Cisco Cloud Security Solutions

EFFICIENT, SECURE, RESILIENT, AGILE, SIMPLE, AND SCALABLE REFERENCE DESIGNS FOR YOUR DATA CENTER

Introduction

Data centers are undergoing rapid changes. But whether organizations are adopting virtualization or considering a software-defined networking (SDN), Cisco® Application Centric Infrastructure (ACI), or Cisco Intercloud Fabric environment, security is a top concern. With the sophistication and complexity of cyber-attacks on the rise, effectively preventing, detecting, and responding to advanced persistent threats and other potential security breaches is among the greatest challenges that organizations today must address. To securely adopt new data center solutions and strategies, organizations require a holistic security approach that spans the distributed data center environment and takes into account the cloud lifecycle, and that is capable of stopping real-world threats at every stage of an attack: before, during, and after.

To address these concerns, Cisco has developed the first in a series of cloud security architectures designed to provide practical, validated solutions to meet the growing challenges of security and compliance. These validated designs greatly reduce deployment risks while simplifying the planning, design, and implementation processes, thereby saving your organization significant time, money, and resources. In addition, we've partnered with third parties to validate these designs as they relate to requirements such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), and Federal Information Security Management Act (FISMA) compliance.

Cisco's cloud security validated design strengthens security in the cloud by:

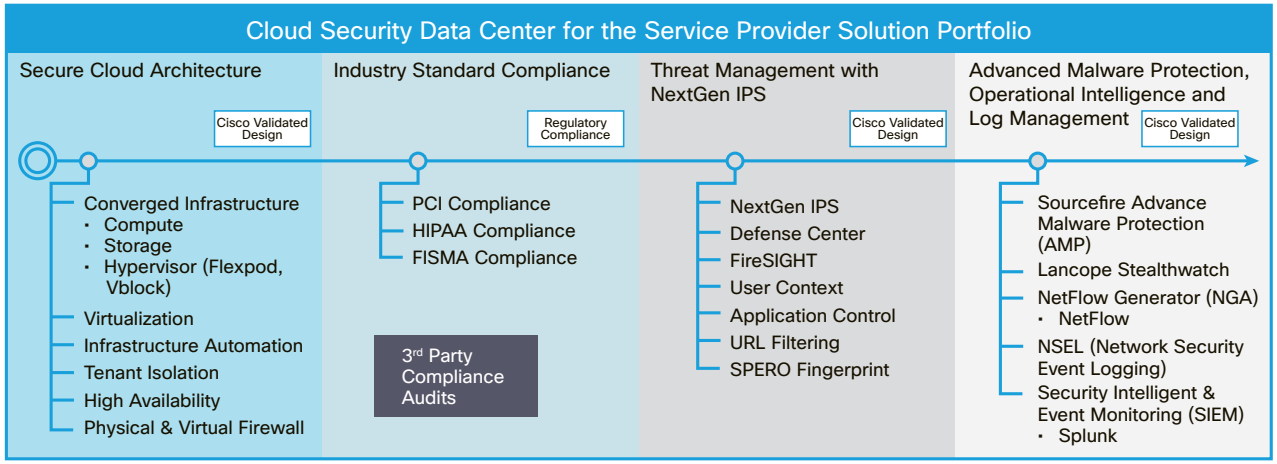
- Providing validated guidance for meeting FISMA, HIPAA, and PCI security regulatory requirements
- Providing tools to implement effective cyber threat management
- Detecting, analyzing, and stopping advanced malware, advanced persistent threats, and targeted attacks across the entire threat continuum: before, during, and after an attack
- Tracking and analyzing network behavior
- Actively monitoring traffic in all directions – east and west and north and south – including asymmetric traffic
- Collecting logs from network and storage devices in a centralized location for forensic investigation
- Supporting solutions from leading third-party technology partners for a robust cloud ecosystem
- Consistently enforcing policies across networks and accelerating threat detection and response
- Accessing Cisco's vast global intelligence in combination with relevant contextual information to make informed decisions and take fast, appropriate actions
- Supporting secure access controls to prevent business and data loss
- Securing data center services using application and content security

Cisco Cloud Security Solution Portfolio

The Cisco Virtualized Multiservice Data Center (VMDC) Cloud Security solution protects cloud environments with cloud security strategies and a comprehensive portfolio of solutions that span the cloud lifecycle and all security domains for cloud service providers and enterprise customers (Figure 1). It offers:

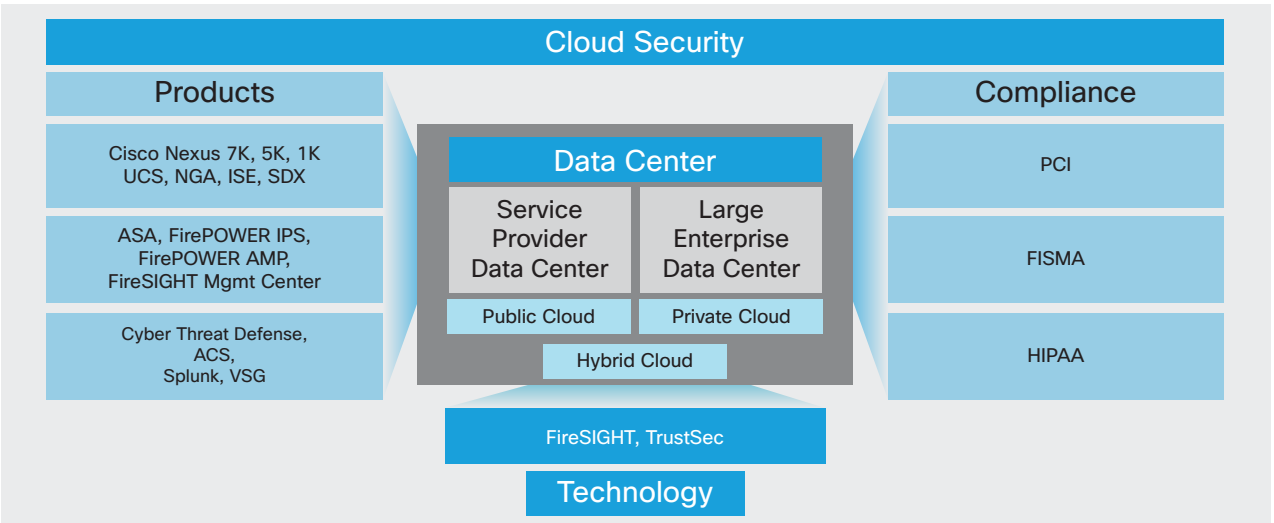
- A detailed design guide and step-by-step implementation guide to reduce time to deployment
- Design guidance and validation of critical Cisco and selected security elements from third-party technology partners in a cohesive Cisco VMDC framework; this design incorporates the Cisco FirePOWER intrusion prevention system (IPS), Cisco Cyber Security and Threat Defense, Cisco NetFlow generator, and security information and event management (SEIM) for intelligent log monitoring using Splunk
- Independent third-party (SecureState) assessment and gap analysis of industry-standard compliance frameworks (PCI, FISMA, and HIPAA) to facilitate regulatory compliance
- An operational framework that reduces deployment overhead and time to market, mitigates risk, and helps ensure end-to-end security of the cloud by providing policies, procedures, and best practices in multiservice cloud data center deployments

Figure 1. Cisco Cloud Security Solution Portfolio



Cisco Cloud Security Architecture

The simplified Cisco VMDC cloud security architecture design reduces deployment risks because we've validated and tested our design with various Cisco products and the products of third-party technology partners, These technologies and compliance mechanisms then enable service providers to deploy public and private clouds securely on a multitenant Cisco VMDC architecture (Figure 2).



Cisco Cloud Security Solution Benefits

The Cisco VMDC security solution incorporates a wide range of innovative Cisco cloud products integrated into a Cisco Validated Design. This validated, best practices security solution provides compelling benefits to public and private cloud providers in multiple ways:

- **Breadth:** The Cisco Cloud Security solution provides a comprehensive security solution across a distributed cloud environment that addresses the entire attack continuum:
  - Before an attack by providing safeguards and defenses against real-world threats, including access to Cisco's comprehensive global threat telemetry database
  - During an attack by providing continuous assessment and policy enforcement to identify and respond to malware and other attacks that have penetrated your perimeter defenses
  - After an attack through forensic analysis and retrospective security that identifies where an attack originated, what resources have been touched, and what steps need to be taken for effective and thorough remediation
- **Compliance:** The Cisco Cloud Security solution provides baseline guidance to help public and private cloud providers achieve regulatory compliance. This guidance reduces the complexity of operations required to achieve compliance with regulatory standards such as PCI, HIPAA, and FISMA.
- **Reduced operating costs:** Validated designs greatly reduce deployment risks and simplify the planning, design, and implementation processes, saving your business significant time, money, and resources.
- **Network visibility and threat detection:** Cisco Cloud Security is designed to proactively detect real-world threats running on an internal network.

- **Real-time operation intelligence with event monitoring and logging:** Cisco Cloud Security provides the capability to monitor, search, analyze, visualize, and act on the massive streams of data generated by the network and security appliances. Cloud providers can monitor IT systems and infrastructure in real time to identify issues, problems, and attacks before they affect customers, services, and revenue.
- **Faster deployment of secure data centers:** Cisco Cloud Security provides cohesive, end-to-end validation of multiple security devices to reduce implementation complexity and enable public cloud providers to improve the time to market for offered services.
- As Cisco continues to evolve, the architectural features of the cloud security system are **applicable to both existing Cisco VMDC and next-generation Intercloud solutions.**

Why Cisco?

Cisco knows data centers and the cloud better than anyone. More organizations rely on Cisco solutions to run, manage, and secure their data center and cloud environments than on the solutions of any other vendor. Cisco meets the security challenges faced by today's extended networks, including the latest zero-day advanced threats, by offering best-in-class security - whenever and however you need it - to provide continuous protection across the entire attack continuum. The Cisco Cloud Security designs and solutions provide validated end-to-end data center security, including security for both the virtual and physical infrastructure, helping ensure high availability and performance with no bottlenecks at any component level. The Cisco Cloud Security solution helps public and private cloud providers reduce the cost of compliance with various industry regulations by providing comprehensive guidance and gap analysis. These analysis helps organizations achieve PCI, HIPAA, and FISMA compliance using a Cisco reference architecture deployment model.

For More Information

See the Cisco security design guide: www.cisco.com/go/vmdc.

C45-732792-00 09/14