



LOCKED DOWN. FREED UP.

BLUE RIDGE/SECURE EDGE GUARD AND MICROSOFT NETWORK ACCESS PROTECTION (NAP)

Blue Ridge/Secure EdgeGuard integrates with and extends the NAP framework to enforce endpoint security policies on and off the enterprise across wired and wireless networks, providing full-time protection against malware attacks, data leakage and unauthorized network access.

Extends NAP Controls to Off the Enterprise

Mobile PCs are exposed to considerably more risks than those that remain within the walls of the enterprise. EdgeGuard ensures that practical preventative measures defined by IT personnel to mitigate these risks are continuously enforced on and off the enterprise network.

When off-enterprise endpoints are found non-compliant, EdgeGuard agents can either warn end-users, auto-remediate, or implement a quarantine to protect the host. These actions can supersede end-user administrative privileges to reduce enterprise dependence on end-users making the right security decisions.

Expands Scope of NAP Endpoint Controls

Extremely diverse and sophisticated risks face fixed and mobile PCs. EdgeGuard adds numerous practical preventative measures to counter them. These policies include:

- ensuring that client security software is running and is up-to-date
- reducing exposure to risks by enforcing hardened configuration settings
- regulating what applications may or must run
- plugging potential data leaks via removable media

EdgeGuard Complements NAP with ‘Set and Forget’ Malware Defense

Today’s malware is created by organized cybercrime syndicates that confirm that their attacks will elude traditional client security software defenses. Eventually, these attacks are identified and “fingerprinted” so anti-virus/spyware agents can stop them. Meanwhile, enterprise endpoints are vulnerable.

EdgeGuard thwarts attacks from zero-day (i.e., unknown) malware without any perplexing configuration or the agent asking end-users baffling “what should I do now” questions. It also does not generate an avalanche of false-positives that require highly paid consultants to analyze.

- Expands/extends NAP to fixed and mobile PCs
- Policies supersede users with administrative privileges
- ‘Set and forget’ endpoint defense to zero-day malware attacks
- Plugs data leaks to removable media
- Blocks malware attacks from untrustworthy USB devices and CD/DVDs
- Features custom health check script support
- Quarantines at-risk PCs on or off enterprise
- Renders undesirable applications “unstartable” and required ones “unstoppable”
- Digitally signs logs for irrefutable regulatory compliance audit reporting

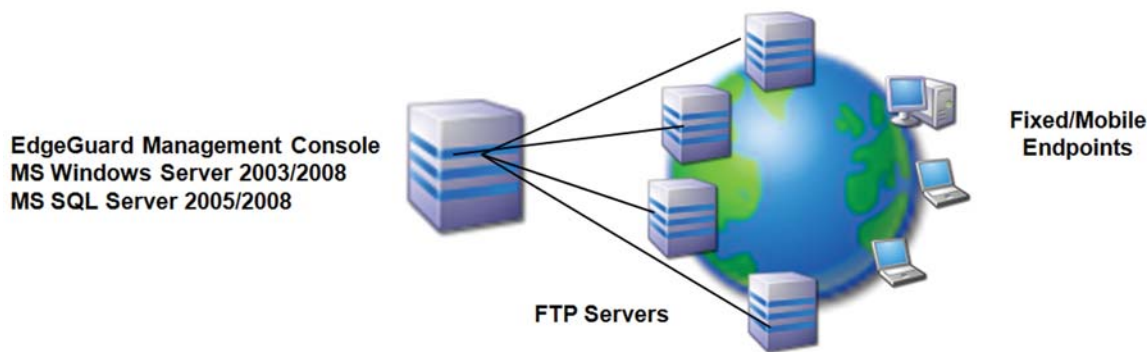


Figure 1: High availability realized with multiple generic servers to distribute policy and collect log data

Features for On and Off the Enterprise:

Endpoint Health Checks

- Client security software enabled and up-to-date
- Microsoft patches implemented
- Applications running
- Configuration settings
- Custom health check script support
 - Assess anything, anywhere, anytime
 - Digitally signed and encrypted

Automatic Remediation and Audit

- Application/service control:
 - Prevent forbidden application or service from launching
 - Automatically launch a required application or service
 - Render a required application or service unstopable
 - Enforce policies regardless of end-user privileges on endpoint
 - Timestamp application and/or service start/stop
- Client security software (anti-virus, personal firewall) optimization:
 - Enable/disable real-time scanning, trigger full scan, update signatures, etc.
- Harden configuration settings (e.g., restrict Internet Explorer ActiveX, Windows Auto-Update enabled, USB/CD Auto-Run, TCP/Syn Flood Protection, etc.)
- Distribute and render application preference files (e.g., Firefox) read-only to disable risky capabilities

Malware Defense

- 'Set and forget' defense to zero-day (i.e., unknown) malware
 - No application-specific tuning, false positives, or user questions
- Prevent executable launches from removable media (e.g., USB drives, CD/DVD)
- Implement workarounds for unpatchable vulnerabilities to PCs On/Off enterprise

Data Leak Prevention

- Block all write operations to USB media
- Disable CD/DVD write operations
- Block read/write operations to network volumes

Off-Enterprise Agent-enforced Quarantine Options

Any combination of the following may be applied to non-compliant PCs anywhere:

- Block Internet access
- Allow access to remediation servers
- Limit VPN access to remediation resources
 - Works with most remote access VPN offerings

TamperGuard

- Malware and administrative end-users cannot alter policies or terminate agent
- Trusted Platform Module (TPM) 1.2 (soft TPM generated otherwise)

Policy Updates and Event Logs

- Policy updates and log retrievals use Internet to reach PCs everywhere, at all times
 - Connections to enterprise not required
 - Encrypted and digitally signed to ensure privacy and authenticity
- Natural disaster recovery and failover
 - Numerous generic servers may be used to exchange policy and log communications between agents and EdgeGuard Management Console to increase system scalability and availability

Rapid Mass Fine-tuning

- Deploy digitally signed and encrypted custom scripts

System Requirements

EdgeGuard Management Console requires:

- Microsoft Windows Server 2008 (NAP requirement), Windows Server 2003
- Microsoft SQL Server 2008, Microsoft SQL Server 2005
- Components may reside on same or separate hosts
- Windows XP/Vista