Cisco Cybersecurity Partner Pocket Guide 2016

Why Security?

Security: A Growth Engine for the Digital Economy

As much as the Digital Economy and the Internet of Everything (IoE) create opportunities for companies and consumers – over $19 trillion in value to organizations over the next decade, they also create opportunities for hackers and cybercriminals. With an expanded attack surface represented by the IoE, cybercriminals look to cash in on the estimated value of $450 billion to over $1 trillion of the Hacker Economy.

The most effective way to confront this dynamic threat landscape is to make security as pervasive as the Internet of Everything itself – extending to wherever employees are and wherever data is – to include Security Everywhere.

By embedding security everywhere across the extended network, security becomes an enabler for business to take full and secure advantage of opportunities presented by new digital business models and the Internet of Things (IoT).

Security: A Critical Boardroom Topic

There is mounting concern at the senior executive and board level regarding information security and the risk of lost intellectual property, compromised customer information and confidence, and valuation impact.

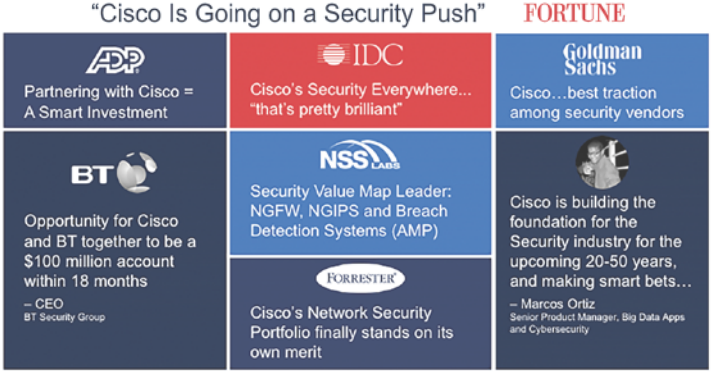
- Chief information security officers (CISOs) are challenged to push boardroom discussions into additional security investment.
- These are critical considerations as organizations become more agile and try to grow their business models in the face of the evolving trends of mobility, cloud computing, and advanced targeted attacks.

Why Cisco?

Cisco: The Leading Security Company

Cisco is widely recognized throughout the industry as offering best-in-class solutions (Figure 1) and was named Best Security Company at the 2016 SC Magazine Awards. Cisco Identity Services Engine (ISE) also won the award for Best Network Access Control (NAC) Solution.

Figure 1 Market Recognition of Cisco Security Solutions



The Cisco security portfolio was rated "positive" in Gartner's 2015 Vendor Rating and is a leader in the Gartner Magic Quadrants for:

- Intrusion Prevention Systems (November 2015)
- Secure Email Gateways (July 2015)

Cisco has been a consistent leader in multiple NSS Labs Security Value Maps (SVM) and had the highest Security Effectiveness score in the following test reports:

- Breach Detections Systems – 99.2% (September 2015)
- Next Generation IPS – 99.5% (April 2015)
- Next Generation Firewall – 99.2% (November 2014)

Third-party tests of IT security solutions validate vendor claims of solution effectiveness and performance. Cisco continues to be a leader in third-party testing year after year.

Cisco Talos Security Intelligence and Research Group: Renowned Threat Intelligence and Expertise from the Leaders in Cyber Security

The Cisco Talos Security Intelligence and Research Group is composed of elite cybersecurity experts whose threat intelligence detects, analyzes, and protects against both known and emerging threats by aggregating and analyzing Cisco's unrivaled telemetry data of:

- 19.7 billion total threat blocks per day
- 1.5 million incoming malware samples per day
- 1.1 billion web-filtering blocks per day
- 1 billion SenderBase reputation queries per day
- 2,557,767 threats blocked per second

The result is a security intelligence cloud producing "big intelligence" and reputation analysis that track threats across networks, endpoints, mobile devices, virtual systems, web, and email.

This provides a holistic understanding of threats, their root causes, and scopes of outbreaks, translating into leading security effectiveness for Cisco security solutions.

Talos also maintains the official rule sets of Snort, ClamAV, SenderBase, and SpamCop.

The OpenDNS Security Labs team also works with TALOS to complement threat researchers with data scientists and infrastructure engineers. OpenDNS builds big data systems, 3D visualizations, and statistical models to automatically identify where attacker infrastructures are staged on the Internet–before attacks launch. OpenDNS also maintains PhishTank, DNScrypt, and OpenGraffiti.

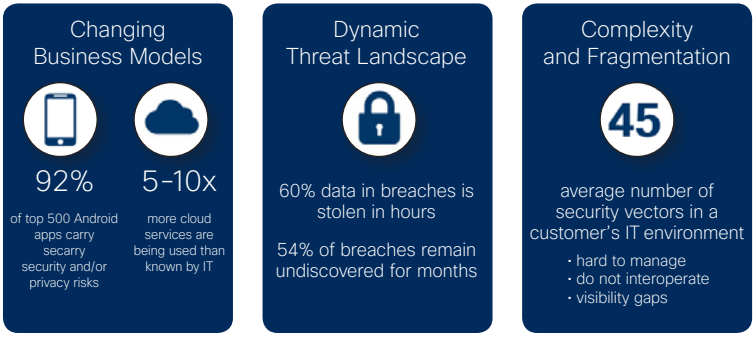
Cisco Security Research: www.cisco.com/go/talos
Cisco Security Reports: www.cisco.com/go/securityreports
OpenDNS Security Labs Blog: labs.opendns.com/blog
Talos Blog: http://blog.talosintel.com

The Cisco Security Strategy

The Security Challenges

A combination of three major realities has made the task of defending a network more difficult than ever, while helping attackers find new ways to evade defenses (Figure 2).

Figure 2 Security Challenges



Changing business models: The Internet of Everything is accelerating change, creating new attack vectors and making it even more difficult to defend the organization. At the same time, however, the IoE opens up huge opportunities for business as long as it is secured.

Dynamic threat landscape: Attackers have become much more sophisticated and well financed, and their attacks have moved from static to dynamic, from visible to hidden. Without near real-time discovery capabilities, an organization will be at a significant disadvantage.

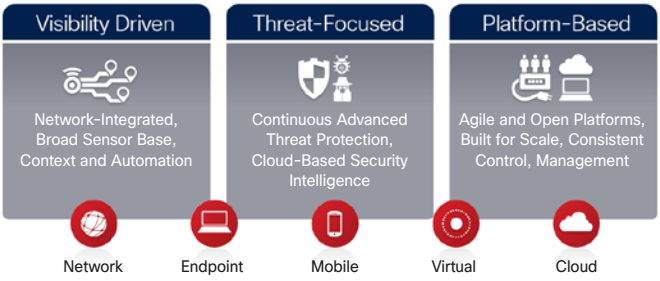
Complexity and fragmentation: Most organizations have dozens of security technologies that often do not interoperate, and this situation is exacerbated by a significant lack of available security specialists in the market.

Attackers take advantage of these security challenges, employing methodical approaches to circumvent the target's security infrastructure. Once inside the network they often remain unnoticed. According to studies by Cisco, more than 50 percent of all attacks manage to persist without detection for months or even years before they are discovered and, once discovered, several weeks before full containment and remediation are achieved.

Cisco's Threat-Centric Security Model

By taking a threat-centric and operational approach to security, the Cisco security model reduces complexity and fragmentation while providing superior visibility, continuous control, and advanced threat protection (Figure 3). The security model focuses on three strategic imperatives:

Figure 3 The Security Model



Visibility-driven: Organizations must be able to accurately see what is happening in the environment. Breadth and depth of visibility provides context and information needed to take rapid security action.

Threat-focused: Traditional security approaches focus on policy and controls, which limit the ability to protect against sophisticated cyberattacks. Cisco's threat-centric approach is different. It focuses on identifying, detecting, and stopping known and unknown threats. This is an ongoing process that requires continuous analysis and real-time security intelligence that is shared across the integrated security architecture, with all individual devices informing each other and acting in unison.

Platform-based: Security is now more than a network issue; it requires an integrated system of open platforms that cover the network, data center and the cloud. These platforms need to be built for scale and centrally managed for unified policy and consistent controls. This constitutes a shift from stand-alone point solutions to a fully integrated threat defense architecture.

Protection Across the Full Attack Continuum

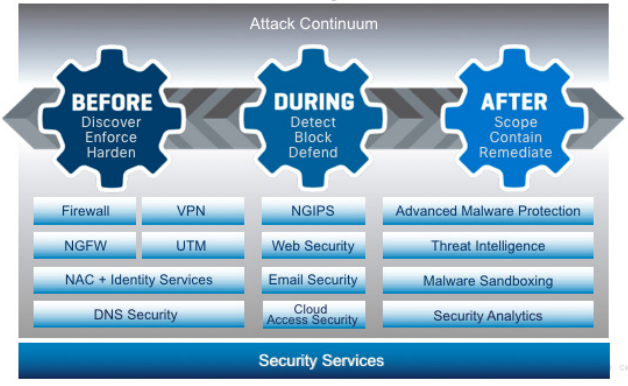
There are three stages to an attack: before, during, and after. Through a combination of technology and services, the Cisco security model implements protection across entire attack continuum:

Before an attack: It begins with visibility - organizations need to know what is on their network to be able to defend it (physical and virtual hosts, operating systems, applications, services, protocols, users, content, etc). If they don't understand what they are trying to protect, they will be unprepared to configure security technologies to control access, enforce policy and defend their infrastructure.

During an attack: Given the nature of advanced attacks today, the best threat detection product alone isn't sufficient to protect the environment. What is needed is a security infrastructure that can aggregate and correlate data from across the extended network with historical patterns and global attack intelligence to provide context and discriminate between active attacks, exfiltration, and reconnaissance versus simply background noise.

After the attack: Invariably, some attacks will be successful, and organizations need to be able to detect malware that is sophisticated enough to alter its behavior to avoid detection. They need to determine the scope of the damage, remediate, and bring operations back to normal.

Figure 4 Security Products Used Along the Attack Continuum



Only Cisco delivers an architectural security model with platform-based solutions that integrate into an overall security system. Continuous monitoring, automated analysis, and control automation exist already. But to extend these capabilities everywhere requires an architectural approach – the new Security Everywhere approach.

Cisco Security Product Portfolio

Next-Generation Network and Data Center Security

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

Cisco Firepower Next Generation Firewall (NGFW)

Cisco Firepower NGFW is the industry's first fully-integrated, threat-focused next-generation firewall that keeps customers safer, mitigates advanced threats faster, and streamlines operations better. This allows customers to stop more threats, get more from their resources and positions security as a growth engine to seize new business opportunities.

Cisco Firepower 4100 Series

- Threat-focused security platform to address use cases from the Internet edge to the data center
- Performance and density optimized – 10Ge and 40Ge interface options and over 60,000 Mbps in 1 RU box
- Unified visibility and management of firewall policy, application control, Firepower Next-Gen IPS, and advanced malware protection

Cisco Firepower 9300

- Scalable, carrier-grade platform designed for service providers and others requiring low latency and exceptional throughput
- Apply security inspection services dynamically across the network fabric, with intelligent provisioning of Cisco and partner security services.
- Security Module architecture enables flexible configuration and performance scaling

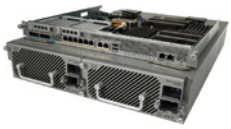
Cisco Firepower Management Center

- Fully integrated management of Cisco's threat-focused network security devices (NGFW, NGIPS, AMP) in a single console.
- Centralized management of firewall rules and configuration, control of over 4,000 applications, intrusion prevention policies, and advanced malware analysis.
- Automatically correlates Indications of Compromise across network and endpoint sensors, with automated risk ranking that empowers your security team to better focus their efforts.

Cisco ASA 5500-X with FirePOWER Services (NGFW)

- Offers the industry's first threat-focused NGFW
- Combines ASA firewall with Cisco next-generation IPS (NGIPS) and Advanced Malware Protection (AMP)
- Platform series with wide range of sizes and form factors

Cisco ASA 5585-X with FirePOWER Services (NGFW)



- Purpose-built security appliance for data centers
- Delivers highest performance, resiliency, and scalability through leading-edge clustering
- Combines ASA firewall with Cisco Firepower NGIPS and Cisco AMP

Cisco FirePOWER Next-Generation IPS (NGIPS)

- Offers the most advanced threat protection in the industry
- Delivers industry-leading throughput, threat detection efficacy, and low TCO
- Platform series with wide range of sizes and form factors
- Reduce complexity while gaining superior visibility, consistent control, and advanced threat protection across the entire attack continuum.

Cisco Adaptive Security Virtual Appliance (ASAv)

- Supports both traditional and next-generation software-defined network (SDN) and Cisco Application Centric Infrastructure (ACI) environments.
- Brings full ASA firewall and VPN capabilities supporting multiple hypervisor environments, reducing administrative overhead, and increasing operational efficiency.
- Predetermined configurations accelerate and simplify security service provisioning to provide dynamically scalable security.
- Provides vSwitch support for Cisco, hybrid, and non-Cisco data centers

Cisco Virtual Next-Generation IPS for VMware

- Offers a virtualized Cisco FirePOWER NGIPS solution
- Reclaims the visibility lost when virtualizing
- Extends Payment Card Industry (PCI) compliance to virtual environments

Advanced Threat Solutions

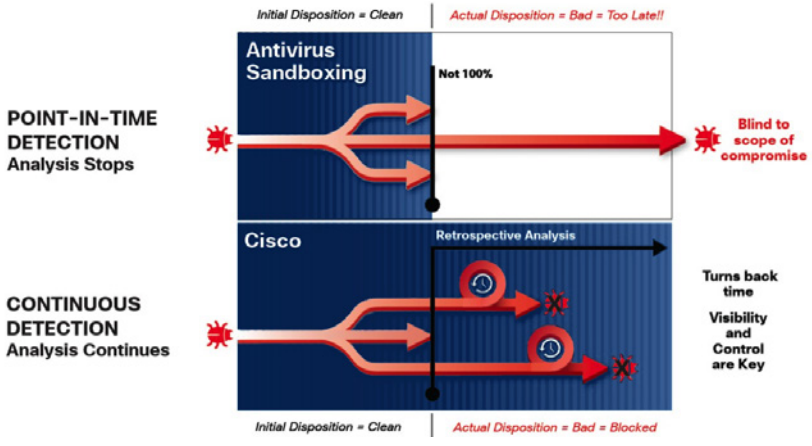
Advanced Malware Protection

Cisco Advanced Malware Protection (AMP) provides the visibility and control security teams need to not only prevent breaches, but also quickly detect, contain, and remediate malware before damage can be done. AMP continuously analyzes and records all file activity on a system (Figure 5). If a file behaves suspiciously, AMP retrospectively alerts security teams, providing a detailed recorded history of the malware's behavior over time. AMP can then contain or remediate with a few clicks.

AMP does this by providing:

- The best threat intelligence and malware analysis to strengthen defenses
- Point-in-time protection in the form of file signatures, file reputation, and sandboxing to block known and emerging threats
- Continuous analysis and retrospective security to detect malware that manages to evade initial inspection.

Figure 5 Point in Time Detection vs. Continuous Detection



Check out www.cisco.com/go/security to learn more.

"**AMP Everywhere**": Cisco offers the industry's broadest portfolio of integrated Advanced Malware Protection solutions providing coverage across multiple attack vectors – network, endpoint, mobile, virtual, email and web.

- Cisco AMP for Endpoints
- Cisco AMP for Networks
- Cisco AMP Private Cloud Virtual Appliance
- Cisco AMP on ASA with FirePOWER Services
- Cisco AMP on Email Security Appliance (ESA)
- Cisco AMP on Web Security Appliance (WSA)
- Cisco AMP on Cloud Web Security (CWS)
- Cisco AMP on Integrated Services Router (ISR)

Cisco AMP Threat Grid

- Combines static and dynamic malware analysis with threat intelligence into one unified solution.
- Integrates real-time behavioral analysis and up-to-the-minute threat intelligence feeds with existing security technologies.
- 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 attacks.

StealthWatch System

The StealthWatch® System dramatically improves network visibility, security and incident response across the entire network. StealthWatch provides real-time situational awareness of all users, devices and traffic on the network, in the data center and in the cloud, allowing security teams to quickly and effectively detect and respond to threats by providing real-time, continuous monitoring and a pervasive view into all network traffic.

StealthWatch does this by leveraging:

- Behavioral analysis to understand normal network behavior as a baseline to easily pinpoint anomalous activity
- Superior forensic investigations with sophisticated security analytics
- Cisco NetFlow, Identity Services Engine (ISE) and TrustSec and the Cisco networking portfolio, to use the network as a security sensor and enforcer

DNS-Layer Network Security and Threat Intelligence

OpenDNS has the largest DNS service built for security. The OpenDNS global network processes 80+ billion Internet requests daily from 65 million users with 100% uptime. The OpenDNS Security Labs applies statistical models to this data to accurately identify, predict and prevent known and emergent threats. Every day 80+ million malicious requests are blocked and predictive intelligence is gained on 17+ million new domain names. Best of all: there is no hardware to install or software to maintain.

OpenDNS Umbrella

Cloud-delivered network security service protects any device, anywhere.

- A New Layer of Breach Protection: block malware, phishing, and command & control callbacks over any port or protocol–before threats reach you.
- Internet-Wide Visibility On & Off Your Network: in real-time, all Internet activity is logged and categorized by type of security threat, Web content, or cloud service.
- API-based Integration with Your Security Stack: in seconds, all malicious activity destined to the domains discovered by your existing systems are blocked.

OpenDNS Investigate

Provides threat intelligence on domains and IPs across the Internet.

- A Live Graph of Global & Historical Internet Activity: the most complete view of the relationships and evolution of Internet domains, IPs, and ASNs.
- Pivot Through Attackers' Infrastructures: use a dynamic search engine or RESTful API to mine diverse data sets and statistical models.
- Enrich Your SIEM Data and Speed Up Workflows: use global context and predictive intelligence to prioritize incident response and stay ahead of attacks

Web and Email Security

Cisco's Web and Email Security portfolio protects organizations from evolving email and web threats. Email and Web security are critical components of a holistic security strategy.

Cisco Email Security Appliance (ESA) and Cloud Email Security (CES)

- Fight spam, viruses, and blended threats for organizations of all sizes
- Enforce compliance and protect reputation and brand assets
- Available as cloud-based and hybrid (onsite appliance plus cloud) solutions

Web Security Appliance (WSA) and Cloud Web Security (CWS)

- Provides on and off network protection for https traffic along with granular usage controls, including application visibility and control
- Protect against advanced threats with Advanced Malware Protection (AMP) and Cognitive Threat Analytics (CTA)
- Flexible deployment, including on-premises and cloud delivered, leverages existing infrastructure and scales to fit
- Customized reporting offers actionable intelligence

Secure Access and Mobility

Enhance network visibility and control with identity-aware highly secure access solutions.

Cisco Identity Services Engine (ISE)

- Centralized and open solution that automates secure access to network resources on Cisco traditional, TrustSec, and multi-vendor networks.
- Includes BYOD, guest, and secure IoT access applications in addition policy and secure device administration (TACACS+).
- Ensures endpoint security compliance and enables open multivendor telemetry sharing and rapid threat containment to automatically stop unsafe endpoints.

Cisco TrustSec® Technology

- Simplifies network segmentation by automating firewall rules and access control list administration, using plain language policies, and defining security groups based on business roles, not IP addresses.
- Quickly isolates and contains threats to limit the impact of a breach
- Embedded in Cisco infrastructure. Supported on 40+ Cisco product families, including Cisco Catalyst® and Cisco Nexus switches, Cisco Integrated Services Routers, and Cisco ASA firewalls
- Open protocol technology, so it can be used in a multi-vendor network

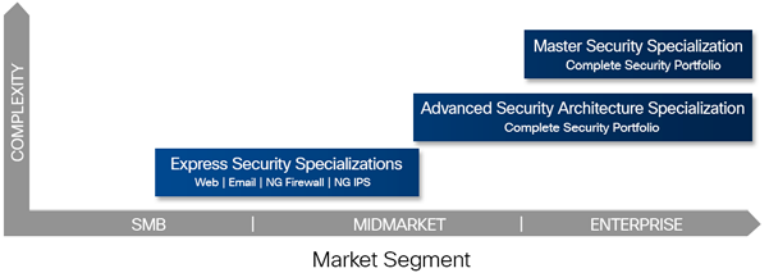
Cisco AnyConnect® Secure Mobility Solution

- Provides highly secure, simple, and reliable access anytime, anywhere, from any device
- Integrates with other Cisco Security Solutions like Cisco ISE, AMP for Endpoint, and Cisco CWS, to enable enterprise-wide risk protection
- Provides visibility into user and endpoint behavior both on and off premises with the Network Visibility Module.

For more information and security reports, visit **www.cisco.com/go/security**.

Security Architecture Specializations

Cisco has re-designed the Security Specialization program, aligning it to the new product portfolio.



Express Security Specialization – A new entry point into security specializations, allowing a partner to focus on one or several specific products (Email, Web, Next-Generation Firewall, IPS).

Advanced Security Architecture Specialization – This specialization covers the breadth of Cisco's Security Portfolio, and offers more advanced enablement for threat defense, secure access, Cloud and management solutions.

Master Security Architecture Specialization – This specialisation builds upon expertise attained in the Advanced Security Architecture Specialization and enables partners to deliver value-added security solutions to their customers.

Security Promotions & Incentives

Incentive Programs & Promotions are Cisco's commitment to Partner Profitability. Increase your revenue potential with upfront discount and backend payment programs, and special promotions that have been designed to help you sell Cisco security products and solutions.
www.cisco.com/go/promotions -> Filter Category "Security"

Marketing & Demand Generation

The free, ready-to-use marketing campaigns are designed to showcase your partnership with us, and help you effectively market Cisco security products and solutions to your customers.
www.ciscopartnermarketing.com/

Demoing Cisco Security Solutions

Cisco dCloud, the Cisco Demo Cloud, provides powerful self-service capabilities for Cisco Partners. From scripted, repeatable demonstrations to fully customized labs with complete administrative access, Cisco dCloud can work for you. **dcloud.cisco.com**

Partner Interactive Webinars

One-hour partner training webinars with sales or technical focus, delivered by Cisco Security Subject Matter Experts. Upcoming webinars and recorded sessions are available under **http://cs.co/SecurityPIW**. Receive a monthly invitation emailing by sending a "subscribe" message to **piw_enquiry@cisco.com**

Cisco Security Connections Partner Newsletter

This monthly publication is your one stop for all things Cisco Security. Subscribe to the newsletter to learn about the latest product updates, sales tools, trainings, and promotions.
https://info.sourcefire.com/SCNL_Partner-Subscription-Opt-In

For More Information

Cisco Security
cisco.com/go/security

Security Partner Community
https://communities.cisco.com/community/partner/security/emear

Cisco Security Blog
blogs.cisco.com/security

Partner Support
www.cisco.com/web/partners/support

Training & Certification
www.cisco.com/web/learning

Certification Tracking
cisco.pearsoncred.com

Marketing Assets Library
bx.cisco.com/cbx-portal

Competitive Information
www.cisco.com/web/partners/sell/competitive

Cisco Security Intelligence Operations
tools.cisco.com/security/center/home.x

Cisco Partner Marketing Central
http://www.ciscopartnermarketing.com/

OpenDNS Partner Portal
https://communities.cisco.com/docs/DOC-64565