Cisco Secure Data Center Solutions

Sales Accelerator

MAY 2015

Overview

Traditional security solutions are a bad fit for today's data center. They haven't kept pace with traffic volumes and features such as virtualization, multitenancy, and rapid service provisioning. Most data center security solutions monitor traffic flowing into and out of the data center, but Cisco estimates that over 75 percent of traffic flows between servers and devices inside the data center. And most data center administrators have no confidence that their firewalls or intrusion prevention system (IPS) solutions can keep up with performance requirements as data volumes spiral upward. Meanwhile, cybercriminals are becoming more adept at targeting both physical and virtual data center environments. Add to all that the growing incompatibility of new data center requirements with older security solutions leading to a preponderance of misconfigured security solutions.

Data center administrators need visibility and control over custom data center applications, not just the traditional web-based applications (Facebook, Twitter) and related microapplications that traditional Internet-edge security devices inspect. Data center environments are migrating from physical to virtual to next-generation software-defined networking (SDN), Cisco® Application Centric Infrastructure (ACI), and network functions virtualization (NFV) models. Security solutions must be able to scale dynamically and provide consistent protection that can work easily across these evolving and hybrid data center environments. A holistic, threat-centric approach to securing the data center – one that includes protection before, during, and after an attack – is needed to protect the modern data center and its specialized traffic (Figure 1). The Cisco Secure Data Center portfolio of solutions is the answer.

The portfolio includes the Cisco ASA 5585-X Adaptive Security Appliance, the Cisco FirePOWER™ next-generation IPS (NGIPS) appliance, the Cisco ASA with FirePOWER Services, the Cisco Adaptive Security Virtual Appliance (ASAv), Cisco FirePOWER vIPS, and Cisco Cyber Threat Defense solutions.

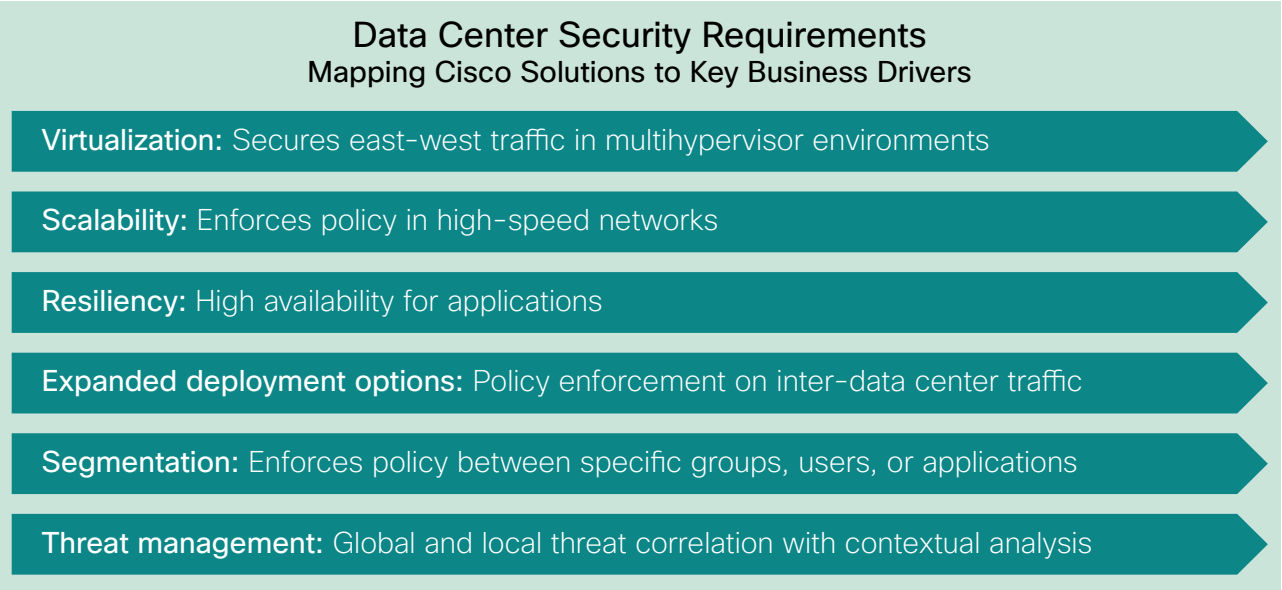
CONTINUED >

Overview

These are purpose-built, integrated solutions designed to protect the entire physical and virtualized data center. They comprise a suite of products and Cisco Validated Designs for systems-level solutions that promote secure data centers. The Cisco Secure Data Center delivers:

- Consistent security across physical, virtual, and cloud environments to help protect against network-borne threats, viruses, and malware.
- Support for traditional and next-generation SDN and Cisco ACI architectures to provide transparent policy enforcement and threat inspection across heterogeneous multisite environments.
- Dynamic provisioning, scalable performance, complete data center integration, patented clustering, and full threat protection to provide powerful protection across the entire attack continuum without compromising data center functionality, agility, or performance.

Purchasing Considerations for Data Center Security Sales Opportunities



Market and Industry Trends

Over the past few years, there has been an explosion in new, highly flexible data center architectures. Virtualization technology allows for dynamic scalability, on-demand resource reallocation, and specialized microsegmentation and multitenancy solutions, even across multiple data center locations.

Now SDN has completely reimagined how data centers are designed, deployed, and managed. New architectures based on SDN provide unprecedented performance, agility, and provisioning capabilities. Organizations have a variety of SDN solutions to choose from, including the open-source OpenStack project, VMware's NSX solution, and Cisco's groundbreaking ACI.

From a security standpoint, these new architectures create new vulnerabilities. Most security vendors do not provide a complete solution for these new architectures, requiring organizations to build completely new security infrastructures that are separate from their traditional data centers. And organizations are not replacing their old data center infrastructures in favor of these new ones. They exist side-by-side. So in addition to the obvious operational expenses and capital expenditures (OpEx and CapEx) associated with protecting a new environment, the creation of separate security silos within an organization for old and new infrastructures means that policies and protocols are inconsistently applied and enforced. The gaps between these security silos provide many opportunities for exploitation by attackers. Customers need a flexible data center security solution that protects their physical and virtual infrastructures today while helping to enable a secure migration to next-generation SDN or ACI data centers without losing comprehensive protection.

What Buyers and Influencers Care About

Target Buyer	What They Care About
Chief Information Officer (CIO)	· Maintaining competitive advantage through IT by delivering new services cost-effectively · Getting more out of the IT infrastructure within budget constraints · Reducing the complexity and cost of managing risk and ensuring compliance
Data Center IT Architect Data Center Network Engineer	· Having sufficient network bandwidth, scalability, and resiliency to support various computing needs · Meeting service-level agreements (SLAs) for network uptime, bandwidth, and latency · Complying with regulatory requirements to reduce risk to data center · Scaling the data center and network to meet the server or application team requirements within and across data centers
IT Manager or Director, Enterprise Architect	· Keeping up with planned and unplanned business growth · Handling the expected steep increase in data center traffic · Remediating outages and delayed response times

CONTINUED >

What Buyers and Influencers Care About

Target Buyer	What They Care About
Security IT Director Security Administrator	· Maintaining visibility and control across the extended network · Deploying new services with a high degree of security · Maintaining data security and integrity · Implementing and enforcing security policy · Meeting regulatory compliance requirements
Application Development Manager or Administrator	· Working with infrastructure peers to match application performance, stability, and resiliency with data center design and capacity · Having input into data center processes based on user needs

Positioning Statement

For Enterprise, midmarket, and service provider customers

Who are looking to address data center security priorities while maintaining the agility to meet ever-increasing business demands

The Cisco Secure Data Center Solution portfolio comprises purpose-built and validated solutions designed specifically for today's dynamic data center environments

That provides

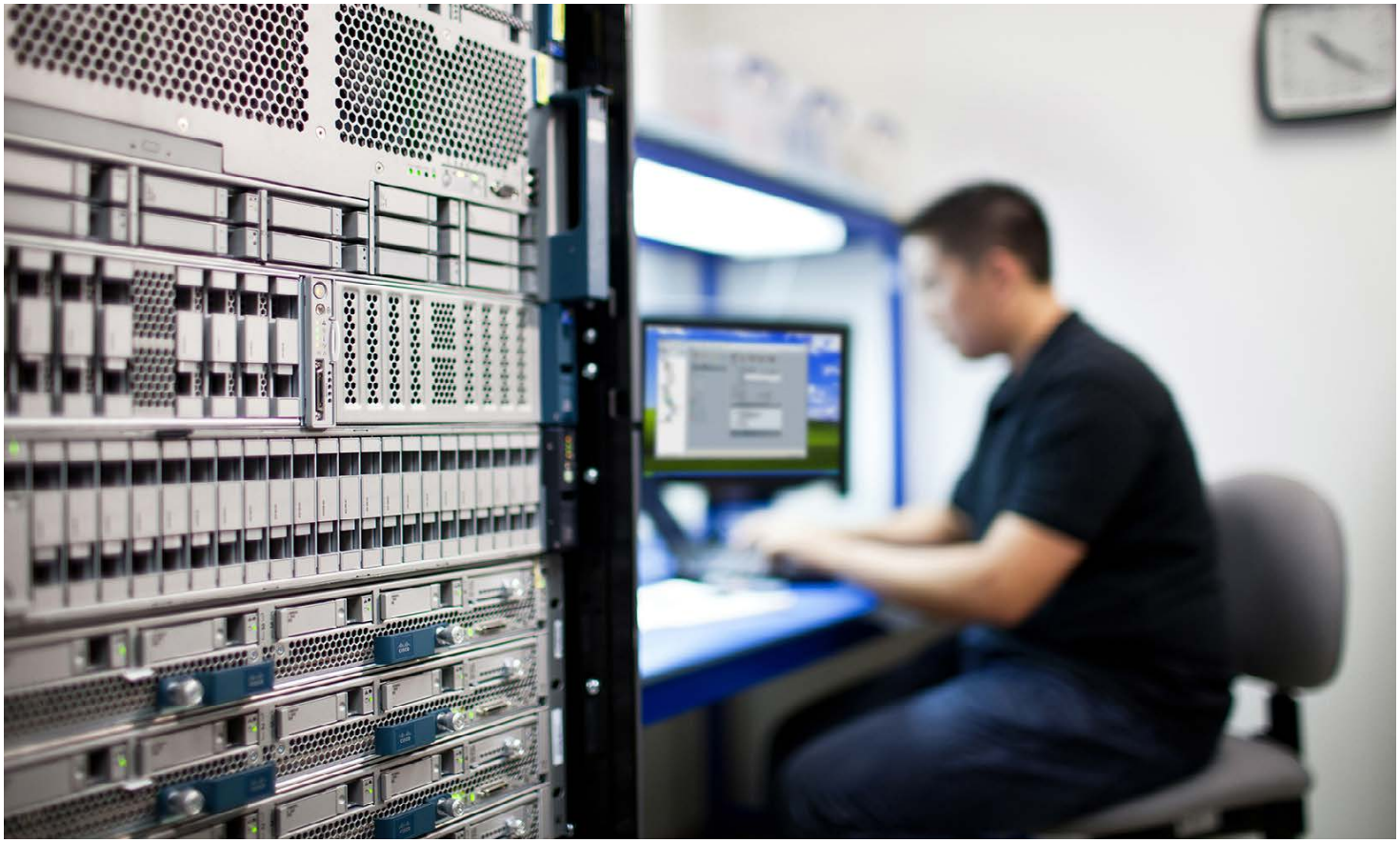
- Consistent security across physical, virtual, and cloud environments
- Support for traditional and next-generation SDN and ACI architectures
- Dynamic provisioning, scalable performance, complete data center integration, and full threat protection

Unlike competitive security products that were designed for the Internet edge and do not support unique data center requirements like full-flow asymmetric traffic, fully active redundant design, fault tolerance and resiliency, intersite clustering, and consistent policies across physical and virtual deployments

The Cisco Secure Data Center portfolio of solutions delivers business applications and services reliably and securely

Use Cases

Protect Business-Critical Data Located in the Data Center	Protect data center infrastructures and applications from advanced persistent threats (APTs) and other sophisticated attacks. Identify and protect against emerging attacks targeted at virtual devices deployed inside the data center.
Achieve and Maintain Compliance	Meet industry and regulatory compliance standards and regulations.



Elevator Pitch

No doubt you've seen the statistics on the rising incidence of data theft, malware, and other forms of cyberattacks. The news is full of companies and individuals suffering monetary losses, broken reputations, loss of confidence by customers, and lower valuations. Yet data centers are still full of legacy security solutions. Point solutions. Products that are not integrated. Meanwhile, you've been racing to keep up with new demands for network agility, rapid provisioning, and new application-oriented approaches to networking, so the infrastructure of your data center has probably changed dramatically in the past few years. Where and how do you begin to retool to fight the new war against advanced threats? Cisco continues to invest in security and our solutions with mulitple acquistions and talent. Our Secure Data Center portfolio of products is based on purpose-build solutions with Cisco Validated Designs for today's data centers, not yesterday's. Our powerful products provide:

- Consistent security across physical, virtual, and cloud environments to help protect against network-borne threats, viruses, and malware.
- Support for traditional and next-generation SDN and ACI architectures to provide transparent policy enforcement and threat inspection across heterogeneous multisite environments.
- Dynamic provisioning, scalable performance, complete data center integration, patented clustering, and full threat protection to provide powerful protection across the entire attack continuum without compromising data center functionality, agility, or performance.

Buyer Conversations

Challenge 1:

Protect your business-critical data in your data center.

How this affects you

You need to protect data center infrastructures and applications from advanced persistent threats (APTs) and other sophisticated attacks to maintain your company's competitive edge and keep it out of the headlines as the latest security breach victim.

What if you could...

Protect your data center from attacks using threat intelligence, passive OS fingerprinting, and reputation and contextual analysis.

With Cisco you can!

The Cisco Secure Data Center Solution detects and blocks internal and external threats at the data center edge as well as inside both physical and virtual data center zones.

Challenge 2:

Meet compliance regulations.

How this affects you

You have industry requirements and government regulatory controls that must be adhered to, or you risk penalties, fines, and lawsuits.

What if you could...

Help your business meet compliance requirements for physical, virtual, and next-generation data center infrastructures.

With Cisco you can!

Using the Cisco portfolio of Secure Data Center products, you can create an environment that helps your company meet compliance requirements for physical, virtual, and next-generation data center infrastructures. The portfolio of Cisco Validated Designs for Secure Data Centers provides step-by-step guidance designed to address a wide range of compliance standards and regulations.

Challenge 3:

Balance the performance demands of your business against the need for a secure data center.

How this affects you

The volume of traffic that needs to be inspected and safeguarded inside the data center is increasing at unprecedented speeds. Security cannot be a bottleneck for critical business processes.

What if you could...

Increase security without compromising performance using Cisco solutions.

With Cisco you can!

Cisco ASA and FirePOWER solutions with Cisco Nexus® switches uniquely support shared virtual PortChannels, Cisco FabricPath innovations, and equal-cost multipathing (ECMP) for better network integration. Your security is now operating at the speed of your data center.

Identifying and Qualifying Prospects

Look for companies that:

- Have an existing need for a data center upgrade. Upgrading the infrastructure is an optimal time for a refresh that takes advantage of the latest security advancements. Upgrades may include migrating from Cisco Catalyst® to Nexus switch platforms; upgrading the server infrastructure to the Cisco Unified Computing System™ (Cisco UCS®); or deploying a new data center.
- Are investigating new network architectures such as Cisco ACI or SDN.
- Have recently been the subject of a data breach or attack.
- Have made a recent investment in virtualization or cloud technologies.
- Are buying one of the Cisco UCS Integrated Infrastructures such as VCE Vblock Systems, VMware FlexPod, or the VersaStack solution.

Qualifiers and Conversation Starters

Starting the Conversation

1. What are you trying to do with your data center?
   - Map out plans, business objectives, and strategies.
2. What are the risks of doing those things?
   - Understand what systems are being connected. What data is being exposed? Is security complexity a risk?
3. How can we help you reduce those risks as much as possible?
   - This is Cisco's strength. See the data center as a system. An integrated, collaborative approach will always reduce risk more than any individual product.

Qualifying Questions

1. Are you looking for security solutions for your virtualized environment?
2. Are you interested in consistent security between physical, virtual, and cloud-based environments?
3. Are you concerned about regulatory requirements for virtual or cloud environments?
4. Would you like to dynamically add security policies whenever you provision data center resources?
5. Are security concerns holding you back from migrating to new data center environments, such as NFV, SDN, ACI, cloud, or Cisco Intercloud?
6. Are you interested in increasing application deployments without sacrificing security or creating performance bottlenecks?
7. Are you concerned about meeting your data center business priorities securely?
8. Would you like to simplify your data center security solution while lowering your TCO, especially across complex environments?

Potential Objections and Responses

Objection	Your Response
Security slows the speed of my data center, resulting in poor application performance	Get high performance with Cisco ASA's advanced clustering capabilities, dynamically scalable virtual solutions, and enhanced availability and resilience through shared virtual PortChannel and Cisco FabricPath innovations with Cisco Nexus 7000 Series Switches.
Security is too hard to provision. Deploying new services takes too long and lowers the efficiency of my data center	Deploy new, highly secure services in minutes or hours, not days or weeks. Take full advantage of the benefits of the Cisco ASA 5585-X Adaptive Security Appliance and security group tags to reduce manual firewall rules and security policy management.
Security is an extra cost to deal with	Cisco Secure Data Center solutions provide redundancy, resiliency, and high availability to prevent downtime caused by attacks and threats, or equipment or link failures, in order to lower the risk to businesses and their employees and data. This capability ultimately helps you reduce OpEx.
Security products just don't integrate into data center environments well	Cisco Secure Data Center solutions are designed to operate efficiently inside your complex data center environment. They natively support data center designs such as asymmetric traffic, the Link Aggregation Control Protocol (LACP), ECMP, and geographically dispersed data centers. In addition they move easily between physical, virtual, and cloud environments; support complex multihypervisor designs; and can safeguard traditional, SDN, and ACI architectures.
Most security vendors are not data center experts. They cannot provide best practices for the design and implementation of security in the data center	The Cisco Validated Design portfolio provides design and implementation guidance for organizations that want to deploy physical and virtualized workloads in their data centers. Cisco Validated Designs can provide exceptional protection to address today's advanced data security threats. The Secure Data Center validated design portfolio covers a number of interrelated solutions that can help security and system architects, network design engineers, advanced specialists, and customers.

What to Sell

Product, Solution, or Service Name	Short Description
Cisco ASA virtual firewall (ASAv)	Supports fabric-based deployments within ACI, SDN, and traditional Layer 2 and Layer 3 tiered data center deployments. The ASAv supports consistent, transparent security across physical, virtual, and cloud environments. This product would integrate well as part of a Cisco UCS sales opportunity.
Cisco ASA 5585-X Adaptive Security Appliance	Delivers superior scalability, performance, and security. Easily handling high traffic volumes, it helps organizations meet the increasing performance demands in today's data center environments. It can be deployed with the new Cisco FirePOWER NGIPS services blade, or side by side with the Cisco FirePOWER NGIPS appliances.
Cisco FirePOWER 8000 Series network security appliances	Provide multilayered threat protection and intrusion prevention at high inspection throughput rates, with a low cost of ownership. Gartner Magic Quadrant NGIPS leader.
Cisco virtual FirePOWER NGIPS	Provides the same control and protection as the physical Cisco FirePOWER 8000 Series, and helps you inspect traffic between virtual machines and combine and manage up to 25 physical and virtual appliances. This product would integrate well as part of a Cisco UCS sales opportunity.
Cisco Advanced Malware Protection (AMP)	Provides visibility and control to protect against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.

CONTINUED >

What to Sell

Product, Solution, or Service Name	Short Description
Cisco Identity Services Engine (ISE)	Provides highly secure access control with context. Cisco ISE delivers superior user and device visibility to support data center access control, and resource and workflow provisioning.
Cisco Cyber Threat Defense	Provides guidance for detecting threats already operating in an internal network or data center, providing deep and pervasive visibility. It helps security operators understand the how, what, when, and where of network traffic to identify suspicious and anomalous activities.

Case Studies

Company Name	Summary and Link to Full Case Study
Telindus	Cloud and telecom operator accelerates next-generation revenue streams using Cisco security. http://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/unified-computing/telindus_apr_2014_external_casestudy_fnl_04_11_13.pdf
Beachbody	Fitness company builds secure data center using Cisco UCS and Cisco security products. Customer deployment based on Cisco Validated Designs. http://www.cisco.com/c/en/us/products/security/beachbody-llc.html
Montana Economic Revitalization and Development Institute	MERDI boosts statewide business with Cisco multitenant next-generation firewalls. http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/case_study_c36_730874.pdf

Customer Quotes

"We are not serving one entity; we're supporting many different people and projects. That makes a huge difference in the kinds of network services we need and the demands we place on our hardware. The Cisco ASA 5585-X platform was the most capable solution for meeting our multitenancy and other project-related demands."

– Phillip J. Curtiss, *Chief Technology Officer, MERDI*

"We chose the 5585 because of clustering, virtualization, and pure throughput power within the virtualized environment. We like that we can virtualize the ASA itself to fit to our environment – and through that virtualization protect our development tier, our quality assurance tier, our application tier, all our different tiers."

– Bill Dugger, *Senior Network Engineer, Beachbody*

Competitors and Cisco Differentiators

	Checkpoint	Palo Alto Network	Fortinet
Offer	Network security, endpoint security, data security, and security management.	Its main offer is advanced firewalls. Believed to be first to market for next-generation application-aware firewalls.	Its main offer is a high-performance firewall.
GTM (go to market) and pricing	It focuses on global enterprise and service provider managed services markets through channel partners.	It focuses on enterprise customers. Strong presence in North America.	It focuses on North American enterprise market. Main business is through channel partners.
Strengths	Management, credibility among security administrators.	It sells on the strength of the firewall features. Heavily markets its application awareness and precise control of network activity based on application, user, and content identification.	Primarily known as a fast, high-performance firewall. But no ability to track an outbreak or mitigate a breach.
Weaknesses	Lack of data center scalability, performance, and resiliency. Data sheet claims don't match real work performances.	Mainly Internet edge application protection – not purpose built for the data center. Security weaknesses validated by third parties, including Network World, NSS Labs, Miercom.	No contextual awareness of the firewall solution. No VM traffic visibility or endpoint analysis for comprehensive threat protection.

CONTINUED >

Competitors and Cisco Differentiators

	Checkpoint	Palo Alto Network	Fortinet
Strategy	It positions itself as a best-in-class security vendor.	It positions its NGFW for everything.	Will heavily discount firewall features to win deals. Firewall is inexpensive but IPS is very expensive (2x Cisco cost with half the performance).
How We Win	Emphasize ASA performance and network integration features as better data center security option.	Emphasize Cisco's breadth and depth of product portfolio (best in class versus Palo Alto Networks' position of NGFW for everything). Lack of network integration features – hard to integrate with switches based on Cisco Nexus customer feedback.	Emphasize total security solution from Cisco that offers a holistic, threat-centric approach to securing the data center and its specialized traffic across the attack continuum – before, during, and after an attack.

Services for Partners

Service Name	Short Description
Cisco E-Consulting for Partners	Cisco E-Consulting for Partners is a powerful business intelligence platform that combines services metrics, product metrics, and Cisco experience to help partners manage, optimize, and transform their services and technology practices.
Cisco Express Security Specialization (ESS)	With Cisco ESS, partners can get their security business going faster. They can focus on business needs in four areas: email security, next-generation firewalls, web security, and intrusion prevention systems. Once they have completed the requirements of one or more focus area, they are positioned as a Cisco Express Security Specialized Partner.
Cisco Advanced Security Architecture Specialization	With the Cisco Advanced Security Architecture Specialization, partners access training to gain product expertise and learn how to integrate security across their portfolios. Partners are eligible for the following certifications: Premier, Silver, or Gold.
Cisco Master Security Specialization	The Cisco Master Security Specialization builds on the Advanced Security Specialization and demonstrates the highest level of expertise with Cisco security solutions.

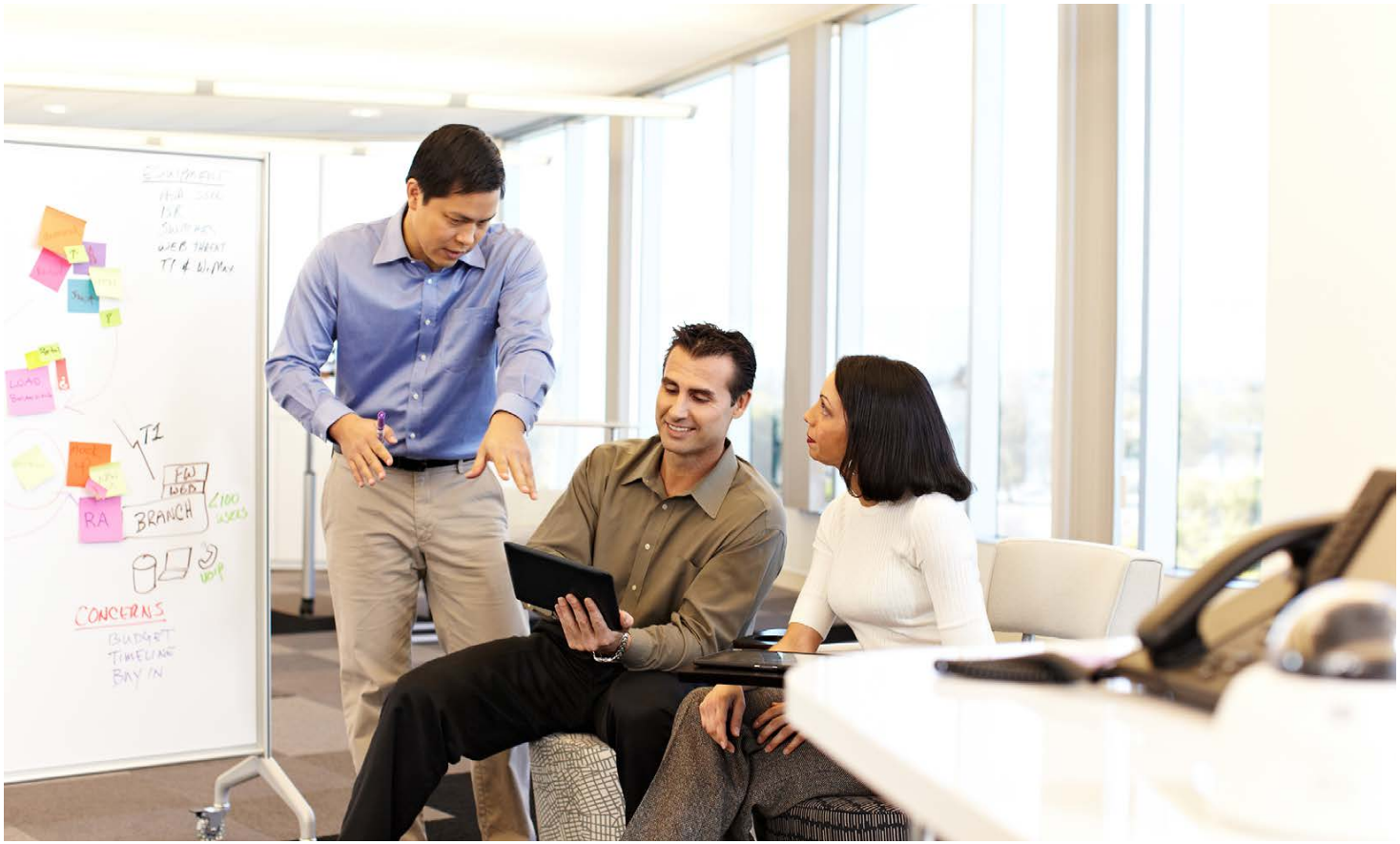
Partner Programs, Incentives, and Promotions

Name and Short Description	URL for More Information
Cisco Nexus 7000 Bundle and Cisco ASA 5585-X Bundle. Increase your deal size by 41 percent when you sell Cisco security as part of your data center deals.	http://www.cisco.com/web/partners/incentives_and_promotions/cisco_nexus.html
Earn Discounts on New Security Business (available through July 25, 2015). Through Security Ignite, partners get additional upfront discounts on new next-generation security business registered through the Opportunity Incentive Program (OIP) or Teaming Incentive Program (TIP).	http://www.cisco.com/web/partners/incentives_and_promotions/security-ignite.html
Cisco FirePOWER Migration (available through July 31, 2015). Receive trade-in credits when migrating to Cisco FirePOWER security products through the Technology Migration Program.	http://www.cisco.com/web/partners/incentives_and_promotions/firepower-migration.html
Data Center Nexus Promotions, Ongoing. Our "bundle and save" promotions and technology refresh credits create an irresistible value proposition for customers to migrate to or upgrade their Cisco Nexus products.	http://www.cisco.com/web/partners/downloads/partner/WWChannels/promotions/download/nexus_promo_details.pdf
Unified Access Cyber Threat Defense Bundles (available through July 25, 2015). Get Lancope StealthWatch at a 36 percent discount by purchasing Catalyst® switch promotional bundles.	http://www.cisco.com/web/partners/incentives_and_promotions/cyber-threat.html
Cisco Incentives and Promotions site	http://www.cisco.com/web/partners/incentives_and_promotions/index.html

Cisco Sales Resources

Selling and Technical Resources

- Secure Data Center Incentive. This program provides incentives for data center teams to include architectural designs and security in data center switching sales.
- Selling Security IWE Site
- Data Center Security Portal
- Selling Data Center IWE Site



Where to Send Customers for More Information

Resource

- Cisco Security Main Product Page
- Cisco Secure Data Center Solution Page
- Design Zone for Cisco Secure Data Center Portfolio
- Cisco ACI Security Solution Page

Glossary

Term	Definition
SDN	Software-defined networking (SDN) is an architecture purporting to be dynamic, manageable, cost-effective, and adaptable, seeking to be suitable for the high-bandwidth, dynamic nature of today's applications. SDN architectures decouple network control and forwarding functions, so network control becomes directly programmable and the underlying infrastructure can be abstracted from applications and network services. (Source: Wikipedia)
Cisco ACI	Cisco Application Centric Infrastructure (ACI) in the data center is a holistic architecture with centralized automation and policy-driven application profiles. It delivers software flexibility with the scalability of hardware performance. Cisco ACI is our implementation of the fundamentals of SDN.

Contacts

Resource	Contact Info
asa-pm@cisco.com	For product questions (features, roadmap) for the Cisco ASA 5585-X, the ASA 5500-X Series product, and ASAv.
asa-tme@cisco.com	For technical questions (deployment, installation) for the Cisco ASA 5585-X, the ASA 5500-X Series products, and ASAv.
ask-firepower-pm@cisco.com	For technical and product questions about Cisco FirePOWER appliances and FirePOWER services on the ASA security appliance product family.
positron-pm@cisco.com	For Cisco Identity Services Engine product questions.
cyber-pm@cisco.com	For Cisco Cyber Threat Defense product questions.
ask-amp-pm@cisco.com	For technical and product questions about Cisco Advanced Malware Protection.