



## Why ZeroPort?

ZeroPort delivers secure remote access solutions that are hardware-enforced to ensure that networks remain un-breached, data stays locked down, and threats have nowhere to go. No leaks, no attack surface - just secure access without compromise.

## Main Use Cases

- **3rd-Party Vendor Access**  
Controlled & monitored access for external vendors ensuring sanctioned and isolated time-limited access.
- **Hybrid Workforce.**  
Expand your perimeter to encompass remote work without risk, while securing access to sensitive corporate environments.
- **Infrastructure ICS & OT**  
Maintain air-gapped security while enabling controlled remote operations and connect IT to OT securely.
- **Public Sector**  
Removing the barriers of access to secure databases, government systems and national infrastructure.
- **Defense & HLS**  
Classified and sensitive networks, forensics & investigation systems retain absolute isolation while enabling remote access.

# Expand Your Perimeter with Malware-Proof Remote Access

## Introducing Fantom

The first non-TCP/IP remote access solution  
for real-time, latency-free work

## The Threat Landscape

As organizations expand remote connectivity, traditional VPN's and cloud-based tools are fraught with vulnerabilities risking:

- Credential Theft & Phishing Attacks
- Ransomware & Malware Spread
- Data Leakage & Corruption

These risks demand a malware-proof solution that provides real-time remote access while truly eliminating these vulnerabilities.

## The Future of Remote Access Security

Fantom redefines secure remote connectivity by providing:

- Non-TCP/IP Connectivity.
- Hardware-enforced to physically prevent risks.
- Real-time work with no-latency and unlimited scale.

## Fantom Main Features

- 200 concurrent user connections per system.
- Fantoms can be stacked for unlimited scale.
- MFA & session monitoring included.
- Standard rack-mount configuration.
- Zero-touch, no downtime deployment.

