Cisco Stealthwatch for Federal Organizations

Cisco Stealthwatch™ technology is widely deployed throughout the civilian, Department of Defense, and intelligence communities. It enables agencies to continuously monitor the network for behavioral anomalies and advanced threats.

With network visibility from the gateway to the host level, Cisco Stealthwatch provides government organizations with actionable security intelligence for faster, more informed decisions. It helps them prevent costly and damaging data breaches while accelerating incident response and forensic investigations.

With Cisco Stealthwatch you can:

- Use your existing equipment by cost-effectively transforming your network into a powerful security sensor for detecting sophisticated attacks
- Quickly uncover suspicious behaviors associated with zero-day exploits, advanced persistent threats (APTs), insider threats, and other sophisticated targeted attacks
- Protect sensitive information by thwarting attacks before they lead to a devastating data loss
- Build and maintain a lightweight yet context-rich record of all conversations that crossed the network to assist with forensic investigations

Cisco Stealthwatch is a cornerstone incident response solution for Phase 3 of the Department of Homeland Security's Continuous Diagnostic and Mitigation (CDM) program. Stealthwatch supports CDM by:

- Providing native integrated capabilities in Stealthwatch for awareness and quick response that identify, prevent, and report on key cybersecurity indicators of compromise (IOCs) by focusing on visibility and context.
- Integrating with key CDM technologies for security automation and improved detection and correlation, achieving pervasive network visibility and security for improved threat defense and incident response.
- Working closely with approved system integrators who are authorized to sell CDM program components and systems under the auspices of a General Services Administration (GSA) Blanket Purchase Agreement (BPA).

Cisco Stealthwatch Provides Internal Visibility

Use Your Network as a Sensor with Cisco Stealthwatch

At the Horizontal Gateway

(Trusted Internet Connections and Computer Network Defense Service Provider)

Gain transparency of network connections across the security stack gateway and increase security operations center (SOC) capabilities.

Through the Network

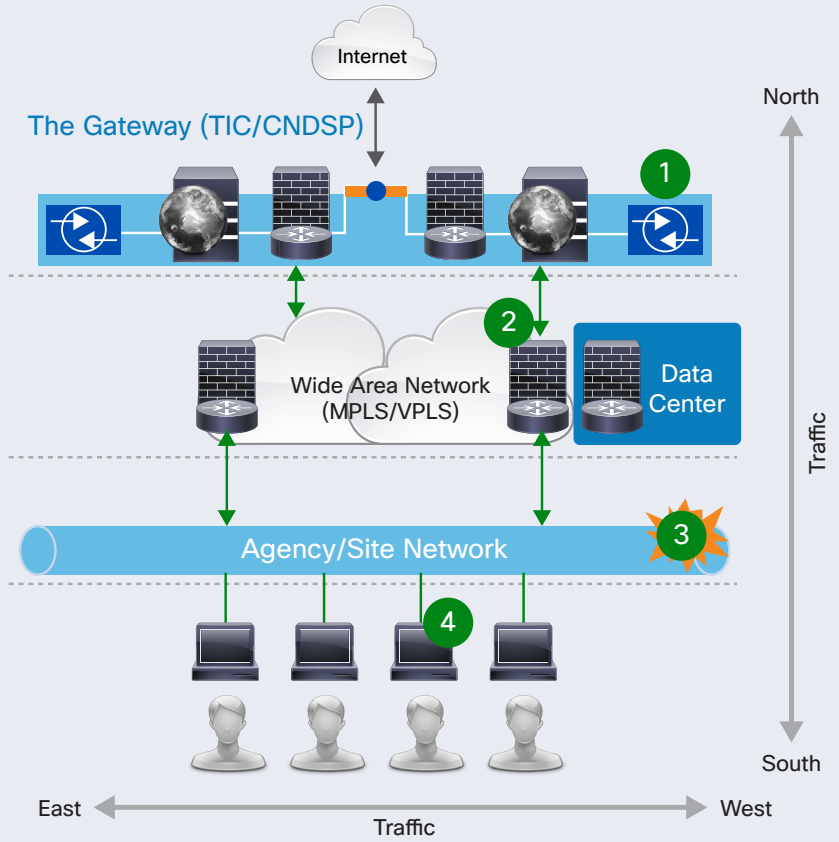
Use flow collection to determine the ultimate source of internal traffic, understand network behavior, and increase network operations center (NOC) capabilities.

As Traffic Moves Laterally across the Network

Understand user behavior in your environment to uncover suspicious activity and detect insider threats, APTs, and DDoS attacks.

To the Host

Track internal users for policy violations and anomalous activities with internal endpoint host attribution and user validation.



1 Continuous Monitoring of TIC

Observe baseline activity at the gateway to profile normal behavior and detect anomalous activity. Fill critical security monitoring gaps. Monitor and verify the percentage of network activity passing through TIC and the Managed Trusted Internet Protocol Service (MTIPS).

2 Vertical Transparency

Store detailed flow records for an extended time to gain valuable visibility at the network gaps and gateway. Harness the full power of flow data by analyzing large amounts of stitched, deduplicated 1:1 flows.

3 Incident Response

Obtain a complete audit trail of all network activity including device, identity, location, application, and time details to the host and endpoint level. Quickly analyze and access detailed information in massive volumes of network and security data.

4 Lateral Visibility and Behavioral Anomaly Detection

Use your existing network to detect sophisticated internal attacks. Baseline normal user behavior so that anomalies can be swiftly identified and investigated. Detect insider threats including unauthorized access, data hoarding, and data loss.

C22-737930-00 10/16