



**LOCKED DOWN. FREED UP.**

# **BORDERGUARD® 5000**

## **OVERVIEW**

The Blue Ridge Networks™ BorderGuard™ secure communications platform defines security for today's widespread and mobile enterprise. There is no better source for ensuring the security of remote offices and remote workers whether they connect to your network via wired or wireline methods.

The BorderGuard 5000 is an enterprise secure communications solution. BorderGuard 5000 enforces compliance to corporate security policies to maximize network performance and reduce exposure to security violations. It quickly and easily scales to meet your needs – regardless of how many users you have and where they are located.

The BorderGuard 5000 is built from the ground up as a highly adaptable modular solution. The BorderGuard 5000 solution provides VPN appliances, clients, and KeyGuard™ two-factor authentication to lock remote devices down to your network. Plug and play capability means that the BorderGuard 5000 line is pre-configured for rapid deployment, easy to install and use, and modify to meet your requirements.

With advanced features, such as the pre-login client, Tunnel-Lock™, and a central management system, BorderGuard 5000 handles any remote network environment. Seamless Wi-Fi roaming means that devices resume secure VPN sessions after periods of poor wireless coverage without requiring the client to re-login.

### **THE BORDERGUARD 5000 PRODUCT SUITE COMPRISES:**

- VPN Appliance
- Client
- KeyGuard Two-Factor Authentication
- Management Console

- Strong Public Key Authentication
- Built-in Digital Certificates
- Secure Pocket PC Clients
- Remote Access and Site-to-Site VPNs
- DoD SPOCK, FIPS 140-2, and Common Criteria Certified
- Service Level Agreements

## MAXIMUM SECURITY AT A FRACTION OF IN-HOUSE VPN SOLUTIONS

### THE BORDERGUARD 5000 PRODUCT SUITE

- Built-in digital certificates for the strongest form of authentication
- Saves time and reduces the cost of digital certificate registration with registration authority and authentication server in one box. No RADIUS or SecurID ACE server required, thereby significantly reducing total operating costs and eliminating man-in-the-middle attacks
- Credential management system for two-factor authentication
- Closed system: No external user controls or access
- Redundancy for VPN Appliances and Internet connectivity to ensure maximum availability for missioncritical applications and protection against Denial of Service attacks
- Easy integration of existing security devices with extensible APIs

### CLIENT FEATURES

- Pre-login provides streamlined registration, authentication, and access
- Tunnel Lock enables:
  - Remote site user and wireless access “lock-down” to the corporate network through your corporate firewall. Preventing company computer and Internet misuse
  - Improvement in security compliance by controlling access to illegitimate networks and restricts repeated re-infection from worms and viruses
  - Reduction in the cost and complexity involved in security enforcement
- Supports mandatory mutual authentication via digital certificates for ease of use and best-of-breed security
- Encryption and encapsulation of delivered data provides privacy and data integrity
- Integrated telephone book and dialer option

### KEYGUARD TWO-FACTOR AUTHENTICATION

Blue Ridge Networks two-factor authentication delivers a much more effective level of user authentication than password-only solutions. By requiring multiple proofs of identity—in this case something you know (a password) and something you have (a token diskette or USB KeyGuard)—it ensures that only authorized users have access to your network.

### MANAGEMENT CONSOLE FEATURES

A key part of organizing and controlling secure communications is managing the process by which security policy is created, approved, and then published. The Management Console, with its intuitive graphical user interface and simple-to-use configuration tools, allows quick and easy:

- Central site secure management of your remote user software and security policy
- Creates, securely distributes, and revokes digital certificates
- Real-time, comprehensive audit trail for access, and security alarms for violation attempts. Time stamps assist in forensic analysis
- Alarm monitoring (e.g., VPN appliance tampering, unauthenticated access attempts, Denial of Service attempts)
- Network administrators can:
  - Define all employees network access to content that match your processes
  - Monitor the status of the corporate network related to the BorderGuard 5000–powered sites
  - Enable real-time user revocation

With the BorderGuard 5000 you can rest assured that your network is secure, your assets are protected, and your security policies are enforced.