Cisco Security Overview v6

Cisco Security Portfolio & related features.

• **Product name**• Former product name

Free trial

Free trial

Cloudlock (CASB)

API for O365 (Azure)

Secure Email Threat Defense (CMD)

■ File analysis / reputation / Spam protection

Insider threats / lateral movement

Cloud App Sec, DLP & App FW

Secure Endpoint (AMP for Endpoints)

Multi OS endpoint malware protection

Antivirus - EDR & EPP (TETRA & ClamAV)

■ Endpoint Isolation & USB Device Control

Secure Malware Analytics (Threat Grid)

■ File / Malware Analysis (Sandbox)

Manage URL Category & Applications

Malware Defense (Intel & Full Proxv)

■ Remote Browser Isolation (RBI) ¹

Realtime DLP for WebEx

Security Connector (iOS)

Advanced Search (Orbital)

Data Loss Prevention (DLP)

Umbrella Investigate ¹

User / Device

cisco
Partner
https://cs.co/1page

Application / Data

Application Delivery Controller (ADC)

- Monitors and manage network traffic
- SSL Inspection (SSLi) Bundles

Cisco Hypershield

- Al-native security for DC and cloud
- Distributed Exploit Protection
- Autonomous Segmentation

Cisco Multicloud Defense (Valtix)

- Multi-Cloud Network based Firewall SaaS
- Cyber asset visibility
- Unify Security: AWS, Azure, Google, Oracle
- Free Trial (SCC)

Cisco Vulnerability Management (Kenna)

- SaaS Vulnerability and Risk Intelligence
- Prioritize and manage high-risk vulnerabilities
- Threat intel and predictive modeling
- Free trial

Isovalent

- Integrates with Kubernetes for deep visibility
- eBPF kernel technology for advanced features

Secure DDoS Protection

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

Secure Web Application Firewall (WAF)

- Bot Protection
- Defend web apps, mobile apps, and APIs

Secure Workload (Tetration)

- Agent based DC Application Security
- L7 Enforcement within OS
- Micro-segmentation / Visibility
- Available as a SaaS or on-Prem

Cisco Security Suites

- User Suite
- Breach Suite
- Cloud Suite

Cisco Talos

- Threat IntelligenceReputation Center
- Talos Blog
- OpenSource SW

Network / Cloud

Cisco Al Defense

- Protect development and use of AI apps
- Safeguard against misuse of AI tools

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
- <u>pxGrid</u>: Integrate security w/open API
- o Rapid Threat Containment

Meraki MX

- Cloud Managed
- Stateful FW, AVC & <u>Auto VPN</u>
- Intrusion Prevention (IDS/IPS) ¹
- URL. Content & Anti-Malware filters ¹

Secure Firewall & Secure IPS

- Stateful FW + VPN (S2S & Secure 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 Mgmt.

- Firewall Management Center (FMC)
- Device Manager (FDM)
- Cloud Delivered FMC (cdFMC)
- Security Cloud Control (SCC)
- o Free trial (SCC)

Security Analytics & Logging (SAL)

- Logging and Troubleshooting (LT)
- Logging Analytics and Detection (LA)
- Total Network Analytics & Detection (TA)
- <u>Free trial</u> (SCC)

Cisco Duo

- Multi-Factor Authentication (MFA)
- Secure Single Sign-on (SSO)
- Passwordless Authentication
- Device Visibility
- Clientless Remote Access
- Duo Network Gateway (DNG)
- Identity Intelligence (Oort)
- Free trial

Cisco Secure Access

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

<u>Cisco Secure Client</u> (AnyConnect)

- Virtual Private Network (VPN)
- Umbrella, Malware Defense, Posture modules
- Network Visibility Module (NVM)
- Cisco Endpoint Security Analytics (CESA)

Cisco Secure Connect

■ SASE As-a-Service / remote access via Cloud

Secure Email (ESA / CES)

- Spam / Graymail protection
- File Reputation / Analysis ¹

XDR / Threat Intelligence

Free trial

Umbrella (DNS / SIG)

- Manage Cisco Security Cloud products
- View Security Cloud Subscriptions

Security Cloud Control (CDO)

- Al Assistant for policy management
- Unified dashboard for complete visibility

Secure Network Analytics (Stealthwatch)

- Behavior Anomaly Detection
- Encrypted Traffic Analytics (ETA)
- Netflow & VPC analytics (IPFIX & other)Agentless East-West traffic intelligence
- Telemetry Broker: hybrid cloud visibility

Secure Web Appliance (WSA)

- Web Proxy / L7 AVC controls
- AV & Malware Defense options ¹
- Data Loss Prevention (DLP) ¹
 TLS/SSL Decrypt
- 6-----

¹ Licensed feature | Use <u>Licensing & Software</u> for PoV's and Labs | Technology features listed are not comprehensive.

Secure Web & Email Manager

Cisco XDR

- Threat Detection and Response
 - o XDR Analytics (PNM and PCM)
- Network Visibility Module (NVM)
 Integrated Cisco and 3rd party solutions
- Integrated Cisco and 3rd party
 Ransomware Defense
- Prioritization of events by impact

Cisco Talos Incident Response (CTIR)

24-hour emergency response

Managed Detection & Response (MDR)

■ Detection, Analysis, Investigation & Response

Splunk

- Splunk Security
- Splunk Observability
- Free trials