The bridge to possible

Cisco Defense Orchestrator for Government

Centralized government security for simplified protection.

© 2024 Cisco and/or its affiliates. All rights reserved.

The bridge to possible

Benefits

- Centralize management for all Cisco Firewall ASA and FTD form factors
- Gain real-time visibility into network traffic, threats, and security events
- Automate operational tasks including object updates, device provisioning, and fleet management
- Simplify firewall and branch deployment with cloud assisted device onboarding (Low-Touch Provisioning)
- Improve scalability and accelerate continuous feature delivery with Cisco Defense Orchestrator being a Software-as-a-Service (SaaS) offering

Cisco Defense Orchestrator offers a comprehensive solution for government organizations grappling with the surge in cyberattacks. By providing centralized management of security policies for ASA and FTD firewalls, it enhances visibility across diverse network environments. Its capabilities enable rapid response to coordinated attacks, mitigating threat sophistication. With streamlined policy enforcement and adherence to regulatory compliance frameworks, it fortifies operational security resilience, minimizing financial impacts and safeguarding against penalties and data loss.

Achieving FedRAMP authorization highlights Cisco Defense Orchestrator's commitment to stringent security standards, making it a trusted choice for government agencies. This authorization ensures that Cisco Defense Orchestrator meets the highest data protection and risk management standards, supporting secure cloud adoption in government IT infrastructure. By choosing FedRAMP-authorized Cisco Defense Orchestrator, government organizations can streamline security operations, enhance cybersecurity posture, and confidently embrace cloud solutions while meeting regulatory requirements, underscoring Cisco's dedication to modernizing network security within the federal space.

© 2024 Cisco and/or its affiliates. All rights reserved.

The bridge to possible

Enhanced security readiness, consolidated policies, and streamlined network administration for federal, state, and local government agencies.

Centralized management

Consolidated management of Cisco security products, allowing control of policies and objects across multiple devices from a single, user-friendly interface.

Security policy management support across various environments, including on-prem, public cloud, private cloud, and hybrid cloud, allowing consistent security posture.

For on-prem Firewall Management Center (FMC), Cisco Defense Orchestrator enables consistent policy outcomes across hybrid environments.

Regulatory compliance

Meets FIPS 140 requirements as part of the FedRAMP Moderate for government security standards.

Alignment to TIC 3.0 Policy Enforcement Points, Executive Order 14028, and OMB Memo M-22-09 – zero trust and Protective DNS.

Satisfies enhanced state mandates such as TX-RAMP (level 2 certification), fully meeting NIST 800-53 compliance standards.

Holds Cybersecurity Maturity Model Certification (CMMC) and meets the NIST Cybersecurity Framework.

Holistic visibility and control

Real-time visibility into network traffic and security events, allowing government security teams to monitor and respond to incidents promptly.

Actionable insights from network, system, and security data, empowering organizations to make informed, timely decisions regarding security strategy.

Advanced analytics granting insight into remote user traffic, including visibility and geographic distribution guiding how to best manage security.

Administrator ability to terminate individual or multiple users based on geo-location or other metrics, enhancing security measures and facilitating targeted threat response.

Efficiency and scalability

Automation features for object updates and device onboarding, minimizing the potential for human error and streamlining operations for improved efficiency.

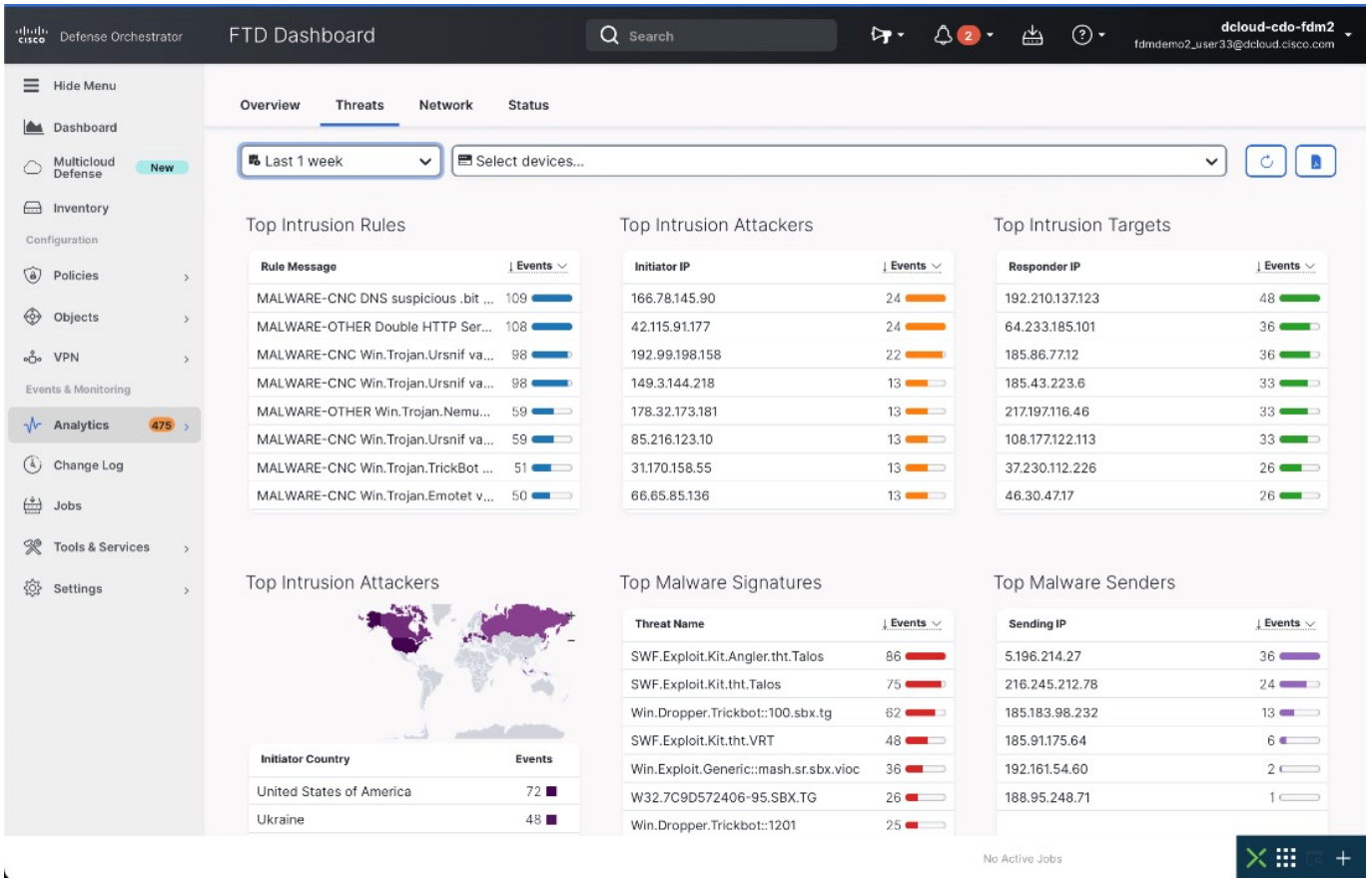
Easily migrate FMC from on-premises to the cloud, including policies, objects, and licenses, without disrupting operations.

Transition from ASA or third-party firewalls to FTD, ensuring efficient management as networks and security infrastructures evolve.

SaaS delivered continuous enhancements, providing government organizations with the latest security features and updates seamlessly.

© 2024 Cisco and/or its affiliates. All rights reserved.

The bridge to possible



Ready to try Cisco Defense Orchestrator?

[Begin instant free trial]

Learn more

[Cisco Defense Orchestrator webpage]

[Cisco Solutions for Government]

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

1332438408 04/24