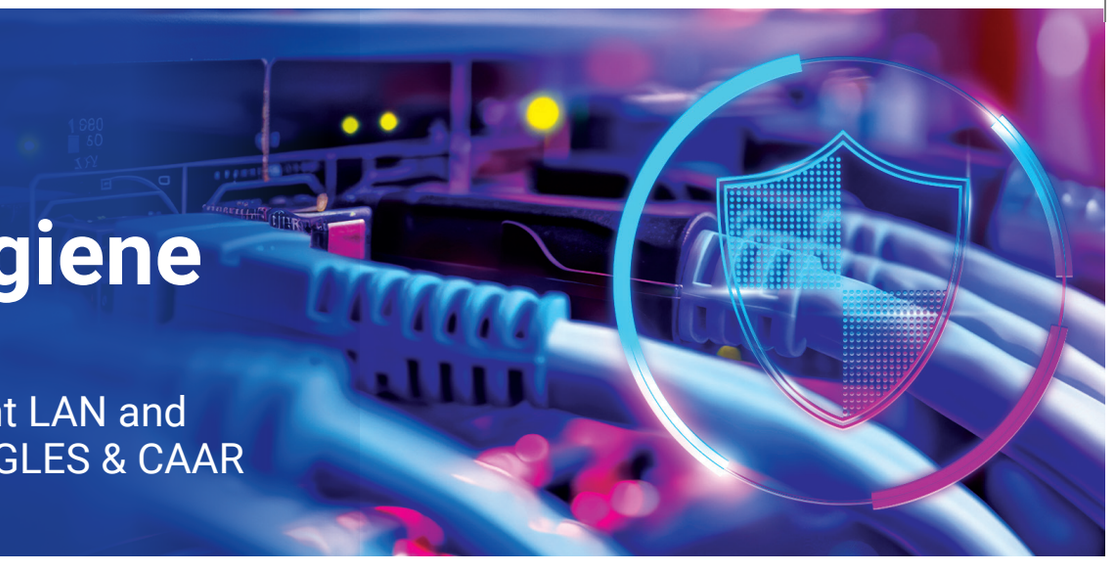
Technology Update

# Cyber Hygiene at Scale

## Securing Government LAN and Endpoints using MOGLES & CAAR



Edited by **MOHAN DAS VISWAM**

Government Cyber Space is an extremely challenging environment targeted persistently by the best in the world with limitless resources at their disposal (read nation-state advanced persistent threat attackers (APTA)). Government infrastructure is a collection of various autonomous systems each with its own policies and controls. So, traditional cyber security models do not fit government's cyber security needs. Hence, there was a need to develop a custom model for securing government Local Area Network (LAN) and Endpoints (EP). NIC developed Model of Government LAN & EP Security (MOGLES) after experimenting with various tools and techniques and finalizing the one that works the best. MOGLES has been successfully implemented in critical ministries/departments and working fine for more than two years. It is a time-tested and proven model. It is built with basic measures but with strict implementation. This model can be implemented at all other ministries/departments/organisations/states in phased manner with necessary resources.

## Building Blocks of MOGLES

### Time, Patience & Consistency

We need to understand & accept that securing an infrastructure is like building a fort, one wall at a time, one moat at a time, one bastion at a time; there are no magic tricks or wands. It is hard work which needs persistent efforts and time along with necessary resources. So, we need to set reasonable & achievable targets and work dedicatedly towards it without shifting goalposts frequently. Typically, a LAN with 500 endpoints may take around 2-3 months without major disruption. It can be achieved within 2 months at war footing.

**Syed Hasan Mahmood**
Scientist - D
hasan@nic.in

**Rajeev Kumar Yadav**
Scientist - C
yadav.rajeev@nic.in

To address the complex cybersecurity needs of government infrastructure, a custom framework—Model of Government LAN & Endpoint Security (MOGLES)—has been formulated and successfully implemented across critical ministries. Complemented by the Continuous and Automated Assessment and Remediation (CAAR) approach, it ensures structured endpoint security, continuous system hardening, and policy compliance. This scalable, privacy-centric model leverages existing technologies to enable robust, cost-effective, and sustainable protection of government networks and digital assets.

### Authority & Ownership

The NIC Head of Department (NIC-HOD) or Nodal Officer (NO) must be entrusted with full authority and responsibility for implementing MOGLES. Their success depends on strong coordination with stakeholders and users within the ministry or department. Commitment and trust are essential from both NIC and the department. Additional L1 support engineers and necessary resources must be provided to the NIC-HOD/NO to handle operational tasks effectively.

### Establishment of ITHD

Each ministry/department must set up an IT Help Desk responsible for provisioning all endpoints. Regardless of how the endpoint was procured, it must pass through the ITHD for formatting and secure configuration before being handed to users. This also applies during personnel transfers or role changes. The ITHD should operate from a dedicated lab space, equipped with tools to handle multiple endpoints simultaneously and a stock of spare devices for replacements. It will function under the NIC-HOD/NO, with a Single Point of Contact (SPOC) nominated from Admin/Purchase/Store sections to manage logistics and coordination.

### Formatting of all old endpoints

All legacy endpoints must be formatted before secure configuration. If an endpoint is already compromised or malfunctioning, other measures will be ineffective, and the endpoint will remain untrusted. Any old device not processed through the ITHD must be formatted, and any device showing abnormal behavior should be reformatted promptly.

### Deployment of EPS Tools

Multiple endpoint security tools are needed for various functions. An ideal environment must have all of them. But we can start with a few necessary ones and augment the others in due course. A typical set of tools is listed below. The systems maintenance and management of these tools will be the responsibility of NIC Endpoint Security (EPS) Team. EPS team will provide technical support needed for deployment of the agents and troubleshooting issues. The policy to be implemented on endpoints will be provided by EPS team. The deployment, functioning of agents on endpoints and endpoint support will be the responsibility of NIC-HOD/NO and its team. Another important responsibility of NIC-HOD/RO is to ensure that all endpoints that are powered on must report to all the central consoles. If an endpoint is not reporting on any central console it will be considered non-compliant. The compliance of the endpoints using the provided tools, policies, guidelines and procedures will be the responsibility of NIC-HOD/NO. In case of any issue or new requirement, NIC-HoD/NO should reach out to EPS team for resolution/solution.

**Mandatory Tools:**

### Network Access Control (NAC)

It acts like a sentry for network access. No endpoint is allowed to access the LAN until the user is authenticated and device posture evaluated for compliance. It will ensure that all endpoints in the LAN are authenticated (to a user) and compliant to the government policy. Any non-compliant device can be moved to a quarantined segment until the compliance is achieved. It can be used to detect and automatically deploy UEM/EDR, if not found installed on endpoint during posture evaluation. DHCP is mandatorily needed for NAC to function correctly. Hence it is also integrated with NIC LDAP and IPAM to automatically update the IP details of each authenticated user in IPAM. The IP inventory will always be updated automatically and correctly.

### Unified Endpoint Management (UEM)

It is the primary tool for managing the endpoint w.r.t. OS deployed & patching, software deployment & patching, policy configuration, compliance and auditing. All other tools can be deployment using it. It is the first and most important tool to be deployed on each endpoint. All the endpoint configuration, policy enforcement and hardening are being deployed using UEM. It will primarily be used for endpoint management without going to user desks and eating up users' working time. All the tasks will be carried out from UEM console silently in the background without interfering with users. UEM will be used instead of Domain Controllers (DC) as it provides all the functionalities needed by government infrastructure without the security risks associated with DC. For example, in a Windows environment, GPO, SecPol etc. will not be configured.

### Endpoint Detection & Response (EDR)

It is the primary security tool for protecting the endpoints from malware and other attacks. If an endpoint is connected to the government network or holds government data without a functional and online NIC approved EDR agent, government data and the entire network are at risk. EDR is a behaviour-based anomaly detection security tool that applies AI/ML models on large amount of endpoint logs and telemetry to detect new and unknown threats. It is not dependent upon signatures. EDR is used for managing the host firewall of the endpoints to prevent network attacks and lateral movements. It is also used to control and manage external USB storage media connecting to endpoints. It is also used for threat hunting and incident response in case of compromise.

### Offline Data Backup (ODB)

In today's cyber world, no system is hack-proof or perfectly safe. Even after trying the level best and putting best of the security controls available, there are small chances that the endpoint may get compromised and data corrupted/encrypted/lost/wiped. In such cases, Offline Data Backup (ODB) comes to the rescue. ODB is based on the philosophy of hope for the best but plan for the worst where data recovery from offline backup is a measure of last resort. It is to be understood that online backup in cloud storages and drives maybe better than no backup but cannot act as a substitute for periodic offline backup. Online or connected backups are fraught with similar risks as data on endpoints. Considering the sensitivity of govt. data, it is recommended to keep periodic backups of user data created on endpoints on individual storage media like portable hard disks.

**Optional Tools:**

### Operating System Log (OSL) Collection

Although EDR telemetry collects most of the relevant logs from the endpoint but not all of it. APTA are well aware and versed with the EDR telemetry of popular products. They continuously hunt, develop and use techniques which escape EDR telemetry data making threat hunting difficult. So, it is important to also capture detailed Operating System Log (OSL) to detect such sneaky and advanced attack vectors. For example, Windows Event Logs and Sysmon logs collect a wealth of data from Windows endpoints including task scheduling events, PowerShell execution events, USB connection events etc. This data becomes critical in case of compromise by APTA for detection and forensics. The problem with OSL is that it has limited capacity and is then overwritten by newer logs quickly resulting in loss of logs. So, they have to be collected on a central data lake to ensure extended periods of retention and analysis. OSL are not forwarded automatically by OS, so some agent has to be installed and configured to ship logs to the central data lake.

### Digital Rights Management (DRM)

DRM focuses on data security. It doesn't concern with the security of endpoints or any other device. Its sole focus is to protect user data, whether at rest or in motion. It provides granular ri ghts for data sharing and access with detailed logging and continuous auditing. It provides persistent protection which ensures that data is safeguarded or protected wherever it resides, including in copies. It supports dynamic policy control which allows data owners to modify the permissions for their protected data at any point in time even if the file has already been shared. DRM has a feature of automatic expiration of files which allows administrators to set expiration dates for access that has been granted beyond which the access rights are automatically revoked. DRM also imposes replication restrictions which ensures that illegal or unauthorized copying of protected data is prohibited.

### Data Loss Prevention (DLP)

DLP is also a data security solution which keeps track of sensitive data on endpoints and prevents leaks via various media like external USB storage, web/email upload, network share, print and copy etc. It is different from DRM as it works automatically in the background without user interaction implementing organisational data security policies. It can work on classification of data by users or automated keyword-based protection. It can be deployed in monitoring or protection mode. Monitoring mode will generate alerts for the administrators and protection mode will prevent movement of files against the defined policies. DLP can also be used to encrypt sensitive files automatically while being copied/shared to external media. These encrypted files will open only on internal endpoints with DLP agent running and remain encrypted on all other endpoints. This prevents inadvertent leakage of files/data.

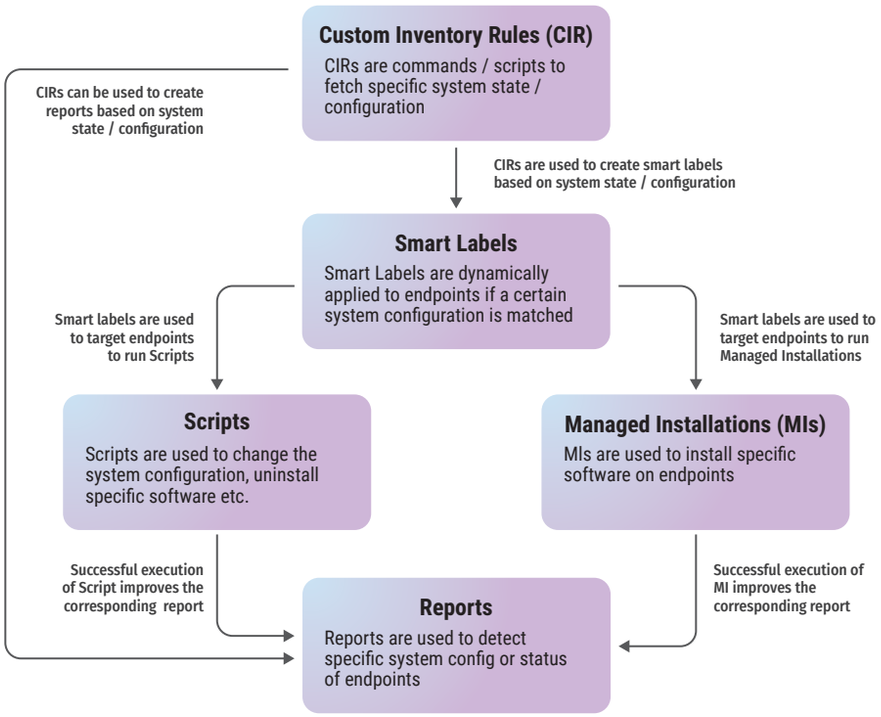
### Proactive Monitoring

Log monitoring at centralized facilities is a standard practise today. It is necessary for monitoring core infrastructure. But it is not so effective for monitoring LAN and EPs due to lack of contextual information. Hence, ministry/department specific contextual monitoring of endpoint and firewall logs is essential. It is proposed to have 1 or 2 dedicated young NIC officers (depending upon load and criticality) continuously monitoring each ministry/department all through the day. They will work closely with NIC-HOD/NO & L1 support engineers to ensure that any threat or incident is duly taken care of. Also, carry out threat hunting by monitoring abnormalities. It is to be noted that they should not be assigned to work on LAN and EP operations, nor supervise operations engineers. They should be allowed to focus on highlighting gaps in compliance, monitoring of logs and threat hunting in their respective ministry/department.

## Continuous and Automated Assessment and Remediation (CAAR)

Cyber security is less about identifying threats and catching malware and more about maintaining posture and compliance of infrastructure. It is less about high flying measure and more about doing the basic cyber hygiene right. An important step towards this aim is system hardening. System hardening is a crucial cybersecurity practice that involves taking specific measures to reduce vulnerabilities and potential attack surfaces in a computer system or network. It's a proactive approach to security, aiming to make systems more resilient against cyberattacks. It is important as it helps in reducing attack surface, enhancing resilience, improving posture and maintaining compliance. Typical system hardening entails the following,

- **Vulnerability Assessment:** Regularly identifying and assessing potential security flaws in hardware, firmware, software, and configurations.
- **Patching and Updates:** Applying security patches and updates to address known vulnerabilities.
- **Configuration Management:** Ensuring proper security settings and configurations, including disabling unnecessary services, closing unused




▲ Fig 10.1 **CAAR Lifecycle**

ports, and adjusting default settings.

- **Removal of Unnecessary Software:** Eliminating programs and services that are not essential for the system's functionality to reduce the attack surface.
- **Access Control:** Limiting user permissions and access to system resources based on the principle of least privilege.
- **Monitoring and Auditing:** Continuously monitoring system activity for suspicious behaviour and auditing security configurations.

The most popular and common technique to implement system hardening is script-based. All the relevant parameters are configured on the endpoint using a PowerShell or batch script in a single execution. The hardening script can be executed on the endpoints either manually on each endpoint or through some delivery system like UEM. The compliance of these hardening parameters are evaluated periodically through audits. The issues with this approach, first, is that if some hardening parameters are modified either by user or APTA utilizing a vulnerability, they can be fixed only after the next audit. The endpoint will remain at risk or compromised till the next audit. Considering the sensitivity and criticality of government data and motivation of APTA, this window of invisibility causes serious risks. Second, if any hardening configuration impacts business function of users, it is cumbersome to troubleshoot, identify and roll-back specific configuration. The quickest possible solution in such cases is formatting of the endpoint which disrupts user functions and causes friction.

▼ **Fig 10.2 : A sample hardening parameter under CAAR framework for configuring NIC DNS server is tabled below for reference**

| NIC DNS | | |
|---|---|---|
| CIR | CIR – Network : DNS Windows | Lists configured primary and secondary DNS Servers (space separated) for network adapters of Windows endpoints |
| Label | @nodns | Device label dynamically applied to windows endpoints where the DNS Server is not NIC DNS Server (1.10.10.10 and 36.50.50.50) |
| Script | Custom – Configure NIC DNS Server | Configures NIC DNS Server on endpoints with label '@nodns' |
| Report | Custom – Endpoints without NIC DNS | Report to list Windows endpoints without NIC DNS Server |

We are proposing a new framework of hardening endpoints, which takes care of the problems of script-based approach, called Continuous and Automated Assessment and Remediation (CAAR). In this approach, the hardening parameters are handled individually or in coherent groups of configuration. Each individual/group parameter is checked on each inventory by UEM through Custom Inventory Report (CIR). If there is a gap then these endpoints are labelled using Smart Labels. Relevant scripts or software installations or uninstallations are triggered based on these labels and remediation initiated. All of these steps are automatic and regular. Ministry / department can get the compliance status on a daily basis through reports. This creates an ecosystem of continuous and automated assessment and remediation of system hardening parameters. It reduces the windows of risk and gives granular visibility of hardening parameters. The advantages of CAAR framework include continuous monitoring, automated remediation, no disturbance for users, roll-back of specific parameter in case hardening affects business functions, regular internal audits, improved posture and compliance, reduced attack surface and overall secure environment. The ownership of the system hardening policy will remain with EPS team and the policy defined by EPS team has to be followed NIC-HOD/NO and their teams. It is important to note that CAAR framework will automatically remediate gaps in hardening parameters in endpoints. However, if some endpoints still remain non-compliant then the issue is mostly with the endpoint itself. NIC-HOD/NO along with the L1 support engineers must get it resolved by visiting the endpoints and running troubleshooting guides.

Government LAN and EP security is unique in terms of resources, requirement and threat perception. Traditional models are not effective in securing them effectively. Hence, there was a need to create a new model and framework which was indigenous and would suit the govt. LAN and EP security requirements better. MOGLES and CAAR were conceived, designed, implemented and successfully tested in various critical ministries and departments of central govt. over a period of two years. They were born in the field and have survived the grind of nation-state APTA in the field. These involve using traditional available technologies and configuring them to suit govt. ecosystem in a novel way. The model is privacy-centric, low cost, autonomous, granular control and provides complete control to ministry/department for their LAN and EP. It is simple and horizontally scalable. It can be easily implemented across various govt. office spread across central, state, district and public-sector.

**Contact for more details**

**Syed Hasan Mahmood**
Scientist -D
NIC HQ, Room#7, A1B6, 5th Floor, A-Block, CGO Complex
Lodhi Road, New Delhi - 110003
Email: hasan@nic.in, Phone: 011-24305379