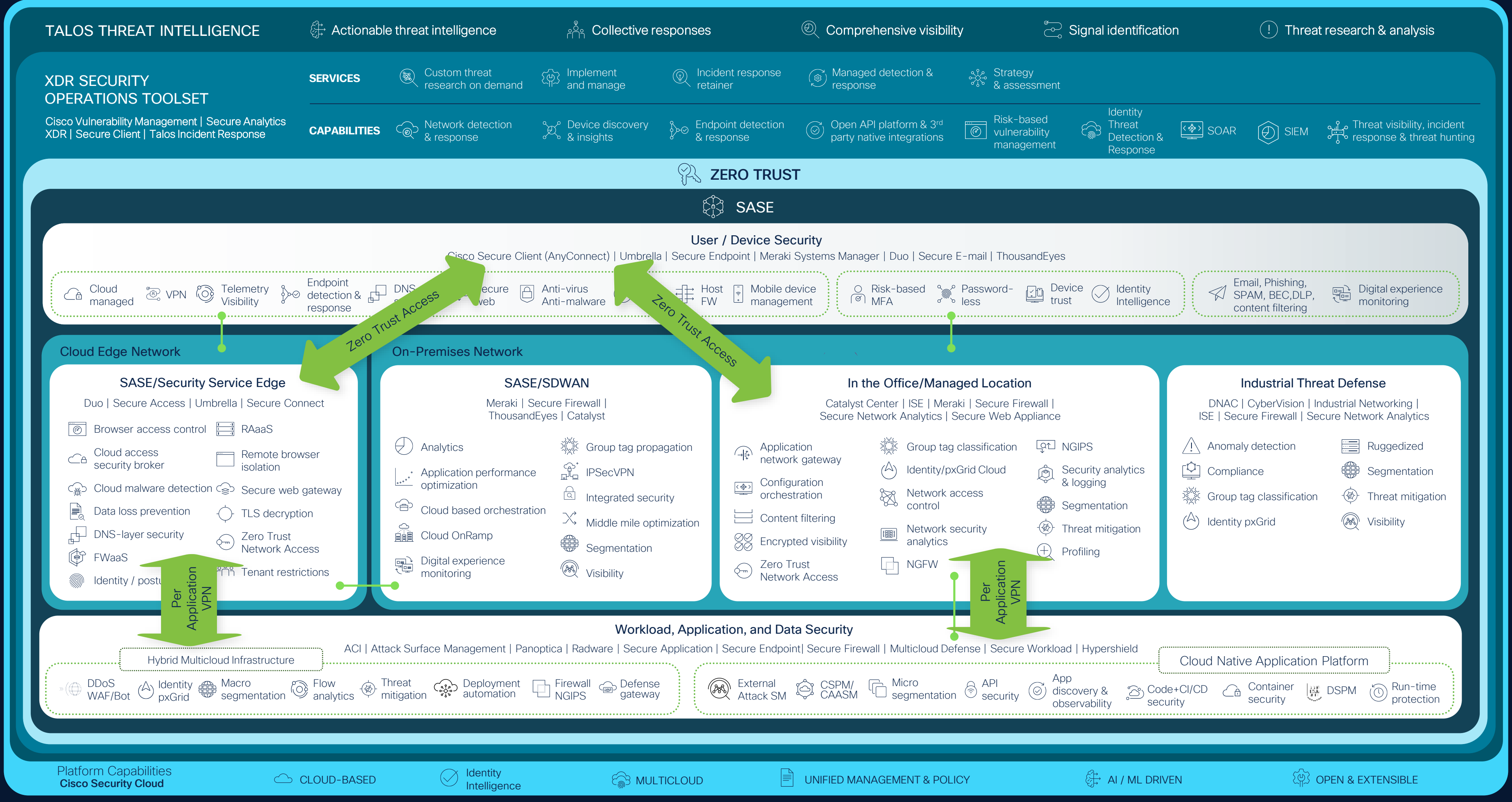
- External Attack SM
- CSPM/ CAASM
- Micro segmentation
- API security
- App discovery & observability
- Code+CI/CD security
- Container security
- DSPM
- Run-time protection

Platform Capabilities
Cisco Security Cloud

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

Zero Trust Access

Security Reference Architecture



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; Identity Threat Detection & Response; SOAR; SIEM; 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; ecure web; Anti-virus Anti-malware; Host FW; Mobile device management

Risk-based MFA; Password-less; Device trust; Identity Intelligence

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

Zero Trust Access

Zero Trust Access

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect

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

Per Application VPN

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Catalyst

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

In the Office/Managed Location

Catalyst Center | 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

Per Application VPN

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 | Hypershield

Hybrid Multicloud Infrastructure

DDoS WAF/Bot; Identity pxGrid; Macro segmentation; Flow analytics; Threat mitigation; Deployment automation; Firewall NGIPS; Defense gateway

Cloud Native Application Platform

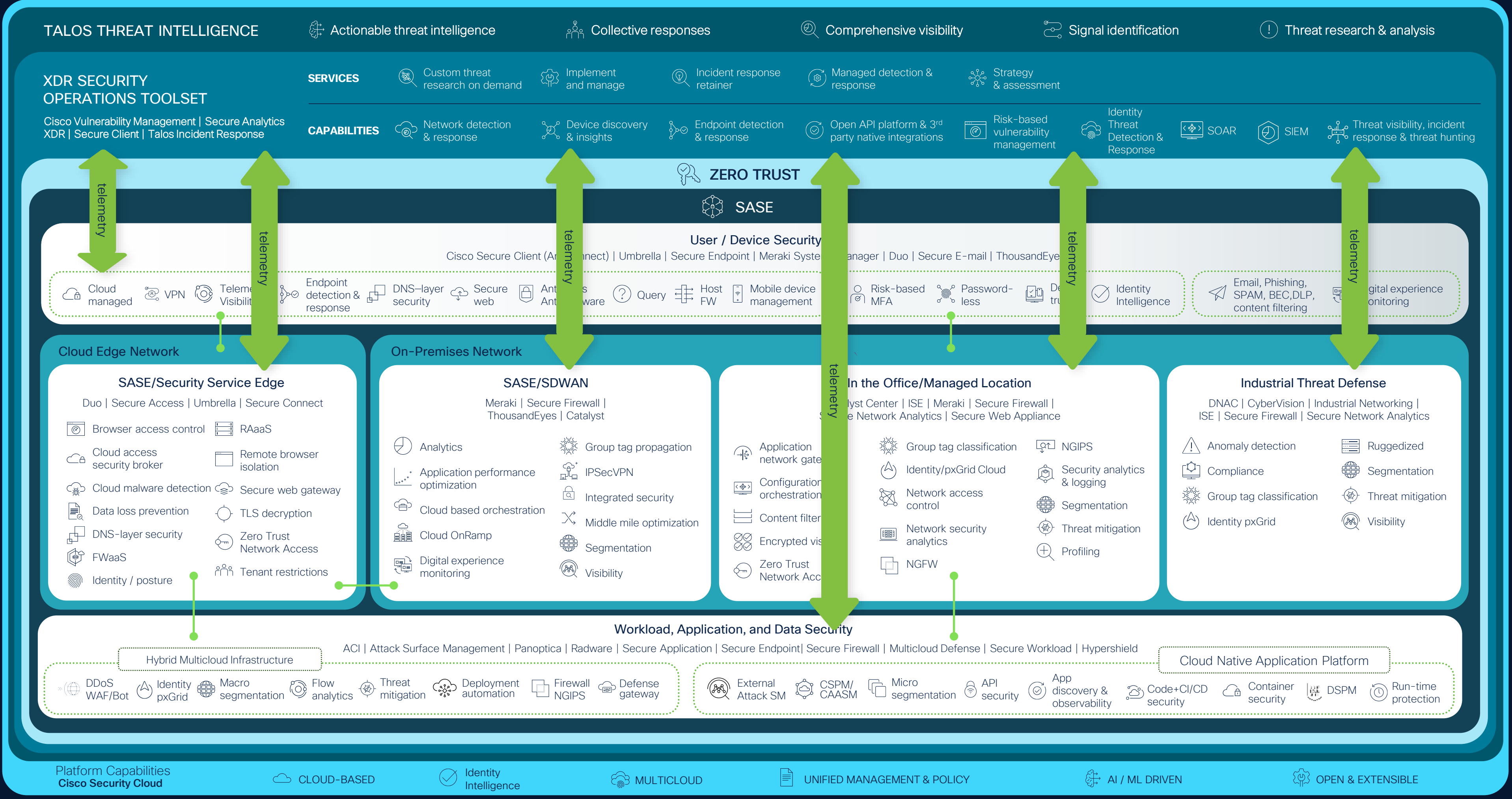
External Attack SM; CSPM/ CAASM; Micro segmentation; API security; App discovery & observability; Code+CI/CD security; Container security; DSPM; Run-time protection

Platform Capabilities
Cisco Security Cloud

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

Extended Detection & Response

Security Reference Architecture



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
Identity Threat Detection & Response
SOAR
SIEM
Threat visibility, incident response & threat hunting

ZERO TRUST

SASE

User / Device Security
Cisco Secure Client (A nect) | Umbrella | Secure Endpoint | Meraki Syste anager | Duo | Secure E-mail | ThousandEye

Cloud managed
VPN
Teleme Visibili
Endpoint detection & response
DNS–layer security
Secure web
Ant Ant s ware
Query
Host FW
Mobile device management
Risk-based MFA
Password-less
De tru
Identity Intelligence
Email, Phishing, SPAM, BEC,DLP, content filtering
gital experience onitoring

telemetry

Cloud Edge Network

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

On-Premises Network

SASE/SDWAN
Meraki | Secure Firewall |
ThousandEyes | Catalyst
Analytics
Group tag propagation
Application performance optimization
IPSecVPN
Integrated security
Cloud based orchestration
Middle mile optimization
Cloud OnRamp
Segmentation
Digital experience monitoring
Visibility

In the Office/Managed Location
lyst Center | ISE | Meraki | Secure Firewall |
e Network Analytics | Secure Web Appliance
Application network gate
Configuration orchestration
Content filter
Encrypted vis
Zero Trust Network Acc
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
Ruggedized
Compliance
Segmentation
Group tag classification
Threat mitigation
Identity pxGrid
Visibility

Workload, Application, and Data Security
ACI | Attack Surface Management | Panoptica | Radware | Secure Application | Secure Endpoint| Secure Firewall | Multicloud Defense | Secure Workload | Hypershield

Hybrid Multicloud Infrastructure
DDoS WAF/Bot
Identity pxGrid
Macro segmentation
Flow analytics
Threat mitigation
Deployment automation
Firewall NGIPS
Defense gateway

Cloud Native Application Platform
External Attack SM
CSPM/ CAASM
Micro segmentation
API security
App discovery & observability
Code+CI/CD security
Container security
DSPM
Run-time protection

Platform Capabilities
Cisco Security Cloud
CLOUD-BASED
Identity Intelligence
MULTICLOUD
UNIFIED MANAGEMENT & POLICY
AI / ML DRIVEN
OPEN & EXTENSIBLE