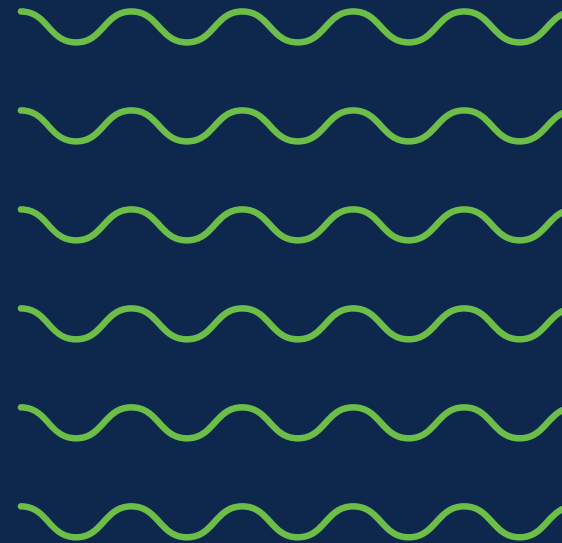


Security Reference Architecture with Use Cases

version 2.0.1

Global Security Architecture Team
February 2022



Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Threat Visibility & Hunting

Security, Orchestration, Automation and Response

Device Insights

Kenna Vuln Mgmt

Incident Response and Remediation Services

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN

Posture

Telemetry

Threat

Query



ThousandEyes (Visibility)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo

ZTNA

DNS-layer security

Secure web gateway

L7 firewall + IPS

Cloud access security broker/shadow IT

RAaaS

SSL decryption

Remote browser Isolation

Data loss prevention

Cloud malware detection

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

SDWAN

Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router

Industrial Firewall

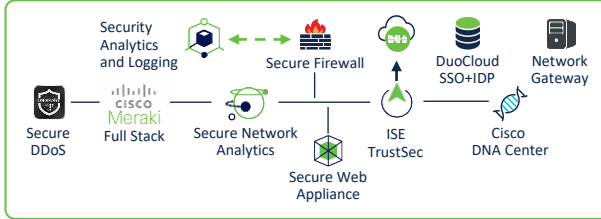
Industrial Switch/AP

Cyber Vision

ISE TrustSec

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility



Application Security

ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security

APIC

Secure Workload

Secure Application by AppDynamics

App Visibility | Detection | Response

Hybrid Private

Public Cloud*

Secure Cloud Analytics

Secure Firewall

ThousandEyes

Security Reference Architecture

Use case: Common Identity / Endpoint Information

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Threat Visibility & Hunting

Security, Orchestration, Automation and Response

Device Insights

Kenna Vuln Mgmt

Incident Response and Remediation Services

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Network Security

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Cloud Edge

Umbrella/Duo

ZTNA DNS-layer security Secure web gateway L7 firewall + IPS Cloud access security broker/shadow IT

RAaaS SSL decryption Remote browser Isolation Data loss prevention Cloud malware detection

SDWAN

Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router Industrial Firewall Industrial Switch/AP Cyber Vision ISE TrustSec

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Secure DDoS Security Analytics and Logging Secure Network Analytics Secure Firewall ISE TrustSec DuoCloud SSO+IDP Network Gateway

Cisco Meraki Full Stack Secure Web Appliance Cisco DNA Center

Application Security

ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

SCN APIC

Secure Workload Secure Application by AppDynamics

App Visibility | Detection | Response

Hybrid Private Public Cloud*

Secure Cloud Analytics Secure Firewall

ThousandEyes

Security Reference Architecture

Use case: Converged Multi-Cloud Policy

TALOS

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

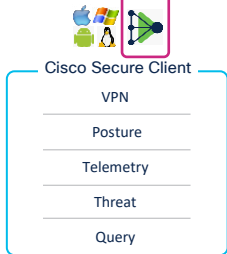
ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



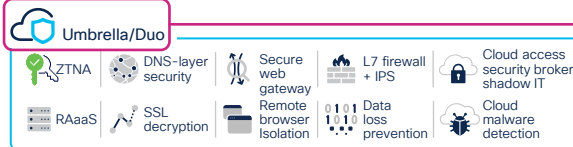
ThousandEyes (Visibility)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access



PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible



On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security



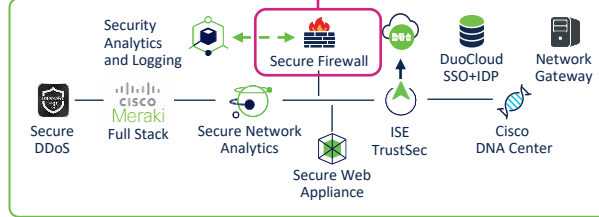
IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

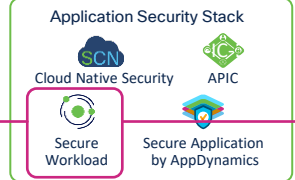


Converged Policy

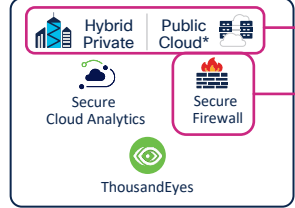
Application Security

ZERO TRUST WORKLOAD

Policy | API Security | Application Segmentation | Run-time Application Security



App Visibility | Detection | Response



Security Reference Architecture

Use case: SASE Integration

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN

Posture

Telemetry

Threat

Query



ThousandEyes (Visibility)

Network Security

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo



Cloud Edge

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

SDWAN



On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security



IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility



Application Security

ZERO TRUST WORKLOAD

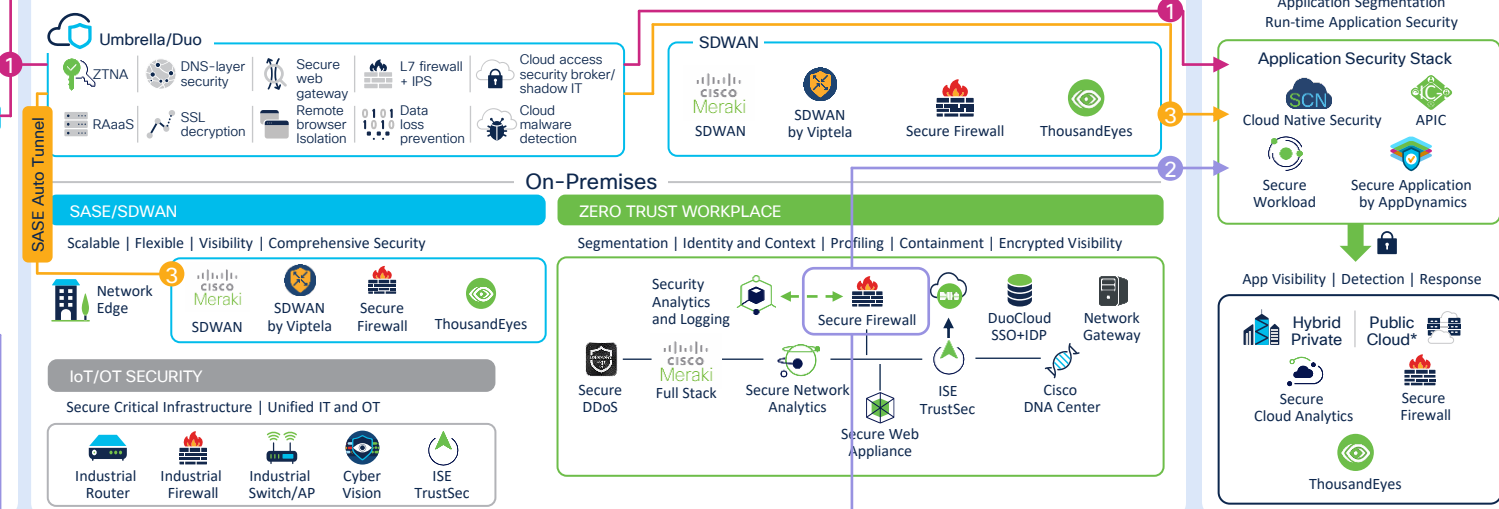
Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security | APIC



App Visibility | Detection | Response



Security Reference Architecture

Use case: Zero Trust Network Access (ZTNA)

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN

Posture

Telemetry

Threat

Query



ThousandEyes (Visibility)

Network Security

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo

ZTNA DNS-layer security Secure web gateway L7 firewall + IPS Cloud access security broker/shadow IT

RAaaS SSL decryption Remote browser Isolation Data loss prevention Cloud malware detection

Cloud Edge

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

SDWAN

Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router Industrial Firewall Industrial Switch/AP Cyber Vision ISE TrustSec

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Secure DDoS Cisco Meraki Full Stack Secure Network Analytics Secure Firewall ISE TrustSec DuoCloud SSO+IDP Network Gateway Cisco DNA Center

Application Security

ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security APIC

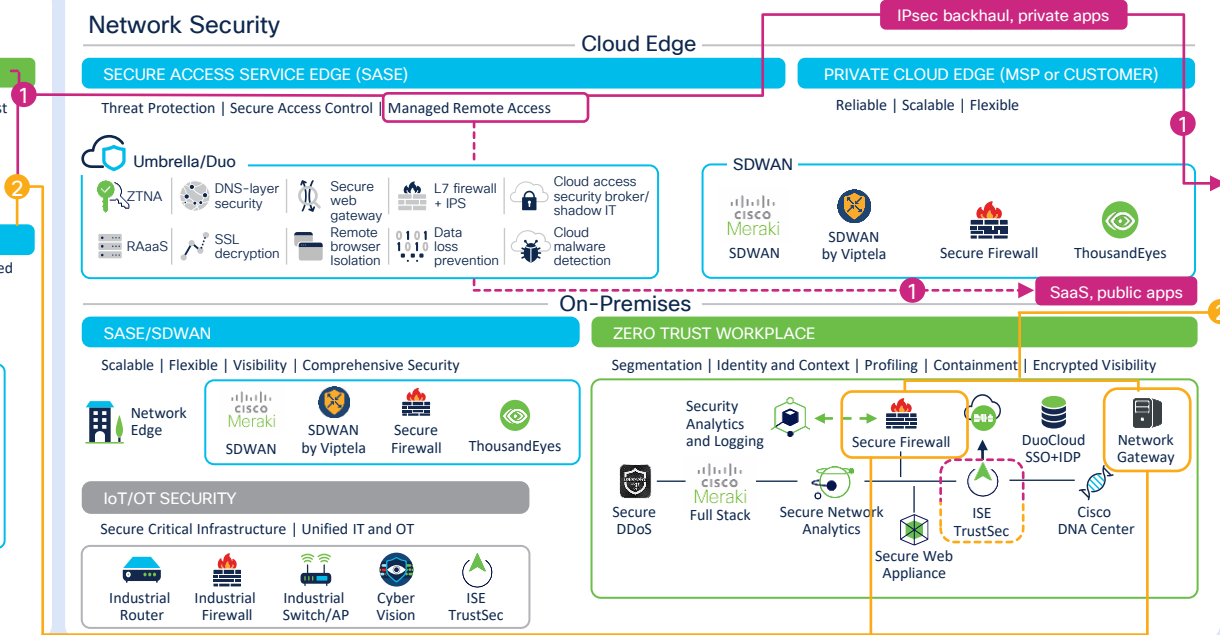
Secure Workload Secure Application by AppDynamics

App Visibility | Detection | Response

Hybrid Private Public Cloud*

Secure Cloud Analytics Secure Firewall

ThousandEyes



Security Reference Architecture

Use case: SecureX Telemetry

TALOS

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

VPN

Posture

Telemetry

Threat

Query

ThousandEyes (Visibility)

Network Security

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo

ZTNA

DNS-layer security

Secure web gateway

L7 firewall + IPS

Cloud access security broker/shadow IT

RAaaS

SSL decryption

Remote browser Isolation

Data loss prevention

Cloud malware detection

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router

Industrial Firewall

Industrial Switch/AP

Cyber Vision

ISE

TrustSec

Cloud Edge

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

SDWAN

Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

On-Premises

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Security Analytics and Logging

Secure Firewall

ISE TrustSec

DuoCloud SSO+IDP

Network Gateway

Secure DDoS

Meraki Full Stack

Secure Network Analytics

Secure Web Appliance

Cisco DNA Center

Application Security

ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

SCN Cloud Native Security

APIC

Secure Workload

Secure Application by AppDynamics

App Visibility | Detection | Response

Hybrid Private

Public Cloud*

Secure Cloud Analytics

Secure Firewall

ThousandEyes

Security Reference Architecture

Use case: SecureX Orchestration

TALOS

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN

Posture

Telemetry

Threat

Query



ThousandEyes (Visibility)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo



DNS-layer security

Secure web gateway

L7 firewall + IPS

Cloud access security broker/shadow IT



SSL decryption

Remote browser Isolation

Data loss prevention

Cloud malware detection

SDWAN

Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security



Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router

Industrial Firewall

Industrial Switch/AP

Cyber Vision

ISE TrustSec

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Security Analytics and Logging

Secure Firewall

ISE TrustSec

DuoCloud SSO+IDP

Network Gateway

Secure DDoS

Meraki Full Stack

Secure Network Analytics

Secure Web Appliance

Cisco DNA Center

Application Security

ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

SCN Cloud Native Security

APIC

Secure Workload

Secure Application by AppDynamics

App Visibility | Detection | Response

Hybrid Private

Public Cloud*

Secure Cloud Analytics

Secure Firewall

ThousandEyes

