At-a-Glance

Benefits

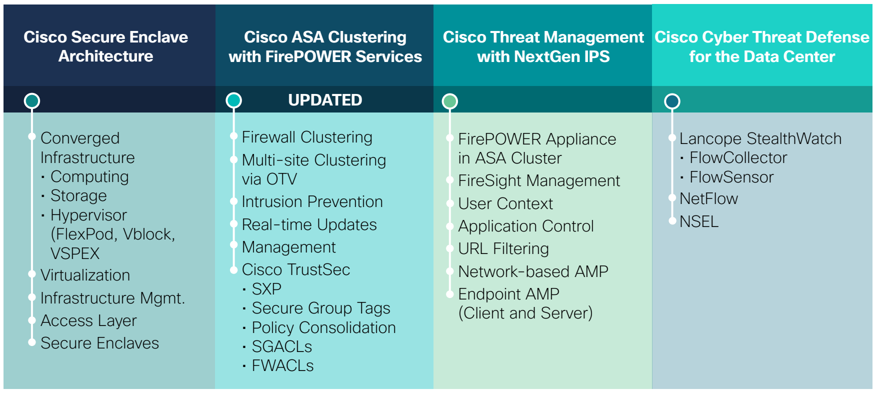
- Speed security solution deployment, reduce risk, and accelerate business objectives with a choice of four interrelated Cisco Validated Designs for security that provide detailed design and implementation guidance.
- Protect the application environment and data center fabric and network services, establish a threat management system, and detect threats already there.
- Secure your data center assets, endpoints, mobile devices, virtual machines, and cloud before, during, and after attacks occur.

Cisco Secure Data Center for the Enterprise Solution Portfolio

Today's data centers store vast quantities of sensitive, business-critical information. They must constantly evolve to meet the needs and expectations of the enterprise while complying with increasingly stringent security regulations, which include supporting new infrastructures such as cloud and virtual resources and bring-your-own-device (BYOD) initiatives.

At the same time, data centers operate in an unpredictable threat landscape. Hacking has become a lucrative industry, targeting business-critical information housed in data centers. For security teams, a simplified and comprehensive strategy that addresses business demands and defends the data center is a necessity. Cisco can help you with a threat-centric approach to your security needs.

Figure 1. Cisco Secure Data Center for the Enterprise Solution Portfolio



Cisco Secure Enclave Architecture	Cisco ASA Clustering with FirePOWER Services	Cisco Threat Management with NextGen IPS	Cisco Cyber Threat Defense for the Data Center
	UPDATED		
Converged Infrastructure · Computing · Storage · Hypervisor (FlexPod, Vblock, VSPEX Virtualization Infrastructure Mgmt. Access Layer Secure Enclaves	Firewall Clustering Multi-site Clustering via OTV Intrusion Prevention Real-time Updates Management Cisco TrustSec · SXP · Secure Group Tags · Policy Consolidation · SGACLs · FWACLs	FirePOWER Appliance in ASA Cluster FireSight Management User Context Application Control URL Filtering Network-based AMP Endpoint AMP (Client and Server)	Lancope StealthWatch · FlowCollector · FlowSensor NetFlow NSEL

Comprehensive, Validated Data Center Security Solutions

The Cisco® Secure Data Center for the Enterprise Solution portfolio for the enterprise features four interrelated Cisco Validated Designs. These are verified, lab-tested architectural designs that provide detailed design and implementation guidance to speed deployment, reduce risk, and accelerate business objectives. They include:

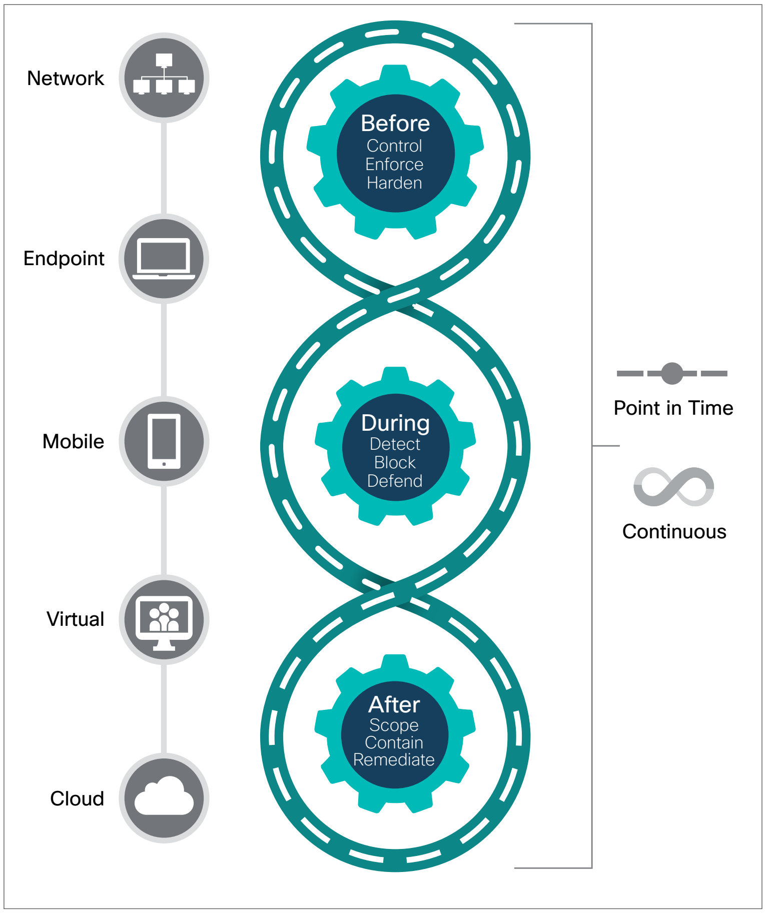
Cisco Secure Enclave Architecture: With this design you can create a more flexible, functional, and secure application environment within the data center. This design provides a uniform foundation that can help protect against compromise while delivering a simplified, standardized, and trusted approach for the management of shared resources.

A New, Threat-Centric Model

The Cisco approach recognizes the need to protect against advanced threats while reducing complexity and supporting the addition of new data center services. This new model provides protection across the full attack continuum. It looks at security not at a single point in time but as a continuous cycle, focusing on actions that occur before, during, and after an attack across the extended network, including data center assets, endpoints, mobile devices, virtual machines, and the cloud.

Cisco has mapped data center functions into the provision of security across the full attack continuum. The Threat Management System Capabilities Matrix outlines the most common security capabilities and descriptions across the continuum along with associated products. This information helps organizations integrate their threat defenses and identify possible gaps.

Figure 2. Attack Continuum



Cisco ASA Clustering with FirePOWER™ Services: This design – now updated for multi-site clustering – brings application awareness and data protection to the data center fabric and network services. Application security and delivery are key operational fundamentals in the data center; however, managing policies for application workloads has created a significant operational challenge. This solution takes a new approach by mapping users to data center assets in a way that provides consistency, simplification, and scalability, plus advanced threat protection across the fabric.

Cisco Threat Management with NextGen IPS: This design provides a comprehensive set of capabilities for a threat management system. Taking a unique approach, it examines how attackers approach data centers and illustrates how customers can integrate Cisco FirePOWER appliances into their architectures to defend against advanced threats.

Cisco Cyber Threat Defense for the Data Center: This design helps you understand how to detect threats already operating in an internal network or data center. The solution uses network telemetry to provide deep and pervasive visibility across the data center to help security operations teams understand the how, what, when, and where of network traffic to identify suspicious and anomalous activities.

Next Steps

Visit www.cisco.com/go/designzonesecuredc for more information, including the Cisco Secure Data Center for the Enterprise Solution portfolio for the enterprise design and implementation guides.

Figure 3. Threat Management System Capabilities Matrix

	Threat Containment and Remediation	Access Control and Segmentation	Identity Management	Application Visibility and Control	Logging and Traceability Management
Description	File-, packet-, and flowbased inspection and analysis for threats	Access control policies, segmentation, secure separation	User identity and access posturing, network-based user context	File control and trajectory, network file trajectory, application quarantine	Threat forensics and compliance
Before	Endpoint protection agents, network-based flow protection	Endpoint group assignments, security zones, user-to-asset access policies	User mapping to groups, resources, and acceptable access locations	Policies to limit and control internal and external client and web applications, including app versions	Proper configuration of threat management system reporting
During	Cloud-based endpoint file analysis, network-based file analysis, network-based flow analysis, signature-based analysis, sandbox analysis	Fabric enforcement, firewall policy enforcements, connection validation and protocol compliance	User context analysis	Enforcement of application control policies	Active out-of-band logging
After	Connections and flows analysis and remediation	Policy enforcement and logging	User access and threat origination analysis and remediation	Visibility into all applications being accessed and running on network	Immediate access by proper threat function management platform; Consolidation of logs into central repository for further forensics and compliance
Products	FirePOWER with FireSIGHT, Intrusion Protection, network-based AMP, email AMP, CWS AMP, FireAMP for end user and mobile	ASA 5585-X, SGTs, SGACLs, SXP, and TrustSec-capable switching fabric or ACI Fabric with ASAv	Cisco ISE, FirePOWER with FireSIGHT	FirePOWER Access Control, FirePOWER NGFW	FireSIGHT Management Center for short-term logs, Lancope StealthWatch for longer-term NetFlow analysis logs, SIEM for log management compliance