CyberGatekeeper Network Access Control

ZERO NETWORK CHANGES

CyberGatekeeper ensures that all endpoints are compliant with security policies in real-time whether on the LAN, VPN or wireless network. The CyberGatekeeper product line secures networks by keeping out unauthorized devices and ensuring authorized ones remain compliant.

- Extends full-featured NAC to all networked devices such as:
  - desktops
  - laptops
  - servers
  - printers
  - appliances
  - handheld devices
- Monitors endpoint configuration continuously
- Protects network from rogues and intruders
- Isolates non-compliant endpoints from the rest of the network
- Permits seamless network access for compliant devices
- Automatically repairs invalid endpoint configurations
- Supports policies for different system and user classes. Distinguish between:
  - employees, guests, and contractors
  - XP, Vista, 2003, MacOSX, and Linux
  - remote, LAN, and wireless access
  - virtualized and real systems
  - corporate, guest, and home computers
  - pilot users and mainstream users
- Use as standalone NAC or to complement IPS / IDS / patch management
- Helps organizations comply with industry regulations such as SOX and HIPAA

*"Your **network's security** has been our business for over **10 years**."*

Dynamic NAC, CyberGatekeeper's flagship enforcement method, is a full featured, easily deployed NAC solution that manages device access to the network, providing complete visibility and compliance.

- Available in a convenient software package or hardware appliance
- Authentication allows only trusted users to access the network
- Ordinary computers are used as enforcers to control network access
- Requires absolutely ZERO changes to your network
- Installs quickly without reconfiguring network equipment

KEY FEATURES

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

Finds Rogue Endpoints by watching and probing the network.

Centralizes Management of all NAC components from a single console.

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

Works with Existing Networks without equipment upgrades, including unmanaged and managed switches, routers, and VPNs

Authenticates Users and Guests before granting access to the LAN.

infoexpress

COMPONENTS

Policy Server

- Grants access based on endpoint compliance, user authentication, and device identification
- Checks for valid applications, up-to-date versions, proper configuration, hardware, operating system, and more
- Authenticates by Windows accounts and groups without additional login prompts
- Supports multiple deployment scenarios including corporate office, satellite offices, remote users, and wireless access
- Available for Windows 2003 or as a 1U appliance (authentication requires Windows 2003 Server)

Report Manager

- Supports multiple policy servers
- Provides web interface to MS SQL database back-end
- Includes:
  - Overall network compliance level report
  - Detailed endpoint report shows collected software and configuration information
  - Access reports show access granted or reason why access was denied
  - Daily logs/statistics and trend analysis for historical review
  - DNAC network report shows rollup compliance statistics for each subnet, with drill-down capability
- Clearly identifies unknown or unauthorized devices
- Shows colorful compliance graphs by OS, Policy Server, and more
- Reports available even in monitor-only mode
- Runs on Windows 2003

Policy Manager

- Quickly builds policies by specifying valid and prohibited device configurations
- Ships with over 700 predefined tests
- Includes regular updates to test libraries with support
- Distributes policies to policy servers with one click
- Easily customizable tests and policies; new tests and policies are simple to create
- Can associate custom remediation actions for each test
- Runs on Windows 2000, XP, and 2003

Client Software

- Desktop agent and dissolvable (web) agent available
- Desktop agent runs when needed, sleeps when inactive
- Dissolvable agent:
  - Loads on demand in web browsers
  - Is useful for guests and contractors
  - Does not require administrative rights
- Silent install, optional systray icon available
- Automatic remediation for misconfigured or deficient endpoints
- Controls network access using ordinary computers when using Dynamic NAC
- Desktop agent: 1 MB, Windows 98, 2000, XP, 2003, Vista, MacOS X, Linux
- Dissolvable agent: Internet Explorer and Firefox on Windows (excl. Vista)

ENDPOINT DETECTION EXAMPLES

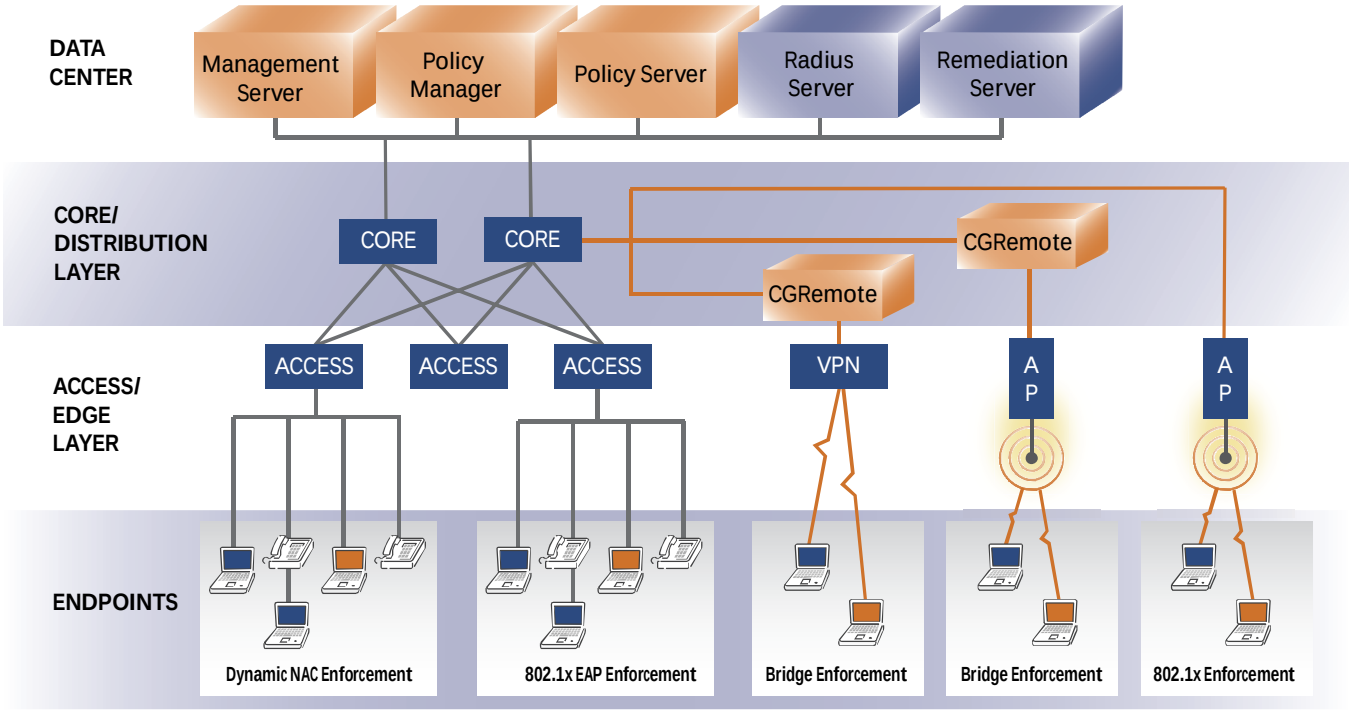
CyberGatekeeper scans endpoints to:

- Detect anti-virus (running, scanning, defs up to date)
- Identify personal firewall (running, in safe policy)
- Mandate Microsoft patches and Service Packs
- Determine Operating System
- Block popular P2P apps
- Discover and block selected high profile malware
- Ensure Windows Automatic Update is enabled
- Provide Windows Security Center integration
- Scan application/system config files
- Detect network settings
- Verify registry keys, values and data
- Detect files on disk, including version, datestamp checksum, and more
- Configure OS and Browser security settings
- Detect running applications/services
- Detect USB mass storage attached
- Detect installed Windows components
- Mandate application versions
- Plus any custom test you create!

BENEFITS

- Ensures business applications vital to your organization's performance and productivity are readily available and working on all desktops. Misconfigured or outdated endpoints are automatically repaired and flagged in reports.
- Continuously monitors endpoints to prevent unwanted, productivity reducing applications from running on user desktops.
- Strengthens network security and policy compliance by ensuring unknown devices (unknown PCs, wireless access points, etc.) are not allowed access to the network.
- Integrates with existing patch management solutions by verifying endpoint posture and automatically updating the system as per the Policy Administrator requirements.
- Ensures desktops are properly equipped with protection and productivity software, and can automatically deploy updates with no user interaction.
- Enforces established connectivity policy by restricting any non-compliant endpoint's access to the network. Does not disrupt vital services like VOIP or helpdesk/operations connectivity to core services. A well designed policy boosts overall machine integrity and availability.
- Ensures Corporate Standard builds are not tampered with in the field.
- Reduces the need for local IT presence where networks are physically dispersed remote locations. CyberGatekeeper ensures corporate assets are used as intended and are not substituted with unauthorized devices.
- Prevents "cross-connectivity" between LAN and Wireless networks by allowing only one connection type at a time.
- Delivers real-time intelligence and continuous assessment. Answering management and auditor questions like "How do you know?" and "How can we ensure PC standards are maintained both in the field and throughout the business?"

ARCHITECTURE



ABOUT INFOEXPRESS

InfoExpress has been in the network security business for over ten years and brought the first network access control solution to the market in 2000. Our large customer base includes many Global 2000 firms and many small to mid-size businesses. InfoExpress products have received numerous awards for their innovation. InfoExpress is headquartered in Mountain View, California with offices in Singapore, the United Kingdom and across North America.

infoexpress

www.infoexpress.com
info@infoexpress.com

HQ 650 623 0260
Fax 650 623 0268

Sales & Support
613 727 2090

UK
+44 (0) 8007 566908

IEX 6.1.383811