# Cisco Provides Essential Cyber Solutions for Continuous Diagnostics and Mitigation

US Government compliance mandates and guidance are driving a move towards continuous monitoring by Federal agencies; an approach that promises improved response times, increased threat visibility, and less down time as they strive to serve our nation's citizens.

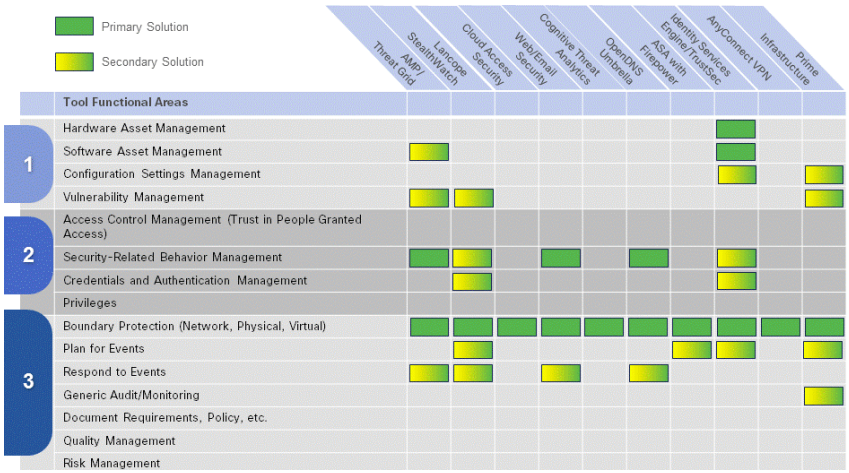
## Cisco Solutions for CDM

Cisco offers a complete set of solutions for the CDM Program including policy and access controls, next-gen network security, advanced threat solutions, and content security capabilities. The Cisco Cybersecurity Portfolio includes:

- **Cisco Solutions for Policy and Access** (Cisco Identity Services Engine (ISE), Cisco TrustSec and Cisco AnyConnect Secure Mobility Client
- **Cisco Solutions for Next-Generation Network Security** (Cisco Next-Generation Firewall and Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS))
- **Cisco Solutions for Advanced Threat Protection** (Cisco Advanced Malware Protection (AMP) + AMP Threat Grid and Cisco Lancope StealthWatch)
- **Cisco Solutions for Content Security** (Cisco OpenDNS Umbrella, Cisco Cloud Access Security (CAS), Cisco Cognitive Threat Analytics, Cisco Email and Web Security, Cisco Solutions for Simplified Management, Cisco Prime Infrastructure, Cisco Firepower Management Center).

## Select the Right CDM Partner

To successfully fulfill the mandate, an agency's CDM partner must understand the program's goals and empower their own solutions with three critical capabilities: **integration**, **consolidation** and **automation**. At Cisco, we understand this and believe these three capabilities are the best way to enhance cybersecurity without increasing complexity.




Cisco cybersecurity solutions are designed to integrate seamlessly and share information in real time (visibility-driven, platform-based and SCAP-enabled). They also consolidate by embedding security in everything we do and by offering many of our cybersecurity solutions as a service from the cloud. Cisco also automates whenever possible to help provide better data, improve workflow, enable faster response to threats and even improve morale due to less stress and overwork.

## Leverage Cisco Solutions for CDM

An end-to-end model with automated analytics can provide network, security and risk management teams with a firm understanding of where security is working, where investment is needed and where their greatest risks of attack lie. By leveraging the **Cisco® Identity Services Engine (ISE)** you can gain the security intelligence needed to actively identify and classify hardware that attempts to connect to the network, and block hardware that is not authorized to connect. Plus, with the **Splunk for Cisco ISE** add-on you can extract and index the ISE AAA Audit, Accounting, Posture, Client Provisioning Audit and Profiler events.

Cisco offers a comprehensive portfolio of threat-centric cyber security solutions that span the entire attack continuum; before, during and after an attack and which align closely with the goals of the DHS CDM program. ISE's superior device profiling and "zero-day" device profile help reduce the number of unknown endpoints (and potential threats) on an agency network. We also provide end-to-end network security through our NAC appliance; a product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. And with Adaptive Network Control (ANC) as a service that runs on the Cisco ISE Administration node, you can reset the network access status of an endpoint to quarantine, unquarantine or even shutdown a device.

### How Cisco ISE Benefits Government Agencies

**Advancing Efficiency:**

- Management + security from a single solution
- Broad breadth of management
- Comprehensive Security
- Manages and secures virtually all enterprise device types
- Optimized for remote environments
- Integrated with desktop management
- Market-leading technology

**Reducing Costs:**

- Cost reduction — $ and IT resources
- Reduced number of support contracts to maintain
- Lowered mobile device TCO through elimination of vendor redundancies
- Single multi-channel access gateway for mobility

**Simplifying Management:**

- Single console to manage and secure laptops and mobile devices
- Management and security tasks occur in a single connection
- Integrated platform means solution will seamlessly work together: no need to "manage the gaps"
- Improved technical product support
- Reduced end-user device complexity

## Other Solution Areas Supported

With a slew of acquisitions of cutting edge security firms, such as Sourcefire, Cisco products are well positioned to handle correlation, context, and visualization of information layered on top of metrics that can make practical and dramatic changes to security. For example, adding Sourcefire's Advanced Malware Protection (AMP) technology into the email and Web security appliances has resulted in AMP using file reputation and sandboxing. AMP also uses a technique called file retrospection for analyzing threats that have made it into the network. File retrospection monitors and tracks user devices that have been exposed to malware so that a company can take steps to remediate the problem. This allows agencies to comply with all three phases of the DHS CDM initiative.

## Next Steps

To learn more about Cisco's US Government Solutions and Services, visit us at http://www.cisco.com/go/federal. For more detailed information about Cisco's Cybersecurity Solutions for Continuous Monitoring and Mitigation, contact:

**Brian Finan** Account Manager, Security Sales
**Email:** brfinan@cisco.com