



EdgeGuard Overview

EdgeGuard provides secure access to enterprise resources located in the cloud, data centers, or corporate offices. It protects the enterprise from potential malicious code on the user's computer and prevents the export of internal/private information by that computer.

EdgeGuard is unique because it authenticates and isolates the remote access session before allowing execution of the user authentication method used by the enterprise, including CAC/PIV, SSL, and VPN. EdgeGuard prevents password and user identity theft, spying and theft of data, and piggyback penetration of the enterprise through an unauthorized and unprotected tunnel. EdgeGuard works by isolating the endpoint so that no malware can enter the secure tunnel it creates with the BorderGuard.

EdgeGuard converts an off-the-shelf laptop or desktop computer to a virtualized trusted thin client terminal, enabling wired or wireless trusted sessions from any device. With the Boot version of EdgeGuard, an enterprise can re-purpose legacy laptops to create a thin client that will improve battery life and increase processing time. EdgeGuard prevents "WikiLeaks" type of data leaks by isolating operations from the host device.

EdgeGuard provides the user with a virtual desktop that can be configured with a web browser, VDI solutions from Microsoft, VMware, Remote Desktop to the user's corporate desktop or a Terminal Server, and Citrix.

EdgeGuard Form Factors – Boot and Virtual

BOOT EDGEGUARD

Boot EdgeGuard is a stateless, portable secure thin client fully contained on a USB crypto device. It contains the bootable host operating system and virtual desktop customized for the enterprise. This crypto device will boot on most computers that can boot from a USB device. This is not a storage device: nothing can be written to it.

USING BOOT EDGEGUARD

The user inserts a Boot EdgeGuard Security Token into a USB port, restarts the computer, and boots from the USB device. Following a successful validation of a password prompt, the user verifies either WiFi or wired connection information. Boot EdgeGuard then creates a virtual desktop that securely connects to a remote Home Network (enterprise cloud resources, or the customer's internal network). When the USB device is removed, the connection to the remote Home Network is terminated and the host computer will reboot. No information is left on the host computer or on the EdgeGuard token.

VIRTUAL EDGEGUARD

Virtual EdgeGuard includes software installed on Windows PCs to provide a stateless thin client. When an EdgeGuard session is started, it uses a separate memory space and is completely isolated from the underlying host. The enterprise remains protected because the desktops (local vs. Virtual EdgeGuard) are completely isolated from one another and no data or malicious code can cross between them. There is no drag and drop, copy or paste, or other interaction allowed between the secure portal and the underlying desktop. The Virtual EdgeGuard configuration is protected from alteration by malware or local admin users by Blue Ridge's proprietary AppGuard security controls.

USING VIRTUAL EDGEGUARD

When the user inserts a Virtual EdgeGuard Security Token into a USB port, the Virtual EdgeGuard application will prompt for a PIN. Once the PIN is validated, Virtual EdgeGuard creates a virtual desktop that securely connects to a remote Home Network (enterprise Cloud resources, or the customer's internal network). When the Security Token is removed, the connection to the remote Home Network will be terminated and the virtual desktop will be closed.

Example EdgeGuard Solutions

Remote Access to Corporate Desktops

Problem: Employees require access to their corporate desktop from unknown locations, anywhere, any time.

Solution: The **Boot** and **Virtual EdgeGuard** virtual desktop includes an icon for access to the employee’s desktop. All work is done on the corporate network; no data will leave that network, and no malware will sneak in.

Healthcare – Remote Access from Non-Enterprise PCs

Problem: A healthcare company needs to allow a doctor's personal computer access to its systems in order to review patient's health records, x-rays, schedules, and other private medical data. Since these are not corporate-owned or maintained devices, the healthcare company cannot guarantee that the doctor's computer is malware-free and can protect patient information.

Solution: Doctors using **Boot EdgeGuard** can use any convenient computer for access to patient information. Once the EdgeGuard device is removed, the computer is returned to its original state with no trace of the connection left behind and the healthcare enterprise is safe.

Civilian Government – Extranet Collaboration

Problem: A Government agency must provide access to case files to a large number of attorneys, law enforcement organizations, and subject matter experts. It is critical that no information is removed from the secure centralized data center where the digital case files are housed.

Solution: **Boot EdgeGuard** enables “extranet” users to access case files. EdgeGuard's authentication ensures only approved users are able to get into the systems. Restricting data from being written to the device or even printed eliminates the chance of data leakage.

Safe Internet Browsing

Problem: Executives and other individuals need access to social network Internet sites from the corporate network, but these sites are blocked by the corporate firewall. Facebook and YouTube are generally blocked by corporate firewalls to keep malware out and prevent data leaks.

Solution: Employees use **Virtual EdgeGuard** to connect to an offsite **BorderGuard** with unrestricted Internet access. Employees can use the browser on their EdgeGuard desktop to securely access any website. Malware cannot infest the device or the network, nor can it compromise any data on the host PC.

EDGEGUARD FEATURES

Feature	Boot EdgeGuard	Virtual EdgeGuard
Remote Desktop	RDP 6.0 Client Included	RDP 6.0 Client Included
VMware View	VMware View Open Client Included	VMware View Open Client Included
Web Browser	Anonymous Web Browsing Firefox supported	Anonymous Web Browsing Firefox supported
CAC/PIV	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 (WiFi) 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 XP, Service Pack 2 and above (32 Bit). Windows VISTA, Service Pack 0 and above (32 and 64 Bit). Windows 7, Service Pack 0 and above (32 and 64 Bit). Windows 8, Windows 8.1 (32 and 64 Bit).
PC HW Platform Support	Min: 1 Gig or more RAM Min: Wired or WiFi connection Min: 1.6 GHz or higher 32-bit capable processor Min: Screen Resolution 800x600	Recommended: Core 2 Duo (>=1.8Ghz) or better; Recommended: Display resolution 1024 x 768 (or larger) Min: Pentium 4 with hyper-threading enabled (>=2.4Ghz) Min: 2.00 GB of RAM; Min: 200 MB free Hard Disk space