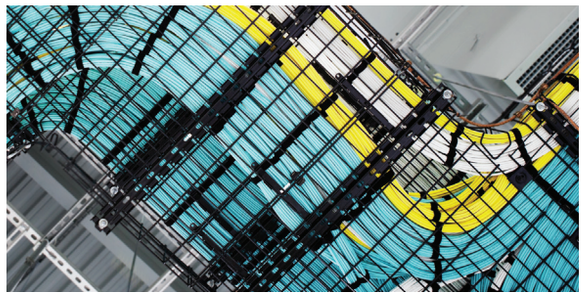
Secure Access and Mobility



Identity Services Engine

Identity Services Engine delivers superior user and device visibility to support enterprise mobility experiences and to control access.

- Simplify guest experiences for easier guest onboarding and administration.
- Streamline BYOD and enterprise mobility with easy, out-of-the-box setup for self-service device onboarding and management.
- Centralize and unify network access policy management to provide consistent, highly secure access to end users, whether they connect to your network over a wired, wireless, or VPN connection.
- Gain greater visibility and more accurate device identification.

AnyConnect Secure Mobility Client

Cisco AnyConnect provides secure access from anywhere, greater visibility into user and endpoint behavior, comprehensive protection and compliance enforcement, with simplified management and usability. With AnyConnect, you gain a comprehensive endpoint security platform providing the security necessary to keep your organization safe and protected.

Cisco TrustSec Technology

Cisco TrustSec® software-defined segmentation dynamically organizes endpoints into logical groups, called security groups. Security groups are assigned based on business decisions using a richer context than an IP address. They are easier for people to understand and manage. And the number of group-based rules is dramatically less than an equivalent set of rules based on IP addresses.

Cisco TrustSec technology is embedded in more than 40 Cisco product families and third-party products. It isolates attacks, quickly restricts the lateral movement of threats with micro-segmentation, enables a scalable bring-your-own-device (BYOD) environment, and reduces the scope of compliance for industry and government regulations.

Professional and Technical Security Services

Work with experts to anticipate and respond to new threats, reduce complexity and fragmentation, and adapt with agility to changing business models.

Advisory Services

Strategic and technical security advisors conduct assessments and identify opportunities to improve performance, reduce risk and promote compliance.

Implementation Services

Accelerate adoption of the latest security technologies with minimal impact to operations, and optimize existing security technologies to increase effectiveness.

Managed Services

Services such as Active Threat Analytics provide continuous monitoring and advanced analytics capabilities combined with industry-leading threat intelligence and expert investigators to rapidly detect advanced threats.

Support Services

Solve problems faster, improve operational efficiency, and reduce risk of downtime.

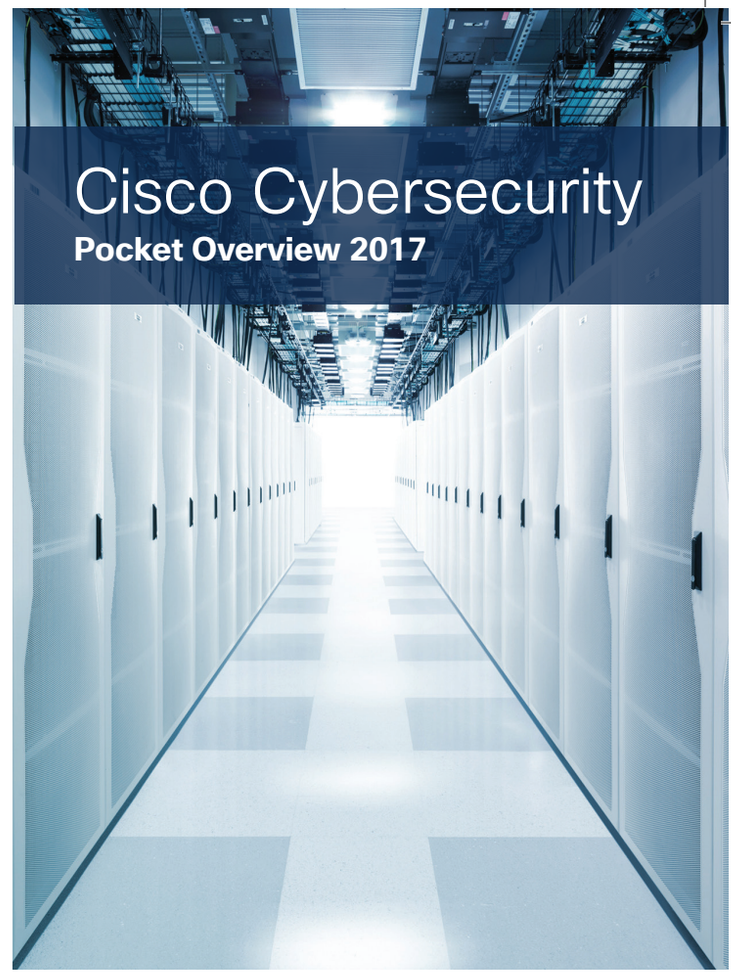
Talos Security Intelligence and Research

Cisco keeps companies safer with the largest threat research team in the world. Talos is comprised of hundreds of threat researchers backed by the sophisticated infrastructure and systems needed to provide exceptional visibility and threat intelligence across the full Cisco Security portfolio.

- Talos is comprised of leading threat researchers supported by sophisticated systems. Talos researchers create threat intelligence for Cisco products to protect customers from both known and emerging threats.
- Talos is backed by unrivaled telemetry data at Cisco, encompassing:
  - 19.7 billion total threat blocks per day
  - 1.5 million incoming malware samples per day
  - 15 billion web requests per day
  - 2,557,767 threats blocked per second

Cisco — for all of your cybersecurity solutions to protect your network and data.

Visit **cisco.com/go/security.** Call your favorite Cisco Partner, your Cisco AM or SE, or call 1.888.Call-Cisco
Download our **2017 Midyear Cybersecurity Report**.



Cisco Cybersecurity

Pocket Overview 2017

Simple Open Automated

The Industry's Most Effective, Integrated Security Portfolio

Global Market Leader in Cybersecurity Solutions

Next-Generation Network and Data Center Security

Protect high-value data with segmentation, application control, threat defense, secure virtualization, and consistent policy control.

Cisco Firepower Next Generation Firewall (NGFW)

- Industry's first fully-integrated, threat-focused next-generation firewall
- Firepower Threat Defense: Firewall, App Visibility and Control (AVC) that integrates with NGIPS, AMP and URL Filtering.
- Optional third-party apps (e.g. DDoS)
- Fully-integrated single centralized manager: Firepower Management Center
- Platform series with wide range of sizes and form factors; specialized features for the datacenter or service providers
- On-box Firepower Device Manager for Firepower 2100 Series and 5500-X Series running Firepower Threat Defense software image.

Cisco ASA with FirePOWER Services

- Combines legendary ASA robustness with advanced threat defense
- Stateful firewall, NAT, VPN
- Threat Defense: AMP, NGIPS, URL Filtering, AVC
- Management: ASDM (local) / CSM (central) and FireSIGHT Management Center (centralized)

FirePOWER Next-Generation IPS (NGIPS)

- Delivers industry-leading throughput, threat detection effectiveness, and total cost of ownership
- Wide model range covering every performance and form-factor need

Cisco Virtual Adaptive Security Appliance (ASAv)

Cisco Virtual Firepower Next Generation Firewall (NGFWv)

Cisco Virtual FirePOWER Next-Generation IPS (NGIPSv)

Meraki MX

Built on Cisco Meraki's award-winning cloud-managed architecture, the MX is the industry's only 100 percent cloud-managed unified threat management (UTM) appliance–combining security, networking and application control in a single device.

AMP & Threat Grid for Advanced Threat Protection

Cisco Advanced Malware Protection (AMP) continuously monitors threat activity across your extended network to automatically prevent, detect, and contain threats. AMP provides you with global threat intelligence from TALOS, advanced sandboxing, and real-time malware blocking to prevent breaches. If a threat is discovered, AMP is the only solution in the world that provides retrospective security so you can see where a threat entered the network, where it went, what it did, and who was infected so you can quickly remediate the problem.

- Cisco Next Gen Intrusion Prevention System
- Cisco ASA with Firepower Services
- Cisco NGFW
- Cisco AMP for Endpoints
- Cisco AMP for Networks
- Cisco AMP for Web and Email
- Cisco AMP on Integrated Services Router (ISR)

Cisco Threat Grid

Combines static and dynamic malware analysis with threat intelligence into one unified solution. Provides integrated sandboxing for Cisco ASA with FirePOWER Services, ESA, WSA, AMP for Networks, and AMP for Endpoints to protect across the attack continuum from both known and unknown malware.

Cisco Stealthwatch® (Security)

Cisco Stealthwatch® (Security) helps automate security by leveraging the network as a sensor to deliver context-aware threat alerts. When combined with ISE, it can identify suspicious flows on the network, understand what user and device they pertain to, and automatically enforce a security policy to quarantine the infected device.

Cloud Security

Cisco Umbrella and Cisco Umbrella Investigate

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. And because it's built into the foundation of the internet and delivered from the cloud, Umbrella is the simplest security product to deploy and delivers powerful, effective protection.

Cisco Umbrella Investigate provides the most complete view of internet domains, IPs, ASNs, and file hashes to accelerate investigations, decrease incident response times, and uncover potential threats.

Cisco Cloudlock

Cisco Cloudlock is the cloud-native Cloud Access Security Broker (CASB) that helps accelerate use of the cloud. Cisco Cloudlock secures your cloud identities, data, and apps, combating account compromises, data breaches, and cloud app ecosystem risks, while facilitating compliance through a simple, open, and automated API-driven approach.

Cisco Email Security

- Fight spam, viruses, and blended threats for organizations of all sizes
- Enforce compliance and protect reputation and brand assets
- The only email security with retrospective security provided by AMP
- Backed by Talos for rapid protection from new and emerging threats
- Cloud-based and hybrid (onsite appliance plus cloud) solutions available; receive the same email protection regardless of form factor
- Cost-effective cloud-based solution that reduces your onsite data center footprint
- Dedicated email security instances in multiple, resilient Cisco data centers promote exceptional service availability and data protection

Web Security

Web Security Appliance (WSA)

Provides on and off network protection for http and https traffic along with granular usage controls, including application visibility and control Flexible deployment, including on-premises and virtual options.

Cisco Content Security Management Appliance

Cisco Cognitive Threat Analytics (CTA)

Identify novel threats and security breaches through behavioral analysis of anomalies in http and https traffic.

CTA is available as a standalone solution or through a seamless integration with the Cisco Web Security portfolio.