CYBER SECURITY—CYBER BUBBLES—CYBER SILENCE

CYLENTIUM builds proven end-to-end Certified Layer 2 encryption software and security platforms.

Specifications

- FIPS & EAL4 certified Cryptography

- Encrypting network traffic at Layer 2 using FIPS 140-2 approved algorithms in a software-only solution.

- Encryption of packets at layer 2 protects more network protocols and makes the topology and details of the network un-snoop able.

- Fully Functional LAN emulation - Cryptographically secure remote computing

- Extends hardened enterprise "Edge" perimeter to include remote users, mobile, wireless, and wired

- Dynamic expansion capability that is unlimited in territory coverage

- Supports 802.1x, 802.1ae, and other advanced security standards and algorithms

- Support all Layers 3 and above

- Support advanced routable Tunneling

- Advanced VPN Protocol is 7 times faster than current industry performance

- Advanced Endpoint Protection

- Certified Cisco, Juniper, Aruba, Extreme, Checkpoint

- Certified Army & Navy Research Labs

- Certified Defense Information Systems Agency (DISA); Department of Defense (DoD); Department of Energy (DOE); Department of Defense(DnD); Department of National Defense Canada (DND)

CYBERSECURITY BUBBLE TECHNOLOGY

CYLENTIUM's strategic mission and function are to protect the wireless and ethernet networks from visibility, detection and penetration.

Cylentium does this by enveloping the environments with cybersecurity "Bubbles".

Cylentium hardens the environments in a "Non-Detectable", "Non-Penetrable", encrypted environment, protecting network traffic using FIPS 140-2 military approved algorithms and deeply sophisticated authentication, in a software-only solution. Cylentium validates client conditions and states before allowing access and usage and monitors behaviour and patterns to ensure absolute cybersecurity compliance.

Cylentium can be embedded in organizations or manufactures existing equipment, routers, switches, bridges, and devices.

Or, it can be deployed as a Cylentium certified standalone device. The Cylentium access devices can be dynamically deployed to expand Bubble coverage to any imaginable size – from a cell phone to a city and beyond.

Cylentium Research is developing new AI and Machine Learning -based pattern detection that will also allow detection and prevention of data intrusion, data leakage, and malicious packet flow.