CDM PHASE 3

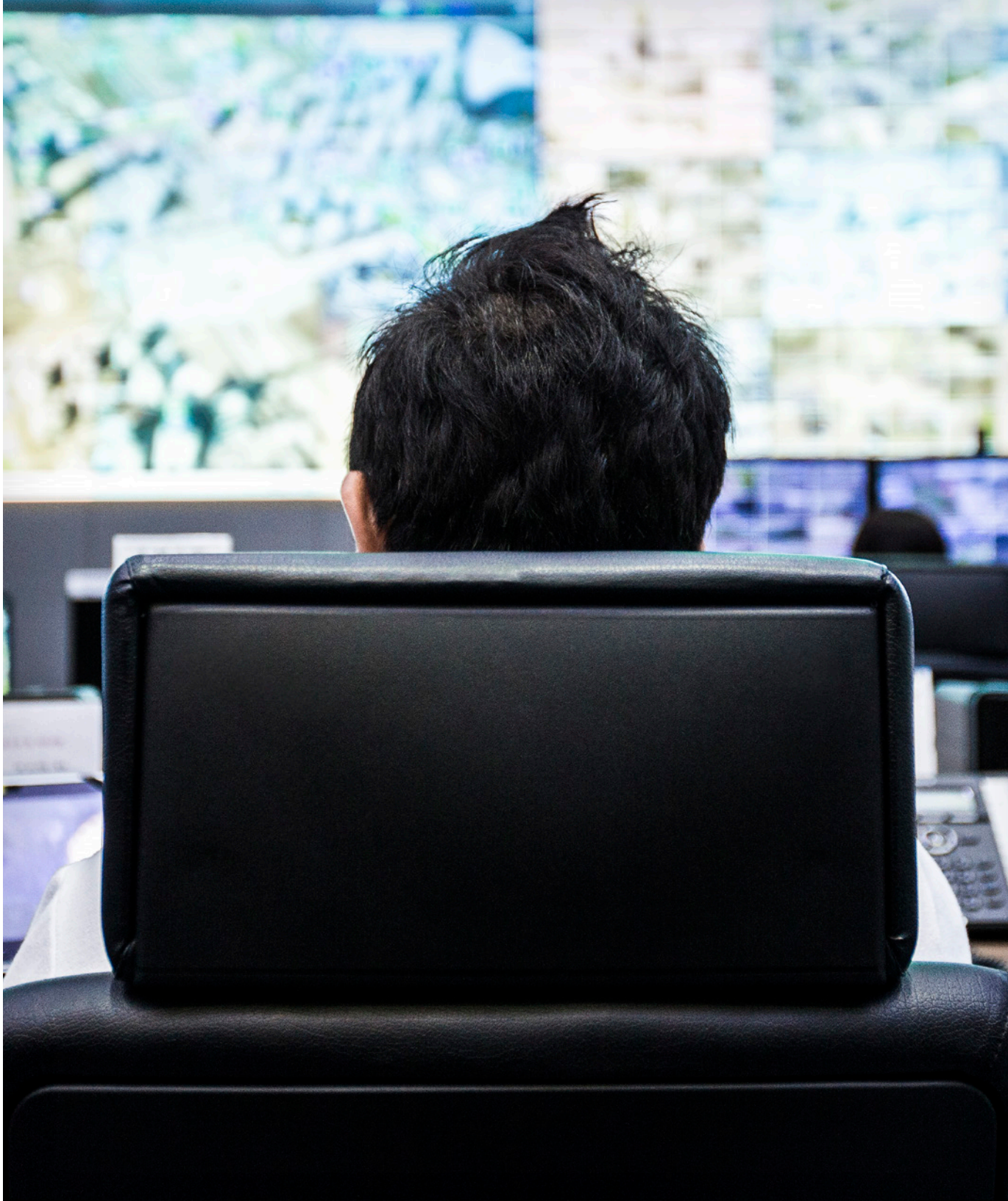
Cybersecurity for federal agencies

An integrated, automated, and threat-driven approach

The Department of Homeland Security (DHS), in partnership with the General Services Administration (GSA), is implementing Phase 3 of the Continuous Diagnostics and Mitigation (CDM) Program – Optimized Cybersecurity Products and Solutions.

Building on Phase 1 (What is on the network) and Phase 2 (Who is on the network), this phase (What is happening on the network) addresses preparing for, detecting, and mitigating security incidents.

As cyberattacks increase in frequency and sophistication, Phase 3 of the CDM is vital in safeguarding, securing, and strengthening your cyber capabilities and the security posture of federal networks.



CDM Phase 3: At a Glance

The Continuous Diagnostics and Mitigation (CDM) program includes three phases:

- **Phase 1:** What is on the network
- **Phase 2:** Who is on the network
- **Phase 3:** What is happening on the network

  CDM Phase 3 elements:

  1. Network boundary protection (BOUND)
  2. Managing network events (MNGEVT)
  3. Designing and building in security (DBS)
  4. Operating, monitoring, and improving the network (OMI)s

Defend

Did you know that a series of new CDM related task orders, known as Dynamic and Evolving Federal Enterprise Network Defense (DEFEND), has been issued? The task orders let Federal agencies like yours use the Alliant Government-wide Acquisition Contracts (GWAC) to more quickly and easily implement cybersecurity products and solutions for Phase 3.

Top cybersecurity challenges for federal government

Protecting the government's networks, systems, and data is a complex matter, with many interlocking elements.

Buying independent elements per phase greatly increases this complexity, and can detract from your mission's efficiency. It's not uncommon for a large agency to have hundreds of security tools from dozens of vendors in its product portfolio. In today's world of dynamic, rapidly evolving threats, this situation has become untenable and dangerous.

8 Cisco advantages for CDM Phase 3

Because of this complex security environment, you need to have an integrated, automated approach to CDM. Dynamic visibility across the entire network (at its perimeter and throughout the infrastructure) – coupled with extensive automation to detect and respond to threats in real time – is essential.

With unsurpassed security and networking expertise, Cisco offers the solutions and experience to safeguard government organizations against the growing threatscape.

#1 Visibility (phases 1 and 2)
Understand who and what is on the network and how it got there (route of access)

#2 Security
Realize dynamic monitoring, deeper visibility, and near-real-time views with integrated, automated, and threat-driven security

#3 Simplicity
Reduce vendor and system complexity with a solution that is simple to provision and operate

#4 Compliance
Work with Cisco's entire portfolio, all of which is on the approved-product list

#5 ROI
Maximize investment with solutions flexible enough to integrate with your existing core infrastructure and future-proofed to support upcoming Phase 4 requirements in cloud, mobility, and automation

#6 Integration
Benefit from Cisco's world-class networking and security expertise to optimally address cybersecurity challenges – from endpoints to network core – without impeding connectedness or productivity

#7 Efficiency
Use the same Cisco tools you use to achieve your mission to implement required standards, reporting, and compliance

#8 Interoperability
Strengthen your existing IT and investment with open Cisco solutions that easily work with other vendors' solutions

Where Cisco fits in CDM Phase 3

Primary Secondary

Cisco Products		How is the network protected?	What is happening on the Network?			Form Factor
		Boundary Protection	Manage Events	Operate, Monitor, and Improve	Design and Built-in Security	
Network Security Products	Route/Switch (LAN)	Primary			Primary	P
	SD-WAN	Primary			Primary	P/V
	ESA/WSA	Primary		Primary	Primary	P/V
	FTD/NGFW/NGIPS	Primary	Secondary	Primary	Secondary	P/V/C
	ISE/TrustSec	Primary	Secondary	Primary	Secondary	P/V
	SW	Secondary	Secondary		Primary	P/V/C
	AMP/TG	Primary		Secondary	Secondary	P/S/C
	Meraki	Primary	Secondary	Primary	Secondary	P/C
	AC	Primary		Primary	Secondary	S
	Umbrella	Primary	Secondary	Primary	Primary	C
	Cloudlock	Primary	Secondary		Primary	C
	ETA	Secondary		Secondary	Secondary	C
Management	FMC/PI/DNA Center	Primary	Secondary	Primary	Primary	P/V/S
	pxGrid	Secondary	Secondary	Secondary	Secondary	S
Threat Intelligence	CTA	Secondary	Secondary		Primary	C
	Talos	Secondary	Secondary		Primary	C

Abbreviations

- **FTD:** Firepower Threat Defense
- **NGFW:** Next-Generation Firewall
- **NGIPS:** Next-Generation Intrusion Prevention System
- **FMC:** Firepower Management Center
- **PI:** Prime Infrastructure
- **DNA Center:** Digital Network Architecture Center
- **ESA:** Email Security Appliance
- **WSA:** Web Security Appliance
- **AMP/TG:** Advanced Malware Protection/Threatgrid
- **ISE/TrustSec:** Identity Services Engine/TrustSec
- **ETA:** Encrypted Traffic Analysis
- **CTA:** Cognitive Threat Analytics
- **Form Factor:** Physical **(P)** – device comes in its own server format/appliance
- **Form Factor:** Virtual **(V)** – device runs as a virtual machine on a hypervisor
- **Form Factor:** Software **(S)** – device is installed as software/agent
- **Form Factor:** Cloud **(C)** – device run in cloud services (for example, AWS, Azure, etc.)

LEARN MORE

Read more about Cisco and CDM in our whitepaper.

Visit cisco.com/go/federalcybersecurity to explore Cisco cybersecurity solutions for federal government.

cisco