Cisco Defense Orchestrator

Cisco® Defense Orchestrator is a cloud-based security policy management product that helps network operations establish and maintain a security posture by managing security policies across Cisco security devices. It is an always available, highly reliable, highly scalable, multi-tenant cloud platform.

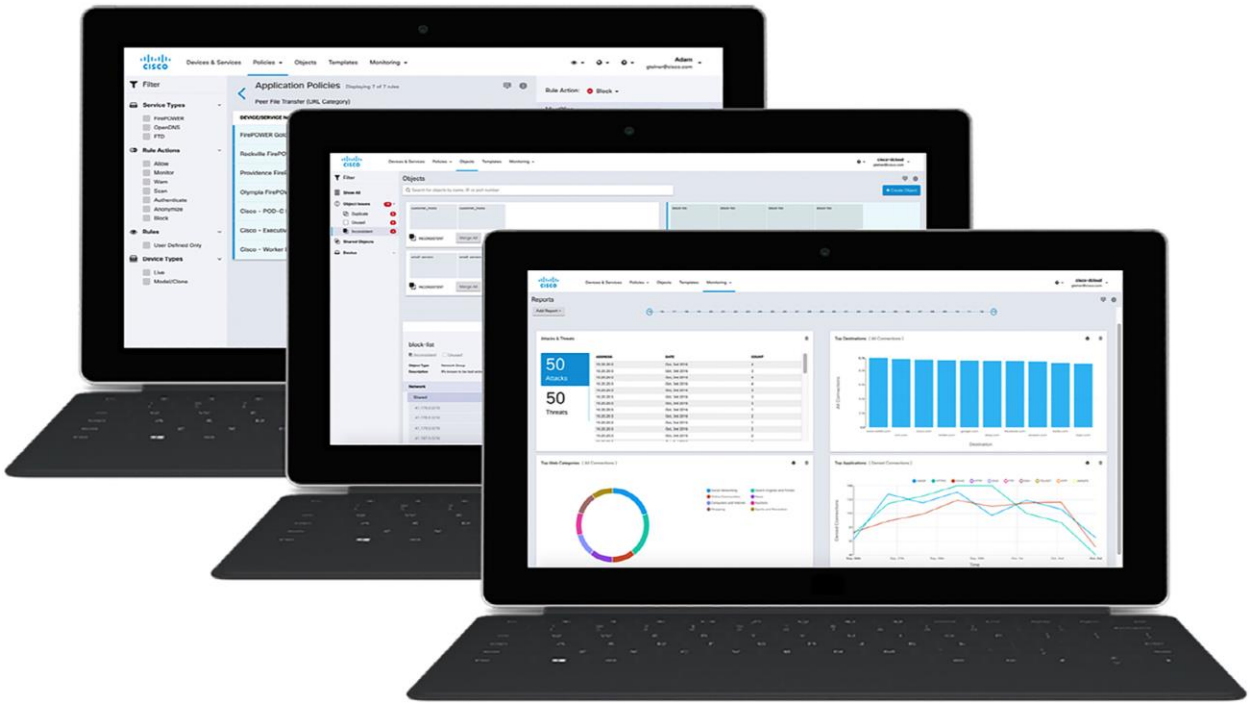
Product overview

The Defense Orchestrator analyzes security policy configurations for Cisco Adaptive Security Appliances (ASA), Cisco Adaptive Security Virtual Appliances, Cisco ASA with FirePOWER™ Services, Cisco Web Security Appliance (WSA), and Cisco Umbrella. It identifies and resolves policy inconsistencies, models policy changes to validate their impact, and orchestrates policy changes to achieve consistency and maintain clarity in your security posture.

The Defense Orchestrator is a cloud-based platform. It reduces the setup time, moves the cost from capital expenditures to operating expenses, and reduces day-to-day operational challenges. It provides a simple, consistent, and highly secure way of enforcing security policies, thus reducing costs and quickly delivering value in your security enforcement.

Figure 1 shows the easy-to-comprehend interfaces of the orchestrator.

Figure 1. Screens showing application protection policies, objects, and visibility with top-N reports



Security posture consistency

The task of managing security is complex. The ability to respond to threats is predicated on well-designed and well-established defenses in individual products and services. Recent threats have demonstrated that an analysis of network security must involve a variety of factors,

including security policies. A continuous analysis, design, and implementation program is essential for maintaining an acceptable security posture.

The Defense Orchestrator analyzes the security configuration to spot misconfigurations in security policies and objects. It helps network operations manage planned or unplanned changes, model the impact of changes before deploying them, and verifies that the correct changes are applied to the devices. It analyzes security policies to identify anomalies in the security policy configuration across multiple devices. This analysis highlights inconsistent rules that may need remediation. Customers can remediate issues at the policy and object level. With gold policy configurations, customers with many locations (stores, hotels, or offices, for example) can be confident that the correct policy configuration is being applied to their security devices and services.

End-to-End policy management

The Defense Orchestrator offers a single pane of glass for security policy configuration across devices and device types. It abstracts network objects, applications, application categories, URLs, URL categories, and actions to help ensure that managing policies across disparate devices is consistent and easy. Administrators can now design and enforce a consistent global security posture for employees that are on premises or remote and can respond to threats quickly. This ability also reduces the need for an in-depth knowledge of each security product and its configuration.

Quick time to value

The Defense Orchestrator is a cloud-based platform that is easy to set up and quick to configure. There is no need for additional capital expenditures, floor space, or application management. The orchestrator manages on-premises or cloud service Cisco security products in no time through direct connection or an offline upload of the configuration. Enforcing security policies in this simple, consistent, and highly secure way reduces day-to-day operational challenges. You gain value quickly for your security enforcement.

Features and benefits

Managing security policy with the Defense Orchestrator provides a number of benefits.

Easy onboarding: You can onboard on-premises or cloud service Cisco security products in no time into the Defense Orchestrator. Either connect directly to the device or upload the configuration offline. Communication between devices and Orchestrator is always highly secure.

End-to-end policy analysis: The Defense Orchestrator offers a single pane of glass for your security policy configuration across devices, even across physical and cloud infrastructure. It can spot misconfigurations and manage planned or unplanned changes in security policies and objects. The end-to-end policy analysis reduces the need to be an expert in device-by-device security configuration.

Modeling: The Defense Orchestrator helps customers create a clean, or "gold," policy template. You can enforce a consistent security configuration with ease to meet business growth. And you can model the impact of any changes before deploying the configuration to your devices.

Remediation: As configuration changes are modeled, customers can confirm that the correct changes are applied to the devices. You'll have confidence that the changes will be deployed in real time or offline in accordance with your change-management process. A consistent security posture can be enforced and maintained across all security products managed by the Defense Orchestrator.

Visualization: The Defense Orchestrator helps you visualize aggregated information about top applications, top destinations, top categories, top attacks, and top risks to determine the effectiveness of web policy enforcement.

Table 1 highlights the best-in-class features and benefits of the Defense Orchestrator.

Table 1. Features and benefits

Feature	Benefit
Management of Cisco security products	Central security policy management of the Cisco security environment, including: • Cisco ASA 5500 Series and 5500-X Series Adaptive Security Appliances • Cisco ASA with FirePOWER Services • Cisco Firepower 4100 series and Cisco Firepower 9300 running ASA software image • Cisco Umbrella • Cisco Web Security Appliance (version 11 and forward)
Cloud platform	Easy setup and quick configuration. No need for additional capital expenditures, floor space, or application management.
Quick on-boarding	Streamlined configuration and simple initial security management setup. Device information can be imported from the configuration file or discovered from the device itself.
Highly secure connectivity	Constant protection of all data transactions through a highly secure communication between device and Defense Orchestrator.
Object and policy analysis	Ability to spot misconfigurations across multiple devices to help manage planned and unplanned changes. A single pane of glass is used for end-to-end policy configuration.
Templates	Consistent security enforcement with clean, or "gold," policy configuration. Customers with many distributed locations (stores, hotels, or offices, for example) can be confident that the correct policy configuration is being applied to their security devices and services.
Deployment of changes according to a set process	Ability to model changes, see the impact of the changes, export or write changes to devices per a change-management process.
Out-of-band detection and notification	Ability to maintain a consistent security posture by getting notified when an out-of-band change happens.
Simple search	Ability to search for any object name, ACL name, network, or application policy element to find how policies are enforced across devices and device types.
Global enforcement of application security	Ability to design and enforce a consistent global security posture for employees that are on-premises or remote. Ability to respond to threats quickly. Google-like search function helps in quickly displaying application protection enforcement across devices and device types.
Reports	Easy-to-visualize aggregated information about top applications, top destinations, top categories, top attacks, and top risks to determine the effectiveness of web policy enforcement.

Platform support matrix

The Defense Orchestrator manages security policies for ASA, ASA with FirePOWER Services, when running ASA software image, Web Security Appliance, and Umbrella.

The ASA with FirePOWER Services policy management includes ASA firewalling, application visibility and control, URL filtering, Next-Generation Intrusion Prevention System (NGIPS), and Cisco Advanced Malware Protection (AMP). Table 2 below outlines the Cisco ASA, Cisco ASA with FirePOWER Services software support matrix.

Table 2. Cisco ASA, ASA with FirePOWER Service, support for the defense orchestrator

Product	ASA Software Version	FirePOWER Services on ASA Software Version
ASA 5505, 5510, 5520, 5540, 5550	8.4 and later	NA
ASAv	9.2.2 and later	NA
ASA 5506-X, ASA 5508-X, ASA 5516-X	9.2.2 and later	5.4.1 or later
ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X	9.2.2 and later	6.0.0 or later
ASA 5585-10, 5585-20, 5585-40, 5585-60	9.2.2 and later	NA
Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150	9.6.x and later	NA
Firepower 9300	9.6.x and later	NA

Ordering information

To place an order, visit the Cisco ordering homepage.

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For more information

For more information about the Defense Orchestrator, visit: https://www.cisco.com/go/cdo.

For demonstration of Defense Orchestrator, please contact cdosales@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USAs

C78-736847-04 08/17