CYLENTIUM

DATA SHEET v4.3

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)

The Challenge

Security can be divided into two main models. First, there is the model where clients can enter the network based on the current standards. We call this the ***Unverified Trust Client Model***. The client is permitted to connect and—with relatively simple one-way authentication—can join without much prior engagement. The client may have even joined other networks which may have been unprotected or under-protected.

This model has the benefit of simple set-up, but any device supporting the standard and can satisfy authentication can join. Maintenance of the client is a simple (perhaps even non-existent), but the compromise is in security of the overall network. The device can introduce vulnerabilities. The device can be out of compliance in many ways. Many current components also support IP or MAC-based authentication to the device, but IP and MAC spoofing are incredibly simple and well-known attacks.

The second model is what we call ***The Verified Trust Client***. CYLENTIUM'S models involve several layers of device and user authentication. It requires a client to be installed, but prevents many of the spoofing attacks. It also requires that each client pass several other role-based and enterprise-based rules (such as successful validation of completion of virus and malware scanning). We have trademarked this client behavior as *NetQuarantine*. If the device is not authenticated, in compliance, and safe, the client will not allow the device to infect or introduce risk into the rest of the network.

The Solution

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 provides a client application that runs independently and intercepts network traffic from the local operating system and applications and encrypts the information at Layer 2 for transmission to the CYLENTIUM Server where it can be routed to other clients.

Specifications

- Strong, certified Layer 2 encryption.
- Standards-based network components
- A strong network firewall driven by policies defined by administrative direction & machine learning
- Anti-virus and encryption of data-at-rest ensure required client state
- Integration with LDAP, MS Exchange, and RADIUS based servers to allow enterprise management and administration
- Anomaly detection
- Context-based data leakage protection -
- Network quarantine
- Rules based engine
- Protection encapsulated in a proven FIPS 140-2 certified layer 2 security
- Rotating encryption keys
- True end-to-end protection at scale
- Packet Authentication
- API's for plug-ins

Incoming encrypted traffic is decrypted by the client and passed back to the local operating system and applications through the normal network connection. No API or active participation is required from the local operating system or applications. Non-encrypted network traffic is rejected by the client and server alike on the encrypted portion of the network.

CYLENTIUM uses the encryption server as the interface between the outside world and the encrypted portions of the network. Standard protective measures (whether AI or standard rules-based firewalls) are expected as a front end to prevent any threats from reaching the exposed unencrypted inputs to the encryption server. CYLENTIUM provides the other half of required protection by preventing threats from being injected to the local network via network penetrations. Prevention of unauthorized users providing valid credentials is left up to the local operating system and applications.

Since CYLENTIUM is a stand-alone application, there is no public Application Programmer Interface (API), but there is a private API.

Benefits

CYLENTIUM provides a client application that runs independently, enforcing correctness rules at the edge and intercepts network traffic from the local operating system and applications and encrypts the information at Layer 2 for transmission to the network bridge where it can be routed to other clients. Incoming encrypted traffic is decrypted by the client and passed back to the local operating system and applications through the normal network connection. No API or active participation is required from the local operating system or applications. This provides true end-to-end protection in a larger set of use cases than classic enterprise networking.

Because CYLENTIUM is designed and built as a software bridge, the software can be deployed in many complex architectures and topologies.

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

Or it can be deployed as a Cylentium certified access point. The Cylentium access devices can be dynamically deployed to expand our Bubble architecture and coverage to unlimited coverage. From as small as 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 Threat Actor behavior.