EdgeGuard®
Datasheet

Protect your Network from Endpoint Threats

EdgeGuard addresses the needs of an increasingly mobile workforce by protecting critical enterprise operations from potential malicious software on un-trusted and un-managed endpoint devices. With EdgeGuard, end users can navigate securely to company resources located in the cloud, data center, or corporate offices, turning any device (including personal devices) into a trusted terminal. It also does not allow any file copies to local devices or storage, making it ideal for preventing information exfiltration.

EdgeGuard can be deployed as a singular solution or as part of a defense-in-depth approach. Nothing that resides on the user system can cross over to the "trusted" network. Nothing from the "trusted" network can cross to the user system. EdgeGuard can also be deployed as a bootable (Boot EdgeGuard) or an installed (Virtual EdgeGuard) solution. Both solutions integrate seamlessly with VMware, WMware Horizon Client, and Citrix.

Boot

EdgeGuard is a stateless, portable, secure thin client fully contained on a USB token. The USB token contains a bootable host operating system (OS), a customized virtual desktop, and utilities that download the environment directly into computer memory rather than installing it to a hard or solid-state drive. Boot EdgeGuard incorporates two-factor and mutual public key authentication for BorderGuard trusted network connections and secure access to the remote network. Nothing is installed on the host computer so nothing remains of the session once the Boot EdgeGuard USB token is removed.

Virtual

EdgeGuard is deployed as a Windows installable software package that creates a stateless thin client and enables two-factor and mutual public key authentication for BorderGuard trusted network connections. After the software is installed, inserting an EdgeGuard USB token triggers establishment of a Virtual EdgeGuard session that uses separate memory space and is isolated from the underlying host. This results in the ability to simultaneously use the native OS and secure thin client access to a remote network. The remote network remains protected because no drag and drop, copy/paste or other interactions are allowed between the secure EdgeGuard portal and the underlying desktop, so no data or malicious code is transferred.

Feature	Boot EdgeGuard	Virtual EdgeGuard
Product Format	USB Thumb Drive or CAC/PIV Device	Installed Software Activated by Secure Token
Remote Desktop	RDP Client	RDP Client
VMware Support	VMware Horizon Client	VMware View Open Client
Citrix Support	Citrix Receiver in ISO, Connect using Firefox Plug-in	Citrix Receiver in ISO, Connect using Firefox Plug-in
Web Browser	Anonymous Web Browsing Firefox Supported	Anonymous Web Browsing Firefox Supported
CAC/PIV and SecureID	Fully Supported	Fully Supported
VPN Support	Blue Ridge VPN Native Compatible with majority of other VPN types including Cisco, Citrix, and Juniper	Blue Ridge VPN Native Compatible with majority of other VPN types including Cisco, Citrix, and Juniper
Wireless (Wi-Fi) Access	Fully Supported	Fully Supported
3G/4G Cellular Access	Not Supported	Fully Supported
Security Block of Local Printing	Fully Supported	Fully Supported
Anonymity of User Location	Fully Supported	Fully Supported
PC Platform Support	BIOS Supporting USB Boot	Windows 7, Service Pack 0 and above Windows 8, 8.1, and 10
HW Platform Support	**Minimum Requirements:** 1 GB or more of RAM Wired or Wi-Fi connection 1.6 GHz or higher 32-bit capable processor Display Resolution: 800 x 600	**Recommended:** Core 2 Duo ≥ 1.8 GHz or better Display Resolution: 1024 x 768 **Minimum Requirements:** Pentium 4 w/hyper-threading enabled ≥ 2.4 GHz 2.00 GB of RAM 200 MB of free hard drive space

BlueRidgeNetworks.com | 14120 Parke Long Court, Suite 103, Chantilly, VA 20151 | sales@blueridgenetworks.com | 1.800.722.1168

EdgeGuard®

DATASHEET

Secure Remote Access...Anytime...Anywhere

EdgeGuard's isolation and containment features provide employees with secure, thin-client access to their corporate desktop from any location. You can be confident that no data leaves the corporate network and no malware sneaks in through the connection.

Allows Use of Employee-Owned Devices

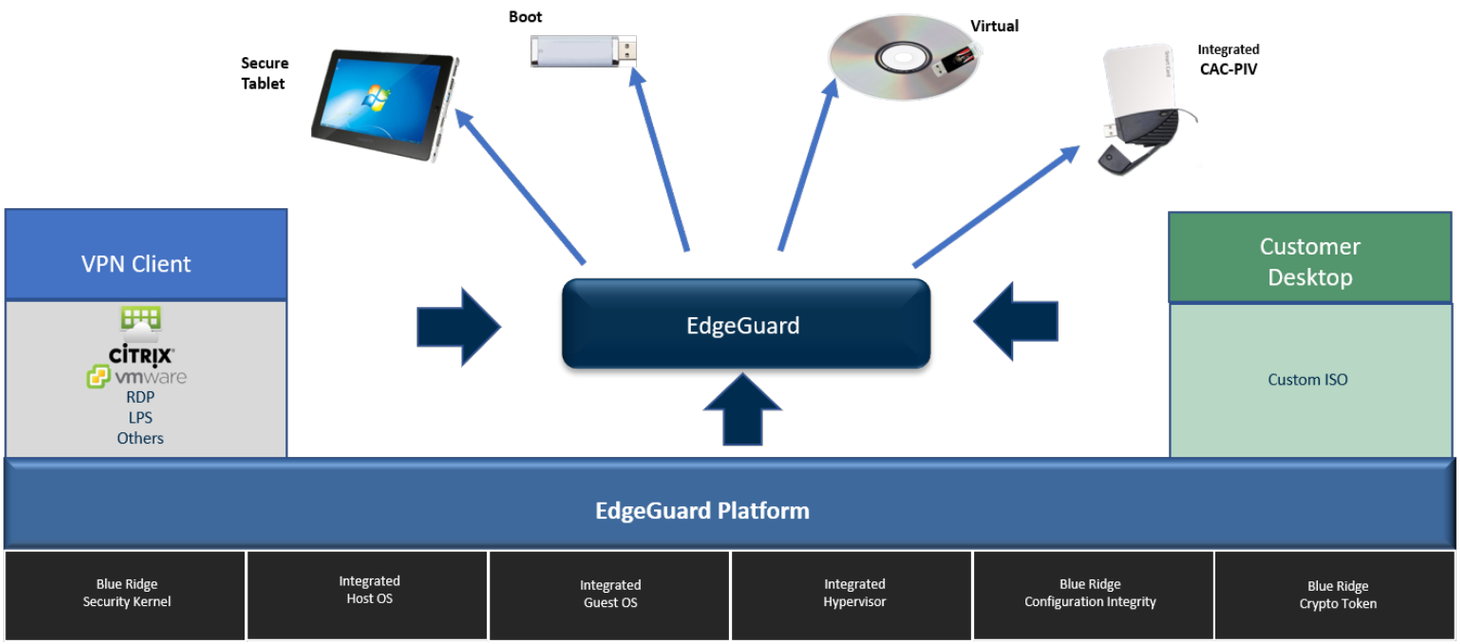
Use EdgeGuard to isolate and secure connections from non-enterprise owned or maintained devices, such as a home computer or BYOD. This approach protects the corporate network from the transfer of malware and prevents exfiltration of enterprise data. The employee uses EdgeGuard to ensure a secure connection. When their work is complete the EdgeGuard token is removed, returning the computer to its original state with no trace of the connection.

Supports Extranet Collaboration

Provides remote employees and third-party vendors with secure access to corporate extranet environments while protecting business-critical files. EdgeGuard ensures that only approved and authenticated users can access restricted files, while limiting their ability to write, print, or download such data.

Isolates Internet Browsing

Gives authorized users a specific path to remotely browse Internet sites typically blocked by firewalls, such as social media networks or sites that may be infected by malware. Using EdgeGuard isolates Internet activity and prevents the transfer of malware to the corporate network and blocks data leakage. EdgeGuard allows employees to securely access any site, via a protected, secure tunnel.



About Blue Ridge Networks

Based in Northern Virginia, Blue Ridge Networks is a visionary cybersecurity pioneer that provides autonomous cybersecurity for the connected world. Blue Ridge Networks' Autonomous Cybersecurity suite protects organizations from vulnerabilities posed by connected devices, endpoints, networks, and people. Blue Ridge Networks solutions have protected critical operations for some of the largest US government, financial, healthcare, and other critical infrastructure customers for more than twenty years with no reported breaches.

1-800-722-1168

sales@blueridgenetworks.com

14120 Parke Long Court, Suite 103
Chantilly, VA 20151

EG-001-DS Rev. B