



BLUE RIDGE/SECURE EDGE GUARD™

Malware outbreaks, data leaks, and attacks on mission critical servers from presumably trustworthy enterprise PCs are causing IT experts to focus enterprise security processes and technologies on the endpoints themselves, at all times, wherever they are. EdgeGuard provides visibility into and control over these endpoints, even when users operate with administrative privileges. EdgeGuard implements policies that reduce risks from malware and data leaks as well as 'set and forget' malware prevention that stops attacks that elude traditional defenses.

Extends Network Admission Control (NAC) Policies to Off-Enterprise PCs

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. EdgeGuard can automatically remediate or confine non-compliant PCs that attempt to access the enterprise. EdgeGuard integrates with Microsoft Network Access Protection (NAP) to protect the enterprise network from unauthorized and/or at-risk endpoints, including guests.

Implements Preventative Measures to Reduce Risks

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

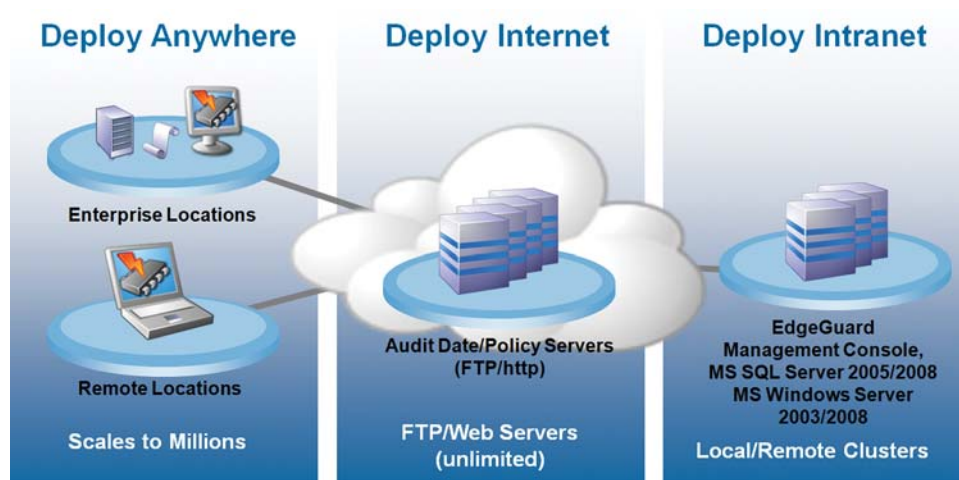
Stops Malware that Eludes Traditional Defenses

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 complex configurations or the agent asking end-users confusing "what should I do now" questions. It also does not generate an avalanche of false-positives that require highly paid consultants to analyze. EdgeGuard also prevents malware infestations by blocking executables from launching from USB drives, CD/DVDs, or network drives.

- Audits and enforces endpoint policies on and off enterprise
- Policies supersede users with administrative privileges
- Defends against malware that eludes anti-virus/spyware systems
- Blocks malware attacks from untrustworthy USB devices and CD/DVDs
- Plugs data leaks to removable media
- Renders undesirable applications "unstartable" and required ones "unstoppable"
- Deploys custom posture assessment and configuration change scripts
- Integrates and complements Microsoft NAP
- Quarantines at-risk PCs on or off enterprise
- Remediate non-compliance issues
- Digitally signs logs for irrefutable regulatory compliance audit reporting

EdgeGuard Architecture and Specifications



Features for On and Off the Enterprise:

Endpoint Posture Assessments and Audit

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

Automatic Remediation and Policy Enforcement

- Application/service control:
 - Prevent forbidden application or service from launching
 - Automatically launch a required application or service
 - Render a required application or service unstoppable
- Client security software 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, 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
- Implement workarounds for unpatchable vulnerabilities to PCs On/Off enterprise

Data Leak Prevention

- Block write operations to removable media
- Block read/write operations to network volumes

Quarantine Options

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

- Block enterprise access
 - Works with existing network infrastructure as is
 - Guest PCs require Microsoft NAP
- 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

Rapid Mass Fine-tuning

- Deploy digitally signed and encrypted custom scripts

System Requirements

EdgeGuard Management Console requires:

- Microsoft Windows Server 2003/2008
- Microsoft SQL Server 2005/2008
- Components may reside on same or separate hosts
- Windows XP/Vista