CyberGatekeeper

Network Access Control and BYOD Security

CyberGatekeeper provides differentiated network access for mobile devices and corporate PCs so they can safely share the same network. Device access is restricted by identity, device type and policy over WLAN, LAN, and VPN.

Contractors, guests, and employees increasingly need personal and mobile device connectivity to be productive. With CyberGatekeeper enforcing compliance, checking what device is connecting and who is logged in, organizations can embrace Bring Your Own Device (BYOD) while maintaining a secure network.

CyberGatekeeper can also be configured to prevent BYOD.

Compatible with All Devices

- Mobile devices
- Laptops
- Desktops
- Servers
- Printers
- Appliances
- Networking hardware
- VoIP and telephony gear

Improves Productivity

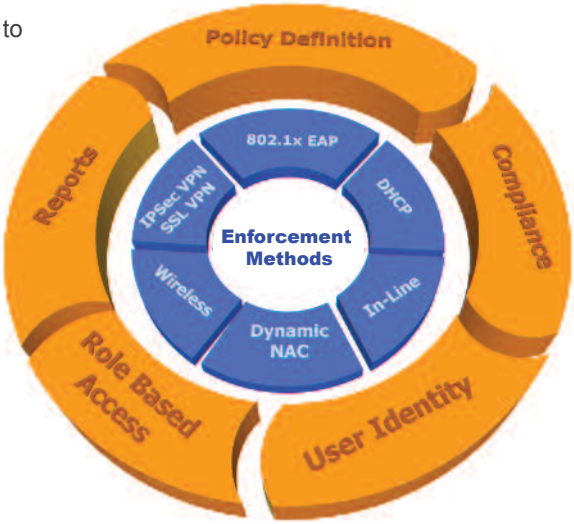
- Ensures endpoint compliance
- Continuously monitors endpoint configurations
- Provides identity-based networking for guests and employees
- Safely enables guest access and BYOD
- Helps comply with regulations like SOX, HIPAA and PCI

Better Security

- Quarantines rogue devices and intruders
- Remediates endpoints with security issues
- Repairs endpoint misconfigurations
- Helps prevent man in the middle attacks

Extensive Audit Policies

- Popular mobile and desktop OSs including Windows, iOS, Android, Mac OS X, and Linux
- Employees, guests, and contractors
- Wireless, LAN, and remote
- Virtual host and guest systems
- Personal devices and corporate endpoints
- Pilot and production users
- Check extensive endpoint characteristics



Enforcement Methods

- Dynamic NAC requires zero network changes by making ordinary endpoints enforcers.
- 802.1x EAP provides standards based network access with identity based networking.
- In-line enforcement supports IPsec, remote access VPNs and site to site access.
- Extensions include direct support for OmniSwitch, Aruba, QIP DHCP server, and Cisco WLC and switches.

KEY FEATURES

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

Finds Rogue Endpoints by continuously monitoring and probing the network.

Centralizes Management of components from a single console

Supports Multiple Enforcement Methods including Dynamic NAC, VPN, 802.1x, DHCP, In-line, and Alcatel-Lucent, Cisco and Aruba CoA.

Avoids Network Changes by using existing network equipment including unmanaged and managed switches, routers, and remote access VPNs.

Enforces Authentication for guests and employees before accessing the network.

Scalable and interoperable with a wide range of networking devices and endpoints.

infoexpress

COMPONENTS

Policy Server

- Grants access based on endpoint compliance, user authentication, and device identification
- Checks for authorized/unauthorized applications, up-to-date software, proper configuration, specific hardware, operating system, policy compliance and more
- Supports multiple deployment scenarios including corporate office, satellite offices, remote users, NAT sites and wireless access
- Available as a hardware or virtual appliance (VMWare ESX Server, Microsoft Hyper-V)

Reporting Server

- Provides web interface to MS SQL database back-end
- Multiple policy servers supported
- Includes:
  - Intuitive 'at a glance' dashboard
  - Network compliance overview
  - Endpoint reports show full audit history and details
  - Access reports show reason access was granted or denied
  - Daily logs and statistics allow 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 compliance graphs by OS, Policy Server, and more
- Reports available even in monitor-only mode
- Runs on Windows Enterprise Server

Policy Manager

- Quickly builds policies by specifying required and prohibited configurations
- Ships with over 800 predefined tests
- Includes free, regular updates to tests and policies
- Distributes policies to all policy servers with one click
- Customize existing tests and policies, or create your own
- Associate custom remediation actions with each test
- Runs on Windows Enterprise Server

Client Software

- Light-weight permanent and dissolvable (web) agents available
- Desktop agent runs when needed, sleeps when inactive
- Silent install, optional systray icon available
- Automatic remediation for misconfigured or deficient endpoints
- Installed agent:
  - Under 6 MB
  - Windows, Mac, iOS, Linux OS, and Android
  - x86 & x64 (32 and 64 bit)
- Supports IPv4 and IPv6
- Dissolvable agent:
  - Loads on demand in web browsers
  - Is useful for guests and contractors
  - Does not require administrative rights
  - Internet Explorer and Firefox on Windows

Authentication Server

- Authenticates by Windows domain accounts and groups without additional login prompts
- Guest access applies ACLs based on AD group membership
- Runs on Windows Enterprise Server

ENDPOINT DETECTION EXAMPLES

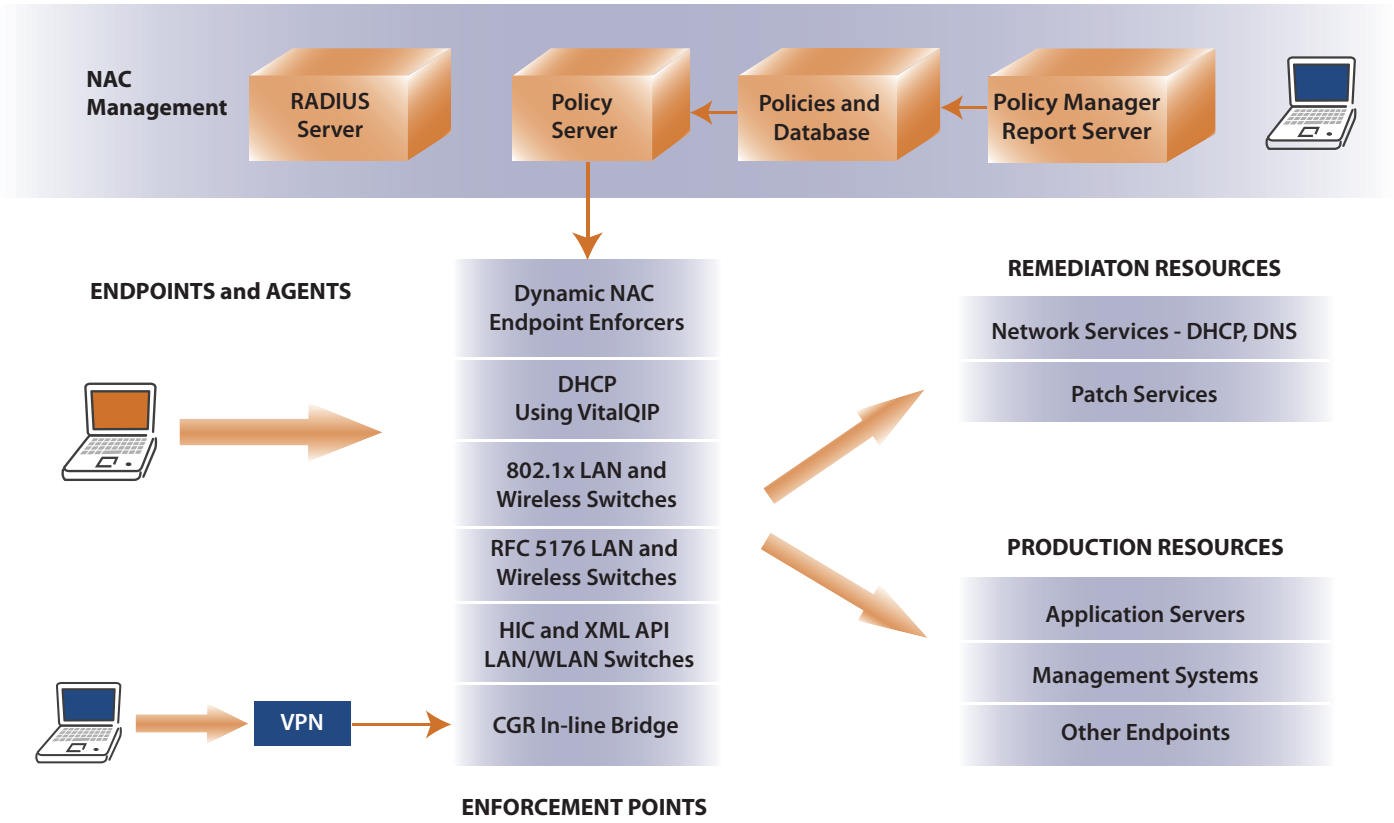
CyberGatekeeper scans endpoints and can:

- Detect anti-virus running with up to date definitions
- Identify properly running personal firewall
- Mandate Microsoft patches and Service Packs
- Detect unsupported operating systems
- Block popular P2P applications
- Discover and block selected high profile malware
- Ensure Windows Automatic Update is enabled
- Provide Windows Security Center integration
- Scan application and system configuration files
- Detect network settings
- Disable wireless NICs when connected to the LAN
- 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
- Ensure software license compliance
- Verify browser and other key application settings
- Plus any custom test you can create!

BENEFITS

- Ensures business applications vital to the organization's performance and productivity are readily available and working on all desktops. Misconfigured or outdated endpoints can be automatically repaired and flagged in reports.
- Continuously monitors endpoints to prevent unwanted, productivity reducing applications from running on user devices.
- Strengthens network security and policy compliance by ensuring unauthorized devices like unknown PCs and rogue access points are not allowed to access the network.
- Integrates with existing patch management solutions by verifying endpoint posture and automatically updating the system according to policy requirements.
- Enables organizations to embrace Bring Your Own Device (BYOD) to cut hardware costs and improve employee productivity without sacrificing security.
- Enforces connectivity policies by restricting unauthorized access to the network while maintaining vital services like VOIP and access to core applications.
- Ensures Corporate Standard / SOE builds are not tampered with in the field.
- Ensures corporate assets are used as intended and are not substituted with unauthorized devices.
- Can prevent "cross-connectivity" between LAN and wireless networks by allowing only one connection type at a time.
- Delivers real-time intelligence and continuous assessment, answering questions like, "Are we sure configurations are maintained in the field and in the office?"
- Ensures desktops are properly equipped with security and productivity software, and automatically deploys updates with no user interaction.

ARCHITECTURE



ABOUT INFOEXPRESS

InfoExpress provides solutions that improve productivity by safely allowing mobile devices and PCs to access resources on the company network. The company has provided the award winning CyberGatekeeper family of Network Access Control products since 2000. The solution ensures endpoints meet security policies with real-time audits and enforces network access for all network-attached endpoints. InfoExpress products have received numerous awards for innovation. The privately held company has been profitable for 13 consecutive years and is headquartered in Mountain View, California. For more information, please visit www.infoexpress.com.

infoexpress

www.infoexpress.com
info@infoexpress.com

HQ +1 650 623 0260
Fax +1 650 623 0268

Sales & Support
+1 613 727 2090

Singapore
+65 9677 1779

IEX 9.0.120529