



BLUE RIDGE/SECURE PIXIE ENTERPRISE™

Use Any PC for Local/Remote Computing Without Malware or Data Leakage

Insert and Boot from Pixie



Isolated from Malware on PC and Locked-Down from Abuse/Mistakes

None of the Risks of SSL VPN



Immune from Network-Based Attacks (Man-in-the-Middle, DNS Poisoning, etc.)

Secure Access to Resources



Limit what End-users May Access, Block All Risky Actions that might Leak Data

Eliminate Enterprise and Cloud Computing Data Leak Challenges

Endpoint Data Leakage



Telework on Home PC's



Security Breach Headlines



Constrained Capital Budgets



Intellectual Property Theft



Rootkit/Botnet Risks



Pandemic Preparedness



Online Banking Trojans



Insider Threats



Pixie Incorporates Patented Security Technology Developed to Overcome Limitations of Legacy SSL VPN, IPsec VPN, and Personal Computer Security

Pixie: USB Virtual Computer Provides a Clean, Secure Working Environment

When Pixie boots up from a computer, the computer's system hard drive as well as any other drives are rendered dormant while Pixie runs, without altering the host. Users enjoy the computational resources of the host computer without any of its inherent risks. Pixie administrators define the desired user-experience in terms of guest operating system, client-side applications (Firefox, rdesktop, etc.), as well as device control and application settings. Administrators may choose security options that prevent file transfers to removable media, site-lock one or more web browsers, snuff-out drive-by download attacks, and/or restrict network file transfers. The contents of Pixie are cryptographically fortified to prevent unauthorized changes. Neither malicious web content, tainted documents, spiked multimedia files, nor determined, sophisticated end-users will alter Pixie. With each launch, it provides a pristine, secure working environment on any PC with BIOS, located anywhere, without any extra hardware or cables.



With Pixie	Any PC	Without Pixie
✓	CPU	✓
✓	RAM	✓
✓	NIC	✓
✗	USB	✓
✗	CD/DVD	✓
✗	Hard Drive	✓

Pixie Disables Sources of Malware and Data Leaks on it's Host Computer

Pixie: Isolates Host Computer from Potentially Hostile Local Network, Securely Connects to Enterprise

UnDNS poisoning, replay, man-in-the-middle, key exchange protocol, and all other potential forms of attack on the host computer from the local network would fail. Confidentiality and data integrity are assured. The virtual workspace provided by Pixie runs atop a virtualized appliance that cryptographically isolates Pixie from the local network and logically connects the virtual computer to the remote, trusted network by encrypting all of its inbound and outbound Ethernet frames, rejecting all others. This virtual force-field and tunnel are formed via an advanced key exchange process embedded within a mutual PKI-authentication process that has been in use for over a decade without any reports of vulnerabilities.



Pixie Benefits

- Safely leverage 3rd party PC's, reduce capital expenses
- Reduce IT operations costs via simplified computer support and slashed trouble ticket volume
- Avoid fraudulent bank transfers, credential theft, etc.
- Purge data and intellectual property leakage and malware caused security breaches
- Boost data inventory/audit, legal discovery
- Withstand disasters and pandemics

About Blue Ridge Networks

For over 12 years Blue Ridge Networks has helped commercial and government customers securely conduct business despite network and endpoint security risks. Our solutions have consistently proved effective and practical in terms of risk mitigation and total cost of ownership. Blue Ridge Networks solutions represent high standards of security as evidenced by numerous government certifications and compliance with key industry standards.