



LOCKED DOWN. FREED UP.

BLUE RIDGE/SECURE MANAGED EDGE GUARD™

MANAGED SECURITY SERVICE FOR ENDPOINT POLICY ENFORCEMENT

Blue Ridge/Secure Managed Endpoint Protection provides endpoint policy enforcement and protection capabilities as a service. This rapidly deployed service monitors endpoints on and off the enterprise to ensure compliance with the latest corporate security policies. Businesses are able to achieve the benefits of a distributed workforce while cost-effectively eliminating the impact of security risks such as malware attacks and data leakage.

Fastest, Least-Cost Path to Endpoint Protection

Blue Ridge/Secure Managed Endpoint Protection allows you to quickly and easily implement endpoint protection in a phased approach. This approach delivers fast time to value and provides a logical progression to regaining control of your distributed workforce. This unique service offering delivers all of the enterprise class protection benefits without the added burden.

With Blue Ridge/Secure Managed Endpoint Protection you:

- Eliminate the capital expenditures required to implement an endpoint security solution;
- Increase efficiency by allowing personnel to focus on high value activities such as security policy and enforcement versus day-to-day security management tasks;
- Quickly meet compliance mandates through automated audit, reporting and policy enforcement;

Rapid NAC Implementaion

Blue Ridge/Secure Managed Endpoint Protection features Quick Network Admission Control (Quick NAC). While market research organizations report that typical network admission control (NAC) implementations take six to eighteen months, Quick NAC is deployed in days or hours because it requires no upgrades or redesigns of the enterprise infrastructure which saves time and eliminates additional capital expenditures.

Automated Quarantine and Remediation

Quick NAC ensures that all enterprise endpoints are running client security software optimally by automating fixes and remediation. Endpoints identified as potentially harmful, either on or off enterprise, can be quarantined from the enterprise while still allowing for vendor-specific remediation. Endpoints can also

- Audits and enforces security policies on and off enterprise to assure compliance
- Delivers out-of-the-box and custom security policy definitions for flexible deployment
- Protects against malware that eludes anti-virus/spyware providing additional defenses
- Quarantines non-compliant endpoints on or off enterprise to secure network and data access
- Regulates remove-able media access to eliminate data leaks
- Digitally signs logs providing irrefutable compliance audit and reporting

be quarantined from specific threats to prevent malware infestation. This capability reduces IT operations costs by automatically fixing problems that previously required attention from IT and Security personnel. It also reduces malware outbreaks that can take weeks to resolve.

Up-to-date Risk Intelligence

Most organizations lack sufficient endpoint visibility, both on and off enterprise, to accurately assess risks and define sufficient endpoint security policies. Blue Ridge/Secure Managed Endpoint Security generates an array of discovery and audit reports that answer the operational questions most important to IT and Security personnel. Using the intelligence found in these reports, endpoint security policies can be defined to reduce exposure to attacks and data leaks. Further, IT and Security personnel can determine what must be monitored on a regular basis. These reports, which are irrefutable because they are based on digitally signed events captured at the endpoint, automate regulatory compliance reporting necessary to demonstrate efforts that counter “reasonably foreseeable threats”.

Centralized Policy Enforcement

Blue Ridge/Secure Managed Endpoint Protection implements customer-defined endpoint security policies

based on the results of the discovery phase and regularly scheduled audit reports. These policies can help lock-down endpoints, discourage end-users from altering their systems in ways that may harm the enterprise, such as installing non-approved software, and/or quarantine specific endpoints. This centralized, remote enforcement approach reduces the risks to business operations caused by malware outbreaks, network intruders and unauthorized data access.

Microsoft Network Access Protection Policy Enforcement

Blue Ridge/Secure Managed Endpoint Protection is integrated with Microsoft Network Access Protection (NAP). It provides “out of the box” enforcement of NAP policies for endpoints operating on and off the enterprise without introducing duplicate management efforts such as redefining policies in a separate management console.

Powered by Blue Ridge/Secure EdgeGuard™

Blue Ridge/Secure Managed Endpoint Protection is based on proprietary Blue Ridge technology. For over 12 years, Blue Ridge Networks has been providing innovative and highly secure network and endpoint security solutions to organizations that make data security their top priority.

Features:

Audit:

- Client applications/services history
- Ensure client security agents are running, up-to-date, full-scans
- Monitor important configuration settings
- Report patch level compliance
- Digitally sign logs prior to leaving endpoint, providing irrefutable reporting to minimize security risks

Automated Policy Enforcement

- Client security agent optimization:
 - Enable/disable real-time scanning, trigger full scan, update signatures, etc.
- 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 PC
- Modify host settings to minimize security risks
- Data Leak Prevention:
 - Block write operations to removable media
 - Block read/write operations to network volumes
- Malware Defense
 - Prevent malware infestations that anti-virus/spyware miss
 - Block covert malware attacks from USB devices

Support:

- Toll Free 24 x 7 Administrator Support

Quarantine Options

Any combination of the following:

- Block intranet access (works with most remote access VPN offerings)
- Allow access to remediation servers
- Block Internet access

Policy Updates

- Unlimited number of policies supported
- Updates reach endpoints via Internet
- Policies are encrypted and digitally signed to ensure privacy and authenticity

Supported Endpoints

- Windows XP SP2
- Windows Vista