Cisco Security Overview

From Endpoint to Cloud and everything in-between

cisco Partner (Partner)

Network Security

Secure Firewall & NGIPS (ASA & FTD)

- Stateful FW + VPN (S2S & Client)
- Application Visibility & Control (AVC)
- Indication of Compromise (IoC)
- NGIPS *
- Geo-based rules
- Security Intelligence *(with NGIPS)*
- Advanced Malware Protection (AMP) *
- URL *(Content, Category etc.)* *
- DDoS protection *(Radware OEM)* *

Secure Firewall Management options

- **Firepower Management Center (FMC)**
  - Best option for SOC (passive inspection)
  - Impact Flags
  - Recommended Rules
  - Hardware or Virtual
- **Firepower Device Manager (FDM)**
  - On-box, $0 additional cost
- **Cisco Defense Orchestrator (CDO)**
  - Cloud based Mgmt., (US, EU, APJ)
  - Manage Firepower, ASA, Meraki MX…
  - Security Analytics & Logging (SAL) *

Meraki MX *(Cloud Managed)*

- Stateful FW & AVC
- Auto VPN *(AnyConnect FY20)*
- Intrusion Prevention (IDS/IPS) **
- URL / Content Filter **
- Anti-Malware filter (AMP) **
- Geo-based rules **
- Umbrella *

Secure Endpoint VPN (AnyConnect)

- Virtual Private Network (VPN)
- Roaming Client (Umbrella) Module
- AMP Enabler Module
- System Scan (ISE Posture) Module
- Network Visibility Module
- Endpoint Analytics + *Splunk®* (CESA) *

* *Licensed feature*
** *Advanced License (Meraki)*

Access & Endpoint

Secure Endpoint (AMP for Endpoints)

- Multi OS endpoint malware protection
- Antivirus (EDR & EPP)
- Continuous analysis
- Retrospective security
- IoC *(Indication of Compromise)*
- Endpoint Isolation
- Advanced Search *(Orbital)*

Secure Malware Analysis (Threat Grid)

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

Secure Email (ESA / CES / CMD)

- On-site hardware or Cloud
- Email Encryption (CRES)
- Reputation filtering
- Spam / Graymail protection
- Advanced Phishing Protection (APP) *
- File Reputation / Analysis *
- Domain protection (DMP) *
- Centralized manager (SMA)
- **Cloud Mailbox Defense (CMD)**
  - Cloud Email Supplemental Security
  - API for *O365*
  - SaaS

SecureX *(Available June 2020)*

- Cloud based Unified Visibility interface
- Automate security workflows
- Integrate Cisco & non-Cisco tools
- $0 cost *(with Security license)*
- **Cisco Threat Response (CTR)**
  - Cloud-based SOC research tool
  - Global & Local integrations

Cloud Security

Secure Cloud Edge (Umbrella / SIG)

- Manage Category & Applications
- Block access to malicious sites
- Identify already infected devices
- AMP *(Smart & Full Proxy)*
- Remote Browser Isolation (RBI) *
- On-site & Roaming capability
- Full Proxy & Logging *(w/SIG)* *

Umbrella-Investigate

- Predictive Threat Intelligence
- Relationships between Domains
- Enrich security data w/ API

Cloudlock (CASB)

- Cloud App security
- Cloud DLP
- Application FW
- SaaS, IaaS, PaaS, and IDaaS

Secure Web (WSA)

- On-site hardware or Cloud Proxy
- Reputation based
- Anti-Virus options *
- Malware Protection (AMP) *
- L7 AVC controls
- Bandwidth throttling
- Data Loss Prevention (DLP) *
- SSL Decrypt
- Centralized Manager (SMA)
- Anomaly Detection (CTA)

Cognitive Threat Analytics (CTA)

- Network Anomaly Detection
- Analyze W3C Proxy logs
- Available for W3C compliant Proxy

Visibility & Segmentation

Secure Network Access (ISE)

- Identity & Access Control *(wired, Wi-Fi)*
- Asset Visibility, Device Profiling
- RADIUS, TACACS+, 802.1x
- Compliance, Posture, Segmentation
- Rapid Threat Containment

Secure Analytics (Stealthwatch)

- Behavior Anomaly Detection
- Encrypted Traffic Analytics (ETA)
- Network Performance Monitoring
- Netflow analytics *(IPFIX & other flows)*
- Agentless East-West traffic intelligence
- Net performance & capacity planning
- NaaS, NaaE

Stealthwatch Cloud

- Secure Private/Public Cloud/Hybrid
- *AWS*, *Azure*, *Google* & On-Prem
- Netflow analytics *(Netflow & IPFIX)*
- Behavioral Threat Detection
- Cloud-based console

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 (Duo / MFA)

- Two-Factor Authentication (2FA)
- Secure Single Sign-on (SSO)
- Device visibility
- Clientless remote access
- On-Prem or Cloud - IDaaS

WO-05272020