



# Dynamic NAC Suite Network Access Control

## Zero Network Changes

The Dynamic NAC Suite solution is a full featured, easily deployed network access control solution. The suite provides managed access to the network without network changes and vastly improves device visibility. Endpoints that fail authentication or don't meet security policy are quarantined. Compliant devices used by guests and employees are unaffected and allowed to access the network.

Dynamic NAC Suite is easy to deploy and maintain. By using ordinary computers as enforcers to control access to the network, the suite requires zero network changes. Installations can be done in an hour, compared to most NAC solutions that can take days for even a small network.

The solution continuously monitors endpoint compliance by comparing baseline policy requirements with the endpoint configuration. Dynamic NAC Suite includes checks for patch levels, configurations, and application settings. When the suite finds discrepancies, it quarantines rogues to isolate them from the rest of the network. Policies can be updated at any time to reflect changing requirements.

After identifying a non-compliant device, Dynamic NAC Suite can perform transparent remediation and notify users to reduce load on support staff. If an endpoint configuration is invalid, remediation options can repair the deficiency or walk the user through the process.

## Key Features and Benefits

**Authenticates Users and Guests** before granting access to the network.

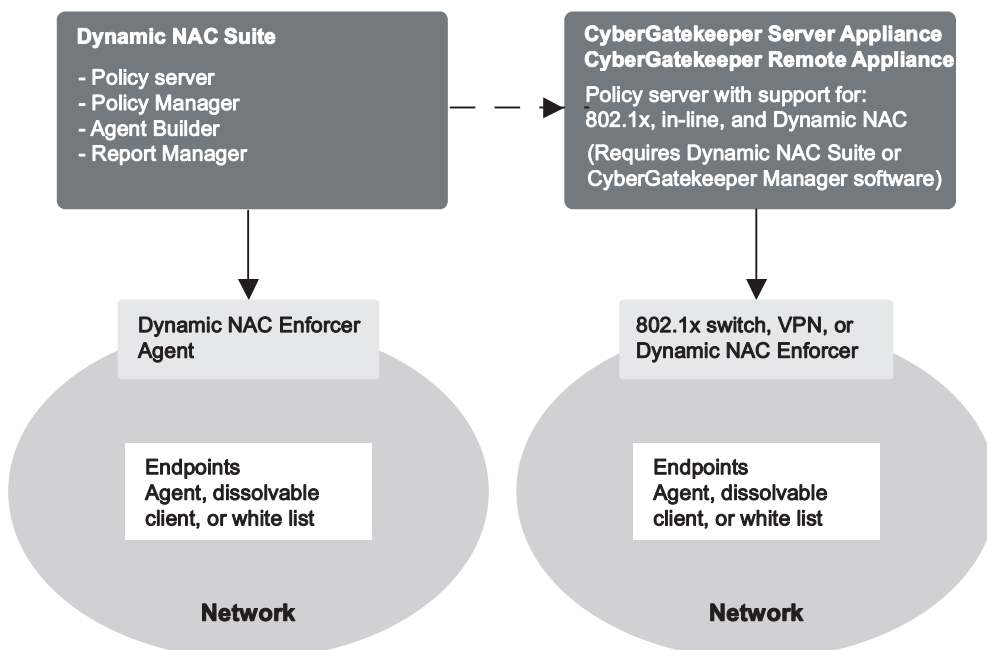
**Quarantines Unauthorized Devices** that are non-compliant or unknown, and remediates unhealthy endpoints.

**Finds Rogue Endpoints** by watching and probing the network.

**Centralizes Management** across multiple servers from a single console.

**Supports Multiple NAC Methods** including Dynamic NAC, SSL VPN, 802.1x, and in-line filtering.

**Works with Existing Networks** including unmanaged and managed switches, routers, and VPNs - all without equipment upgrades.



# Dynamic NAC Components and Specifications

## Zero Network Configuration

### COMPONENTS

#### Policy Manager

The policy manager builds policies specifying valid device configurations and distributes them to policy servers. Policies consist of tests that check operating system and service pack levels, system processes, registry settings, file properties, and other criteria. Tests can be tailored to meet an organization's requirements, and can be associated with custom remediation actions.

#### Policy Server

Dynamic NAC uses ordinary computers as enforcers to control access to the network. The policy server identifies the devices authorized to use the network, and lets enforcers know who should be quarantined. The policy server is part of the Dynamic NAC Suite, and included in the optional CyberGatekeeper appliances. The CyberGatekeeper appliances also support 802.1x NAC, in-line filtering, and other enforcement methods.

#### Report Manager

The report manager collects logs from policy servers and creates reports showing details and summaries of the network. Reports show the number of endpoints in compliance, various attributes, and whether access was granted. Unknown or unauthorized devices are also identified in the reports.

#### Client Software

Client software is available as agents and dissolvable web clients. Agents run in the background at all times, and dissolvable clients run on demand in web browsers. Agents audit with the policy server automatically, remediate misconfigured computers, and can enforce to network access. Agents identify unauthorized devices by communicating with the policy server and can quarantine rogue endpoint traffic.

Dissolvable clients are used by guests and contractors on browsers like Internet Explorer and Firefox. Dissolvable clients participate in audits, but cannot enforce access to the network and do not remediate the endpoint. Dissolvable clients do not require administrative rights and stop running when the browser is closed.

### ENFORCEMENT OPTIONS BY PRODUCT

	Dynamic NAC Suite / GE Windows Software	CyberGatekeeper LAN Appliance	CyberGatekeeper Remote Appliance	Used for...
Dynamic NAC	Yes	Yes		All switches, WLAN, no network changes
In-line Bridge NAC		Yes	Yes	IPSec VPNs, remote sites, NAS
802.1x NAC		Yes		Managed switches, WLAN
SSL VPN Enforcement		Yes	Yes	SSL VPNs from Cisco, F5, Juniper, Nortel
Other NAC Frameworks		Yes		Cisco NAC

## SPECIFICATIONS

---

### **Dynamic NAC Suite Software**

#### **Dynamic NAC Guest Enforcer Software**

Full install requires Windows 2003 Server

Enforcement methods: Dynamic NAC

Includes Policy Manager, Report Manager, client software, and Policy Server

### **CyberGatekeeper Manager Software**

Full install requires Windows 2003 Server

Includes Policy Manager, Report Manager, and client software

### **CyberGatekeeper Server Appliance**

CGS-1000 - 1U Rackmount, single power supply

Up to 10,000 concurrent audit sessions

Requires CyberGatekeeper Manager, Dynamic NAC Suite, or Dynamic NAC Guest Enforcer

### **CyberGatekeeper Remote Appliance**

CGS-1000 - 1U Rackmount, single power supply

Up to 10,000 concurrent audit sessions

Requires CyberGatekeeper Manager, Dynamic NAC Suite, or Dynamic NAC Guest Enforcer

## SOFTWARE

---

### **Policy Server for Windows**

- Windows 2003

### **Report Manager**

- General reports: Compliance by NAS/CGS/OS, daily logs/statistics, access report

- Dynamic NAC reports: Audit and access status for endpoints by subnet

- Windows 2003

### **Policy Manager**

- Audit checks: programs, files, registry, process, libraries, versions, profiles, IP address, operating system, third party applications, antivirus, personal firewall. Plugins to check WMI and other APIs on the PC.

- Windows 2000, XP, 2003

### **Client Software**

- Agent: 1 MB, Windows 98, 2000, XP, 2003, Vista, MacOS X, Linux

- Dissolvable client: Internet Explorer and Firefox on Windows

# Dynamic NAC Suite Network Access Control

Zero Network Changes

## FOR MORE INFORMATION

---

InfoExpress has provided policy-based network access control solutions since 2000. The company's flagship Dynamic NAC product line protects enterprise networks by ensuring the integrity of its endpoints. By keeping unauthorized systems out, Dynamic NAC makes networks safe and productive.

Today, hundreds of network security conscious organizations use InfoExpress technology to secure their networks. InfoExpress products have received numerous awards for their innovation. InfoExpress is headquartered in Mountain View, CA.

For more information, call InfoExpress at 650.623.0260 or contact our sales office at 613.727.2090.