



## Network Security

### Firewall Threat Defense & NGIPS (ASA)

- Stateful FW + VPN (S2S & Client)
- Application Visibility & Control (AVC)
- NGIPS w/Security Intelligence <sup>1</sup>
- Malware Defense (AMP) <sup>1</sup>
- URL (Content, Category etc.) <sup>1</sup>
- DDoS protection (Radware OEM) <sup>1</sup>
- [Free trial link](#) <sup>3</sup>

### Firewall Threat Defense Management

- **Firewall Management Center (FMC)**
  - Impact Flags / Recommended Rules
- **Device Manager (FDM)**
  - On-box, \$0 additional cost
- **Cisco Defense Orchestrator (CDO)**
  - Cloud based Mgmt., (US, EU, APJ)
  - Manage Firepower, ASA, Meraki MX...
  - [Free trial link](#) <sup>3</sup>

### Meraki MX (Cloud Managed)

- Stateful FW & AVC
- Auto VPN
- Intrusion Prevention (IDS/IPS) <sup>2</sup>
- URL / Content Filter <sup>2</sup>
- Anti-Malware filter <sup>2</sup>

### Secure Email (ESA / CES)

- On-site hardware or cloud
- Spam / Graymail protection
- Phishing Defense (APP) <sup>1</sup>
- File Reputation / Analysis <sup>1</sup>
- Secure Email Encryption Service
- [Free trial link](#) <sup>3</sup>

### Secure Web Appliance (WSA)

- On-site hardware or cloud proxy
- Anti-Virus & Malware Defense options <sup>1</sup>
- L7 AVC controls
- Bandwidth throttling
- Data Loss Prevention (DLP) <sup>1</sup>
- TLS/SSL Decrypt

## XDR

### Secure Endpoint (AMP for Endpoints)

- Multi OS endpoint malware protection
- Antivirus - EDR & EPP (TETRA & ClamAV)
- Continuous analysis
- Retrospective security
- IoC (Indication of Compromise)
- Endpoint Isolation
- Advanced Search (Orbital)
- **Secure Endpoint Pro**
- [Free trial link](#) <sup>3</sup>

### Secure Malware Analytics (Threat Grid)

- File / Malware Analysis (Sandbox)
- Threat Intelligence through API
- Cloud (SaaS) or On-Premise

### Secure Mobility Client (AnyConnect)

- Virtual Private Network (VPN)
- Roaming Client (Umbrella) Module
- Malware Defense Module (AMP)
- System Scan (ISE Posture) Module
- Endpoint Analytics + Splunk® (CESA) <sup>1</sup>

### Kenna Security

- SaaS Vulnerability and Risk Intelligence
- Manage, Prioritize and Predict risk
- Threat intel and predictive modeling
- [Free trial link](#) <sup>3</sup>

### SecureX

- \$0 cost (with any Cisco Security product)
- Cloud based Unified Visibility interface
- Integrate Cisco & non-Cisco tools
- **Orchestration** (Automate workflows)
- **Device Insights** (FAQ)
  - Type/location of devices connected
  - Device version & vulnerabilities
- **Threat Response (CTR)**
  - Cloud-based SOC research tool
  - Global & Local integrations

## SASE / Cloud

### Umbrella (DNS / SIG)

- Manage Category & Applications
- Malware Defense (Smart & Full Proxy)
- Data Loss Prevention (DLP)
- Remote Browser Isolation (RBI) <sup>1</sup>
- Full Proxy & Logging (w/SIG) <sup>1</sup>
- [Free trial link](#) <sup>3</sup>

### Umbrella-Investigate

- Predictive Threat Intelligence
- Relationships between Domains

### Cloudlock (CASB)

- Cloud App security & DLP
- Application FW

### Secure Email Cloud Mailbox (CMD)

- API for O365 (Azure)
- Inspect attachments & links
- Insider threats / lateral movement
- [Free trial link](#) <sup>3</sup>

### Secure Cloud Analytics (Stealthwatch Cloud)

- Secure Private/Public Cloud/Hybrid
- AWS, Azure, Google & On-Prem
- Netflow analytics (Netflow & IPFIX)
- Behavioral Threat Detection
- [Free trial link](#) <sup>3</sup>

### Secure Cloud Insights

- Cloud security posture visibility
- Relationship mapping
- Security and compliance reporting
- Cyber Asset Inventory
- [Free trial link](#) <sup>3</sup>

### Cisco+ Secure Connect Choice (CSMRA)

- Managed secure remote access
- Hosted ZTNA

### Cisco+ Secure Connect Now

- SASE As-a-Service
- Cloud hosted remote access
- Unified SD-WAN & SSE stack

## Zero Trust

### Identity Services Engine (ISE)

- Identity & Access Control (wired, Wi-Fi)
- Asset Visibility, Device Profiling
- RADIUS, TACACS+, 802.1x
- Compliance, Posture, Segmentation
- Rapid Threat Containment
- [Free trial link](#) <sup>3</sup>

### Secure Network Analytics (Stealthwatch)

- Behavior Anomaly Detection
- Encrypted Traffic Analytics (ETA)
- Network Performance Monitoring
- Netflow & VPC analytics (IPFIX & other flows)
- Agentless East-West traffic intelligence
- Net performance & capacity planning
- **Telemetry Broker:** hybrid cloud visibility
- Security Analytics and Logging (SAL)

### Secure Workload (Tetration)

- Agent based DC Application Security
- L7 Enforcement within OS
- Minimize the Attack Surface
- Protects on-premises & cloud
- Micro-segmentation / Visibility
- Available as a SaaS or on-Prem

### Cyber Vision

- IoT Security (bridge IT & OT security)
- ICS Visibility & Detection
- Behavior Analytics

### Secure Access by Duo (Duo)

- **Multi-Factor Authentication** (MFA)
- **Secure Single Sign-on** (SSO)
- **Passwordless Authentication**
- **Device Visibility**
- **Clientless Remote Access**
- **Duo Network Gateway** (DNG)
- **Adaptive Access Policies**
- [Free trial link](#) <sup>3</sup>