

 Threat Intelligence

 Extended Detection and Response

 ZERO TRUST

 SASE

 User / Device Security

 Cloud Edge Network

 On Premises Network

 Workload, Application, and Data

 Platform



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 & 3<sup>rd</sup> 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
- RAAs
- 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
- Identity / posture
- 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

TALOS THREAT INTELLIGENCE

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

XDR SECURITY OPERATIONS TOOLSET

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

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

- CAPABILITIES
- Network detection & response
  - Device discovery & insights
  - Endpoint detection & response
  - Open API platform & 3<sup>rd</sup> 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
- 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
- Identity / posture
- 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 | DNA | Secure Network | Meraki | Secure Firewall | Cisco | Secure Web Appliance

- Application network gateway
- Orchestration
- Content filtering
- Encrypted visibility
- Zero Trust Network Access
- Group tag classification
- NGIPS
- 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



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 & 3<sup>rd</sup> 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
- RAAs
- 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 | Secure Network | Meraki | Secure Firewall | Secure Web Appliance

Application security | Content filtering | Encrypted visibility | Zero Trust Network Access | NGIPS | 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

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 & 3<sup>rd</sup> 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, EBC, DLP, content filtering
- Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect

- Browser access control
- RAAs
- 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
- Identity / posture
- 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
- 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

- 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

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 & 3<sup>rd</sup> 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 | Secure Web | Anti-virus | Anti-malware | Host FW | Mobile device management | Risk-based MFA | Password-less | Device trust | Continuous Trust | Email, Phishing, SPAM, EBC, DLP, content filtering | Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

- Duo | Secure Access | Umbrella | Secure Connect
- Browser access control | RAAs
- 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 | Identity / posture
- Tenant restrictions

On-Premises Network

SASE/SDWAN

- Meraki | Secure Firewall | ThousandEyes | Viptela
- Analytics | Group tag propagation
- Application performance optimization | IPsecVPN
- Cloud based orchestration | Integrated security
- Cloud OnRamp | Middle mile optimization
- Digital experience monitoring | Segmentation
- Visibility

In the Office/Managed Location

- Catalyst | DNAC | ISE | Meraki | Secure Firewall | Secure Network Analytics | Secure Web Appliance
- Application network gateway | Group tag classification
- Configuration orchestration | Identity/pxGrid Cloud
- Content filtering | Network access control
- Encrypted visibility | Network security analytics
- Zero Trust Network Access | 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

- 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

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 & 3<sup>rd</sup> 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 | Cisco Connect | Umbrella | Secure Endpoint | Meraki System Manager | Duo | Secure E-mail | ThousandEyes

- Cloud managed VPN
- Telem Visibility
- Endpoint detection & response
- DNS-layer security
- Secure web gateway
- Antivirus
- Query
- Host FW
- Mobile device management
- Risk-based MFA
- Password-less
- Device trust
- Continuous Trust
- Email, Phishing, SPAM, EBC,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
  - Identity / posture
  - 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

- Secure Network Analytics | Secure Web Appliance
- Application network gateway
  - Configuration orchestration
  - Content filter
  - 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