Continuous Diagnostics and Mitigation (CDM) Dell Data Security Product Family Compliance

The Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program provides a dynamic approach to strengthen federal cybersecurity. CDM capabilities and tools identify cybersecurity risks on an ongoing basis. Federal cyber leaders can prioritize risks based on potential impacts and mitigate the most significant problems, first.

The CDM program empowers agencies to establish dynamic safeguards against evolving threats. A phased framework delivers a comprehensive approach to secure government data, encompassing three phases and fifteen functional areas. Data feeds into an agency-level dashboard for display and action. Phase 1 and Phase 2 are focused on "What is on the network" and "Who is on the network." Phase 3 builds on these two phases to examine "What is happening on the network" – on premise and in the cloud. Agencies can move from asset management to dynamic security control monitoring.

A federal-level dashboard aggregates data from agency dashboards, supporting security oversight and reporting. CDM Phase 3 measures each agency's time to breach and time to remediation.

DATA IS ON THE MOVE; SECURITY MUST KEEP UP

Government employees working from remote locations connect to cloud-based services and business applications. As a result, agencies need to define the "boundaries" of where data resides. They need advanced, enterprise-wide security to protect the data layer. As data leaves traditional agency boundaries, cybersecurity leaders need visibility into where data travels.

Dell provides comprehensive endpoint security solutions to help agencies achieve their security mission. We know employees need to share data to stay productive. Our CDM-approved solutions deliver seamless security to encourage efficiency and limit exposure to data threats.

TRANSFORM SECURITY WITH CDM-APPROVED SOLUTIONS

Dell Endpoint Security Suite Enterprise
Dell Data Security Product Family with Advanced Threat Prevention

- Uses artificial intelligence and predictive mathematical models, instead of signatures
- Identifies suspicious files before they execute, stopping malware from entering the organization
- Delivers enterprise class encryption; stops evolving attacks
- Simplifies endpoint security and helps exceed regulatory compliance
- Eliminates the need for a cloud connection and frequent updates with intelligence at the endpoint
- Stays ahead of threats with algorithms based on markers extracted from billions of real-world exploits and known good files
- Blocks malware in air-gapped networks with minimal security solution updates; implementation is on premise
- Delivers the industry's only off-host BIOS verification on commercial Dell PCs

Dell Encryption Enterprise
Dell Data Security Product Family with Dell Encryption

- Provides enterprise-class data protection with data-centric encryption and robust on premise key management

- Protects data-at-rest through a choice of full disk or data-centric file level encryption
- Enables data protection on a variety of devices including Windows PC, Mac devices, and Windows Servers
- Manages access to sensitive data with multi-layered / multi-key approach
- Meets federal security standards with dual layer encryption; only PC manufacturer with NIAP and CSfC certifications
    - FIPS 140-2 certified
    - Common Criteria against a NIAP approved protection profile
    - CSfC Listed encryption component

Dell Data Guardian

Dell Data Security Product Family with Encryption (stand-alone license)

- Protects, controls, and monitors data wherever it goes
- Secures data in transit via email, cloud services, FTP, and portable storage devices
- Sets data access parameters – who has access to specific data; when data can be accessed; how data can be used
- Provides analytics on data access, activity, and location with the Dell Security Management Server
- Detects potential risks and enables agencies to take immediate action
- Improves visibility and monitoring with Encryption and Enterprise Digital Rights Management

SIMPLIFIED REMOTE ADMINISTRATION

Enterprise security doesn't have to be difficult to manage or require administrators to jump between disparate management tools and vendor support organizations. Dell Endpoint Security Suite Enterprise and Dell Data Guardian provide an integrated console to simplify security management.

The Dell Security Management Server gives administrators a single pane of glass to manage threat prevention, encryption, and data across the enterprise. Administrators track all data activity, visualized with mapping data, file, and user events. A comprehensive compliance reporter provides standard and customized options. And, security alerts warn personnel of security compromises and enable the required action.

Dell Data Security

Innovative Security for the Evolving Workforce

As the endpoint industry innovator, Dell has been at the forefront of putting customer needs first, always. While data is crucial in driving growth and empowering employees to deliver, it is too often open to great risk.

- Protect Data: The workforce is increasingly mobile and with data as the lifeblood of business it needs to be protected. Dell Data Security can help protect, control, and monitor data anywhere, while multi-factor authentication ensures the right person accesses it and assurance is provided with making backing and recovery simple
- Prevent Threats: With advanced threat prevention such as innovative anti-malware solutions, BIOS verification, and self-healing endpoint visibility, Dell Data Security can detect and respond to breaches faster and remedy them more effectively
- Manage Endpoints: Leading enterprise mobility management that supports every endpoint and every user from a single management console

Dell Data Security brings you award-winning solutions that evolve with your workforce, safeguarding your data from emerging threats.

Learn more at datasecurity.Dell.com or call 866-931-3356.