Cisco Security Overview v5

- *Product name*
- *Former product name*

https://cs.co/1page

Network Security

Secure Firewall & Secure IPS
- Stateful FW + VPN (S2S & Client)
- Application Visibility & Control (AVC)
- Intrusion Prevention (IPS) [1]
- Security Intelligence [1]
- Encrypted Visibility Engine (EVE) [1]
- Malware Defense (AMP) [1]
- URL (Content, Category etc.) [1]
- Secure DDoS protection [1]
- *Free trial*

Secure Firewall Cloud Native
- Scalable RAVPN architecture
- Multi-tenancy
- Clientless Access Gateway (CAG)

Firewall Threat Defense Mgmt.
- Firewall Management Center (FMC)
- Device Manager (FDM)
  - On-box, $0 additional cost
- Cisco Defense Orchestrator (CDO)
  - Cloud based Mgmt., (US, EU, APJ)
  - *Free trial*
- Cloud Delivered FMC (cdFMC)
  - Cloud based Mgmt.

Meraki MX
- Cloud Managed
- Stateful FW, AVC & Auto VPN
- Intrusion Prevention (IDS/IPS) [1]
- URL / Content Filter [1]
- Anti-Malware filter [1]

Secure Web Appliance (WSA)
- Web Proxy
- AV & Malware Defense options [1]
- L7 AVC controls
- Bandwidth throttling
- Data Loss Prevention (DLP) [1]
- TLS/SSL Decrypt
- Secure Web & Email Manager

Cyber Vision
- IoT Security - Bridge IT & OT Security
- DPI on Industrial protocols
- ICS Visibility & Detection
- Behavior Analytics

Identity Services Engine (ISE)
- Identity & Access Control (wired, Wi-Fi)
- Asset Visibility, Device Profiling
- RADIUS, TACACS+, 802.1x
- Compliance, Posture, Segmentation

pxGrid
- Integrate Security products with open API
- Rapid Threat Containment

Secure Endpoint (AMP for Endpoints)
- Multi OS endpoint malware protection
- Antivirus - EDR & EPP (TETRA & ClamAV)
- Endpoint Isolation
- USB Device Control
- Advanced Search (Orbital)
- Managed Detection and Response (MDR)
- *Free trial*

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

Endpoint Security Analytics (CESA)
- Endpoint Analytics + *Splunk®*

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

Application Delivery Controller (ADC)
- Monitors and manage network traffic
- SSL Inspection (SSLi) Bundles

Cisco Talos
- Threat Intelligence
- Reputation Center
- Talos Incident Response
- Talos Blog
- OpenSource software

Cloud and Application Security

Cisco Secure Access
- Security Service Edge (SSE)
- Secure access to all applications
- Modular ZTNA, SWG, CASB, and FWaaS
- ThousandEyes

Cisco+ Secure Connect
- SASE As-a-Service
- Cloud hosted remote access

Umbrella (DNS / SIG)
- Manage Category & Applications
- Malware Defense (Intel & Full Proxy)
- Data Loss Prevention (DLP)
- Remote Browser Isolation (RBI) [1]
- Umbrella Investigate [1]
- *Free trial*

Cloudlock (CASB)
- Cloud App Sec, DLP & App FW
- Optical Character Recognition (OCR)
- Realtime DLP for WebEx

Cisco Secure Client (AnyConnect)
- Virtual Private Network (VPN)
- Umbrella, Malware Defense, Posture modules
- Network Visibility Module (NVM)

Attack Surface Management (Cloud Insights)
- Cloud security posture visibility
- Cyber Asset Inventory
- *Free trial*

Secure Email (ESA / CES)
- Spam / Graymail protection
- File Reputation / Analysis [1]
- *Free trial*

Secure Email Threat Defense (CMD)
- API for *O365 (Azure)*
- Insider threats / lateral movement
- *Free trial*

Secure DDoS Protection
- Layer 3-7 protection against DDoS
- On-prem, cloud, or hybrid solutions

User and Device Security

Cisco XDR
- Cloud based Threat Detection and Response
  - XDR Analytics (PNM and PCM)
  - Telemetry Broker
  - Network Visibility Module (NVM)
- Integrated Cisco and 3rd party solutions
- Prioritization of events by impact
- *Free Trial*

Cisco Duo
- Multi-Factor Authentication (MFA)
- Secure Single Sign-on (SSO)
- Passwordless Authentication
- Device Visibility
- Clientless Remote Access
- Duo Network Gateway (DNG)
- Trusted Endpoint
- *Free trial*

Secure Workload (Tetration)
- Agent based DC Application Security
- L7 Enforcement within OS
- Minimize the Attack Surface
- Micro-segmentation / Visibility
- Available as a SaaS or on-Prem

Cisco Vulnerability Management (Kenna)
- SaaS Vulnerability and Risk Intelligence
- Prioritize and manage high-risk vulnerabilities
- Threat intel and predictive modeling
- *Free trial*

Cisco Multicloud Defense (Valtix)
- Cloud Network SaaS
- Multi-Cloud based Firewall
- Cyber asset visibility
- Unify Security: *AWS, Azure, Google, Oracle*
- *Free Trial*

Panoptica
- Cloud-Native Application Protection (CNAPP)
- Secure Application Cloud

Secure Web Application Firewall (WAF)
- Bot Protection
- Defend web apps, mobile apps, and APIs

[1] *Licensed feature* | *Use Licensing & Software for PoV's and Labs* | *Technology features listed are not comprehensive.*