NS2 Briefing

Using Continuous Diagnostics and Mitigation (CDM) to Protect the Nation

NS2 NATIONAL SECURITY SERVICES

Cutting-edge software solutions to protect your organization's infrastructure and data.

NS2 cyber defense solutions are available to federal, state, local, and tribal government agencies to help protect networks and data from cyberattacks. Powered by gosecure, this cutting-edge technology is on the CDM program approved products list (APL) and is available through the request for service process, which streamlines procurement and augments access to funding in order to quickly deploy critical capabilities to organizations.

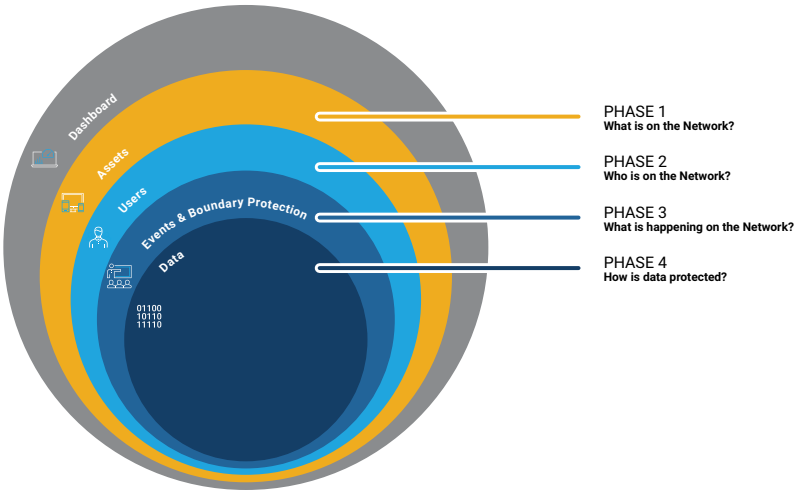
What is the Continuous Diagnostics and Mitigation (CDM) Program?

The CDM program is managed by the Cybersecurity and Infrastructure Agency (CISA) of the Department of Homeland Security. CISA leads the national effort to defend critical infrastructure against today's threats, while working with government agencies and the private sector to secure against the evolving risks of tomorrow.

To help accomplish this, the program provides cybersecurity tools, integration services, and dashboards to support participating agencies in improving their respective security posture.

The objectives of the CDM program are to:

- Reduce agency threat surface.
- Increase visibility into federal cybersecurity strength.
- Improve federal cybersecurity response capabilities.
- Streamline Federal Information Security Modernization Act (FISMA) reporting.



SAP NS2 Continuous Diagnostics & Mitigation

The CDM Program delivers capabilities in five key areas:

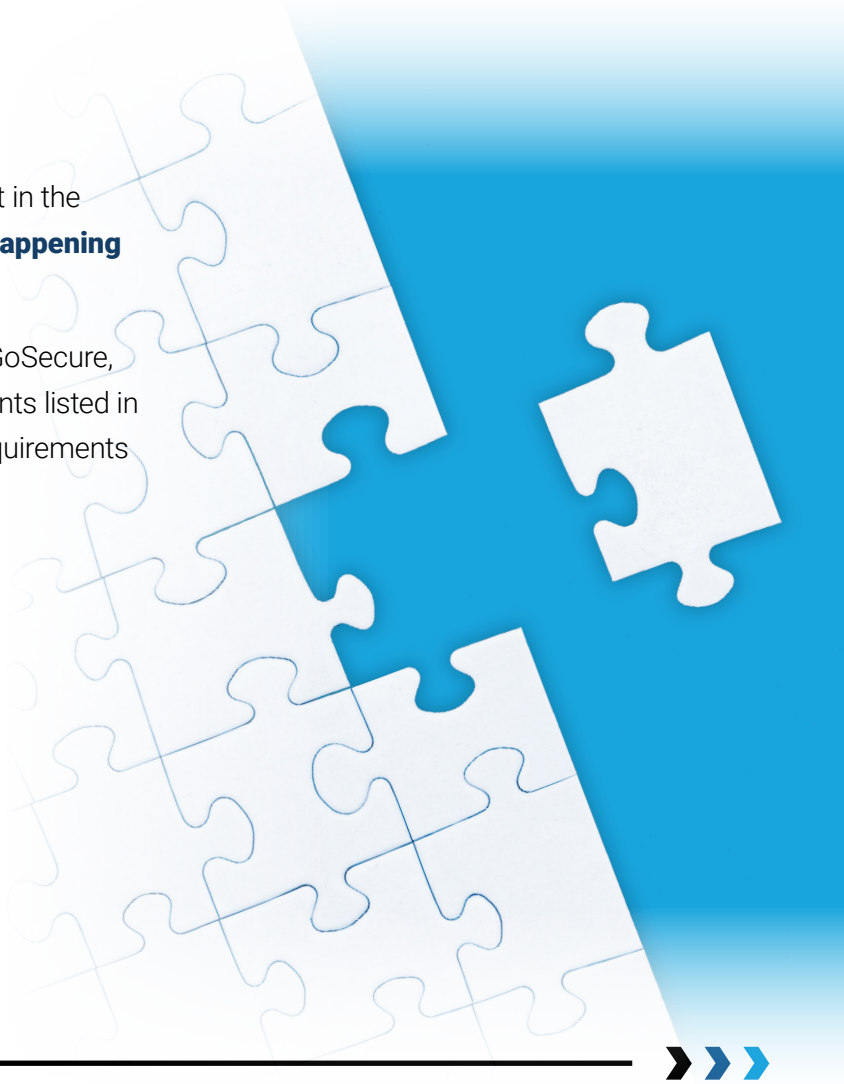
- **Dashboard:** Receives, aggregates, and displays information from CDM tools at the agency and federal level.
- **Asset Management –** Manages hardware assets (HWAM), software assets (SWAM), security management configuration settings (CSM), and software vulnerabilities (VUL).
- **Identity and Access Management –** Manages account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security related training (BEHAVE).
- **Network Security Management –** Manages network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. This includes management of events (MNGEVT); operate, monitor, and improve (OMI); design and build-in security (DBS); boundary protection (BOUND); supply chain risk management (SCRM); and ongoing authorization.
- **Data Protection Management –** Manages the protection of data through the capabilities: data discovery/classification (DISC); data protection (PROT); data loss prevention (DLP); data reach/spillage mitigation (MIT); and information rights management (IRM).

The Solution

Our solutions are listed on the approved products list in the area of **"Network Security Management: What is happening on the network?"**

NS2 provides cyber defense solutions, powered by GoSecure, that have been approved for the following requirements listed in the CDM document: CDM Technical Capabilities Requirements Catalog Volume Two, 2018 Version 1.4):

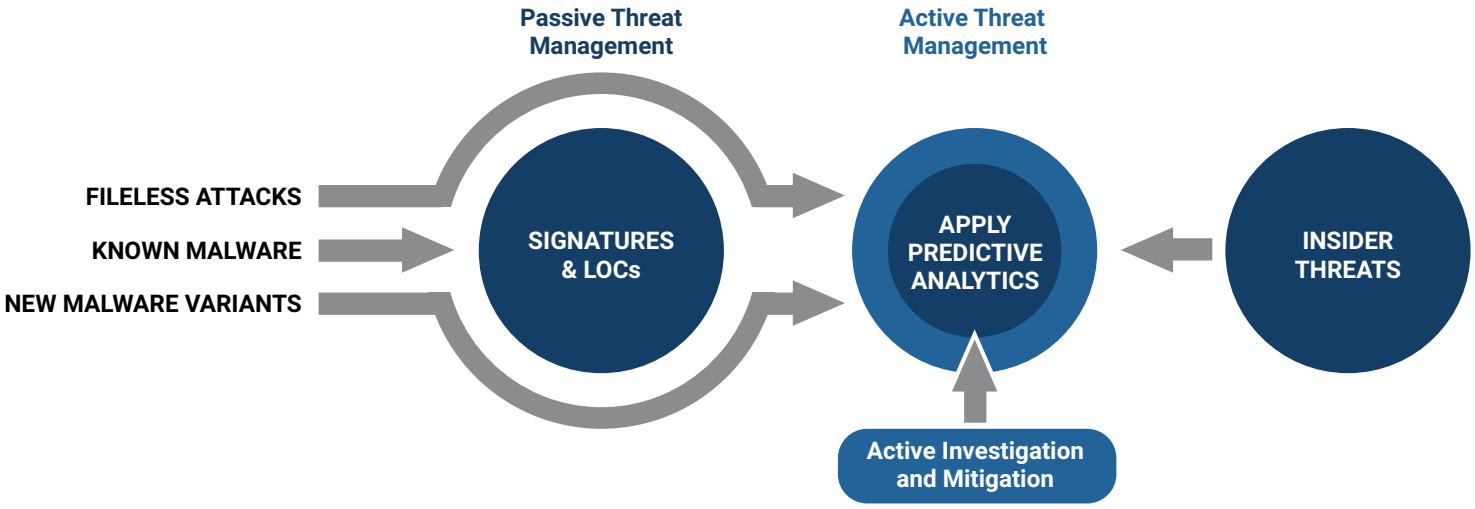
- Incident Response Monitoring
- Ongoing Assessment Monitoring
- Ongoing Authorization
- System and Information Integrity
- Risk Assessment



SAP NS2 Continuous Diagnostics & Mitigation

Our solutions perform endpoint detection and response to protect servers, PCs, and mobile devices in your organization. Common approaches to cyber defense, like passive threat management, are dependent on recognizing the signatures of known malware binary code. Our technology employs active threat management, which uses machine-learning predictive analytics to monitor system and user behaviors. In this way, NS2 offers a tool that can help protect your organization against malware with new and unknown variants, malware that runs in the RAM memory of servers and endpoints, and file less attacks.

The benefits of Active Threat Management:



- Reduce impact from attacks
- Faster time to triage incidents—from days to minutes
- Faster time to mitigate incidents—from hours to seconds
- Capture and respond to malicious behavior in real-time with threat level context (severity scoring)
- Correlate multi-source threat intelligence for unprecedented security context

GoSecure combines a simple-to-deploy unified endpoint agent with a powerful, centralized threat analysis server. This agent gathers data on the endpoint and acts on it locally, while also sending the information to a centralized server for analysis in the context of what is happening elsewhere in your network environment.

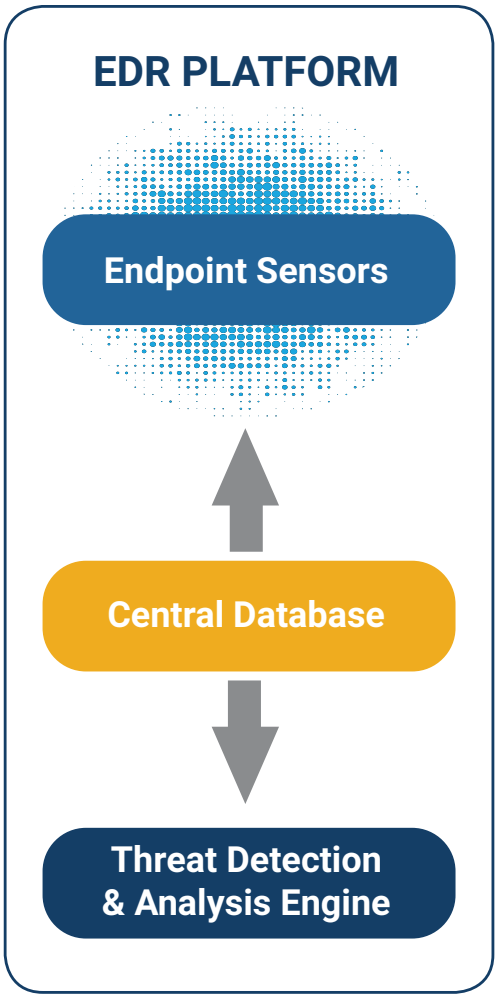
SAP NS2 Continuous Diagnostics & Mitigation

Endpoint Agent Sensor

- Protects servers, desktops, mobile computers
- Automates mitigation
- Unified endpoint agent to simplify deployment
- Low-performance impact
- Real-time on-disk behavioral analysis
- In-memory reverse-engineering of malware
- Scalable to 100,000s of endpoints

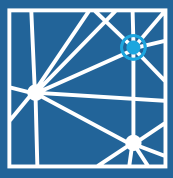
Centralized Threat Analysis Server

- Machine-learning predictive analytics
- Known & unknown threat detection
- Visibility of event types (3x industry average)
- Behavior-based beyond traditional good/bad
- Threat-hunting, ad-hoc search
- Integration with SIEM and other tools



Real-Time Behavior Analysis

- Follows all behavior beyond just detecting malware, like identifying users copying files using a USB drive and other policy violations.
- Immediately quarantines the endpoint to prevent exfiltration of data.
- Spoofs the insider with a honey pot internal IP address to allow continuous threat collection and analysis.
- Advanced behavior profiles with risk scoring.



Real-Time Unknown Threat Detection

When an interaction of interest occurs, the following will occur:

- The endpoint agent collects behavior data
- Threat is scored as an alert and exposed for analysis
- The centralized analysis engine identifies threat behaviors, code injection, file proliferation and lateral movement
- Users can add their own custom malicious behaviors

SAP NS2
NATIONAL SECURITY SERVICES

Available as on-premise software or as Software-as-a-Service (SaaS)

Once the endpoint sensor is installed on your devices and servers, you'll have two options to deploy the central analysis server. It can be installed on-premise in your data center or consumed as Software as a Service in the NS2 Secure Cloud. The NS2 cloud is managed for you at the appropriate security level for your organization, whichever is required: FedRAMP and ITAR, ILM 4-5, DoD SRG and IRS 1075, CJIS compliance.

CDM Program Acquisition Strategy

The CDM Tools Special Item Number 132-44 supports the DHS and Cybersecurity and Infrastructure Security Agency (CISA) CDM program. The CDM SIN is a government-wide contracting solution that provides a consistent set of Information Security Continuous Monitoring (ISCM) tools to federal, state, local, regional, and tribal governments. The SIN includes cybersecurity tools and sensors.

The hardware and software products and associated services under this SIN undergo a DHS CISA product qualification process in order to be added to the CDM Approved Products List (APL). Cyber Defense Solutions from NS2, powered by GoSecure, are on that APL.

The CDM acquisition strategy is a two-pronged approach to provide products and services to meet the CDM program objectives. It includes:

1. The CDM Tools Special Item Number (SIN) on GSA IT Schedule 70.
2. Services executed through the Dynamic and Evolving Federal Enterprise Network Defense (DEFEND), a series of Task Orders (TOs) against the Alliant GWAC.

Agencies can make CDM SIN purchases through eBuy, GSA Advantage!, or by issuing a vendor request for more information. Federal, state, local, regional, and tribal governments can purchase CDM Tools via the Information Technology Category under the Multiple Award Schedule (ITC-MAS).

To learn more about Cyber Defense Solutions from NS2 powered by GoSecure visit our Services and Support page or reach out directly to NS2 today.

NS2 NATIONAL SECURITY SERVICES

877-972-7672
info@sapns2.com
www.sapns2.com

Now, let us help you. Learn more at sapns2.com/security/