At-a-Glance

Benefits

- Enforce consistent security policies
- Simplify security policy management
- Take advantage of next-generation firewall capabilities
- Lower the financial and resource burden of maintaining security

Cisco Defense Orchestrator

Strengthen Your Security Posture with Simplified Policy Management

Comprehensive defense requires multilayer security. But adding security tools makes it harder for network operations to stay on top of security policy, especially for organizations with geographically dispersed locations.

Managing policies across distributed security devices is complex and time consuming, and inconsistencies and gaps are almost inevitable. This creates enormous risks: security device misconfiguration is one of the most common reasons for security breaches.

That's why you need Cisco® Defense Orchestrator, a cloud-based management application that takes the hassle out of policy management across Cisco security devices, including the Cisco Adaptive Security Appliance (ASA), Cisco Adaptive Security Virtual Appliance, Cisco ASA with FirePOWER™ Services, Firepower Next-Generation Firewalls (NGFW), and OpenDNS.

An Easier Way to Defend Business-Critical Information

Cisco Defense Orchestrator provides network operations staff with a simple, consistent way to create and maintain security policies while reducing management complexity and costs. Setup is easy, fast, and friction-free, and, since it's a cloud solution, Defense Orchestrator requires no new capital expenditures, floor space, or application management.

With Defense Orchestrator, you can:

Enforce consistent security

Find policy anomalies with end-to-end analysis and accelerate issue resolution by auditing policies across devices. Clean up policies and easily deploy the right policies to new devices with templates that provide consistent policy application. Monitor policy changes by getting automatic notifications when an out-of-band change occurs.

Simplify security policy management

Set up, apply, and manage rules across disparate devices from a single place, streamlining ongoing policy-change management for both planned and unplanned changes. Optimize policies more easily. Reduce risks by responding to threats faster and modeling the impact of changes before deployment. Extend security policy to the cloud with confidence.

Take advantage of application-layer capabilities

Implement advanced security using next-generation firewall (NGFW) and application protection from FirePOWER Services and Firepower Threat Defense without needing to be deeply familiar with each managed product. Defend both on-premises and remote employees against a greater range of attacks.

Defense Orchestrator allows you to:

- **Analyze:** Operate from a single pane of glass for end-to-end security policy configuration across devices. Analyze security configuration to spot misconfigurations and manage planned or unplanned changes in security policies and objects. Make use of end-to-end policy analysis without the support of an expert in device-by-device security configuration.
- **Model:** Create a standardized policy template that supports the consistent enforcement of security configurations with ease to meet business growth. Model the impact of changes before deploying to devices.
- **Remediate:** Verify that the right changes were applied to devices. Gain confidence that the right changes were deployed in real time or offline per the change-management process. Enforce and maintain a consistent security posture across all security products managed by Defense Orchestrator.
- **Visualize:** Determine the effectiveness of web policy enforcement by seeing aggregated information about top applications, destinations, categories, attacks, and risks.

Learn More

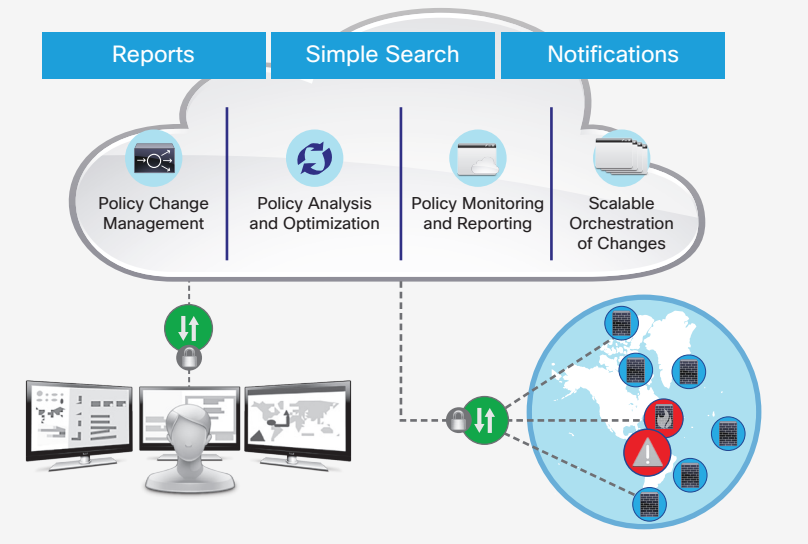
Cisco has more than a decade of experience in security technology and the industry's largest security database. This solution demonstrates our commitment to integrate our portfolio of multiple platforms, including Cisco ASA, ASA with FirePOWER Services, Firepower NGFW, and OpenDNS Umbrella.

Discover more about Cisco Defense Orchestrator at cisco.com/go/cdo.

To experience firsthand how Defense Orchestrator can help you, contact cdosales@cisco.com to get started.

Lower the financial and resource burden of maintaining security
Manage from anywhere with a highly secure, highly reliable, always available, scalable multitenant cloud solution. Free up capacity for other priorities by strengthening and maintaining security posture in less time and with fewer resources.

Figure 1. Main features of Cisco Defense Orchestrator



Feature	What You Can Do
Device onboarding	Use multiple highly secure ways to connect to managed devices, whether online or offline
Object and policy analysis	Uncover and remediate issues such as duplicate or unused policies, inconsistent rules, or inconsistent network objects at the policy and object level across devices
Application, URL, malware, and threat policy analysis	Manage Layer 7 protection through traffic blocking by application or destination hostname
Security templates	Design & manage templates for easy deployment of new devices
Simple search	See how policies are enforced across device types by searching for any object name, ACL name, network, or application policy element
Change impact modeling	Determine the impact of policy changes before deployment by applying changes in a nonproduction environment
Out-of-band notifications	Receive automatic notifications when policy changes occur
Reports	Track policy effectiveness with reports on top applications, destinations, categories, attacks, and risks

Cisco Defense Orchestrator in Action

A national retail company needed a better way to apply a consistent policy structure across several thousand retail branches nationwide without backhauling through corporate operations.

The firm wanted to transition to next-generation capabilities in order to improve end-to-end visibility and control. Through a simple management process, it created a template to cover ports and applications across the network.

C45-736943-00 06/16