CYLENTIUM
WIRELESSWALL

CYBER SECURITY CLOAKING BUBBLE TECHNOLOGY

Who is Cylentium WirelessWall?

CYELNITUM Inc. is a new Cyber Security Technology start-up, reintroducing a mature innovative wireless cybersecurity built on Cloaking Bubble Technology conceived 14 years ago at the United States Naval Post Graduate School, Monterey

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

Who is Cylentium WirelessWall?

A New Cyber Security Company launching an established mature product and technology

- The technology is the brainchild Dr. Dennis Volpano, Professor US Navy Post Graduate school
- Technology originally developed in as a private venture in 2000 for, and in cooperation of the U.S. Navy.
- The strategic mission of the technology was to provide secure, mobile shipboard networks that were non-detectable and non-penetrable.
- With Independent validation & verification achieved:
  - 1st FIPS 140-2 WLAN certification, March 2003
  - Common Criteria process started February 2004

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

Cyber Security Cloaking Bubble Technology

CYLENTIUM's strategic mission and function are to protect wire-less and ethernet networks from visibility, detection and penetration

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 behavior 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’s Micro Segmentation Technology enables fine-grained security zones & security policies to be assigned from cloud & data center applications, down to the micro workload levels.

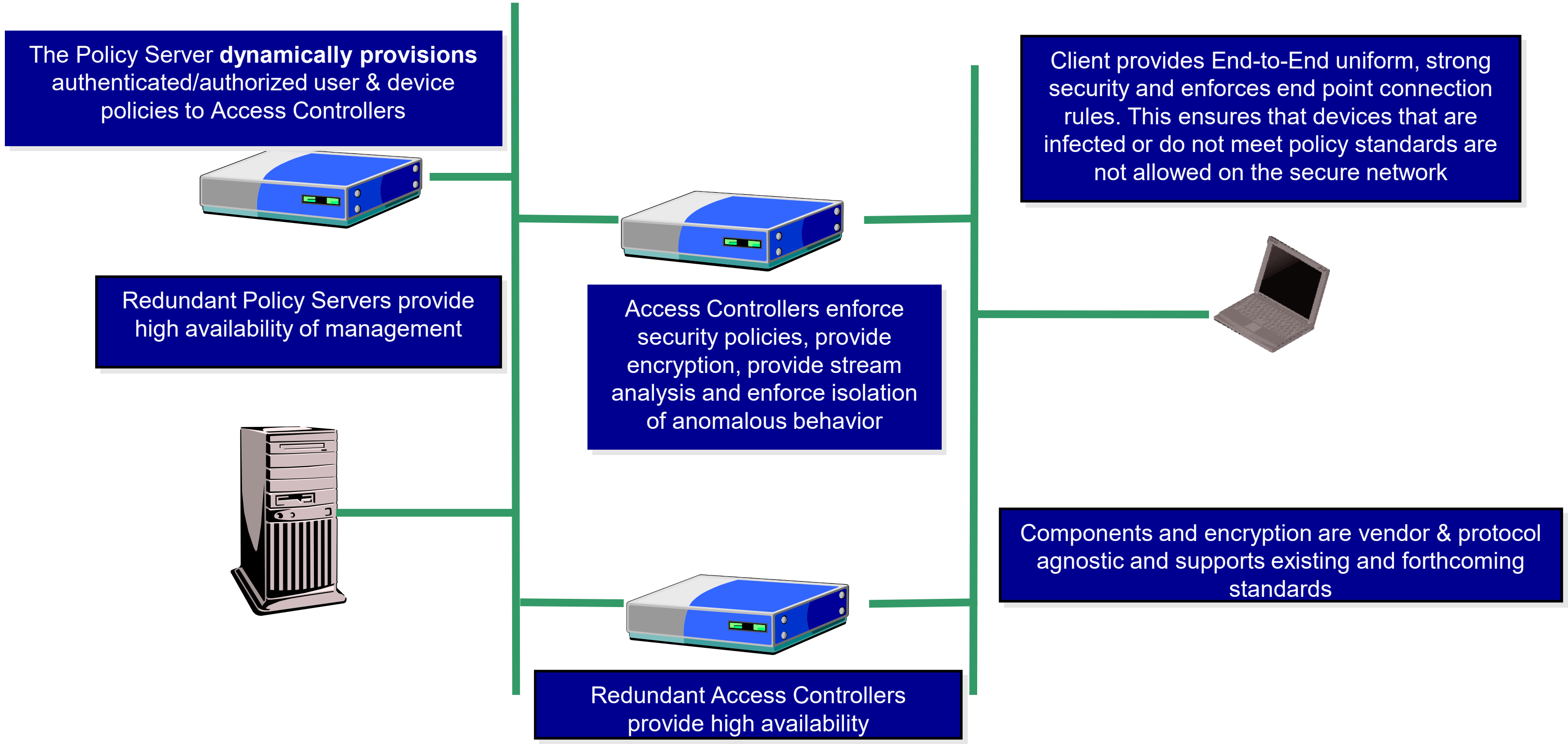
CYLENTIUM builds proven end-to-end Certified Layer 2 encryption software and security platforms

- 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 algorhythms
- 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)

What does Cylentium WirelessWall "DO"

CYLENTIUM provides client applications and Cloaking Bubble Technology that runs independently, enforcing cyber protection rules at network and environment edges and Fog Computing, and intercepts network traffic encrypting the information at Layer 2.

Incoming encrypted traffic is decrypted and shared with the local and secured environments. This provides true end-to-end protection where Cylentium can then wrap, deploy, and network cybersecurity bubbles.



The Policy Server **dynamically provisions** authenticated/authorized user & device policies to Access Controllers

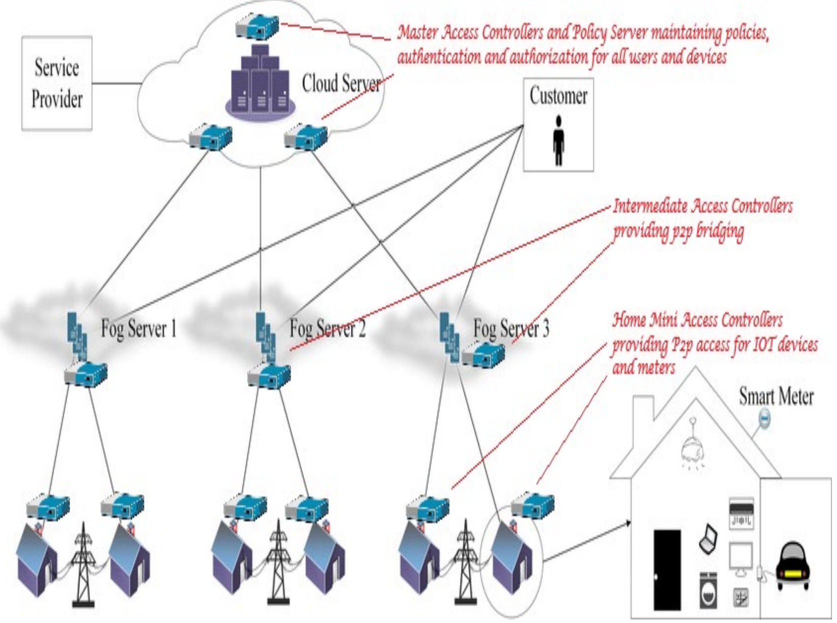
Redundant Policy Servers provide high availability of management

Access Controllers enforce security policies, provide encryption, provide stream analysis and enforce isolation of anomalous behavior

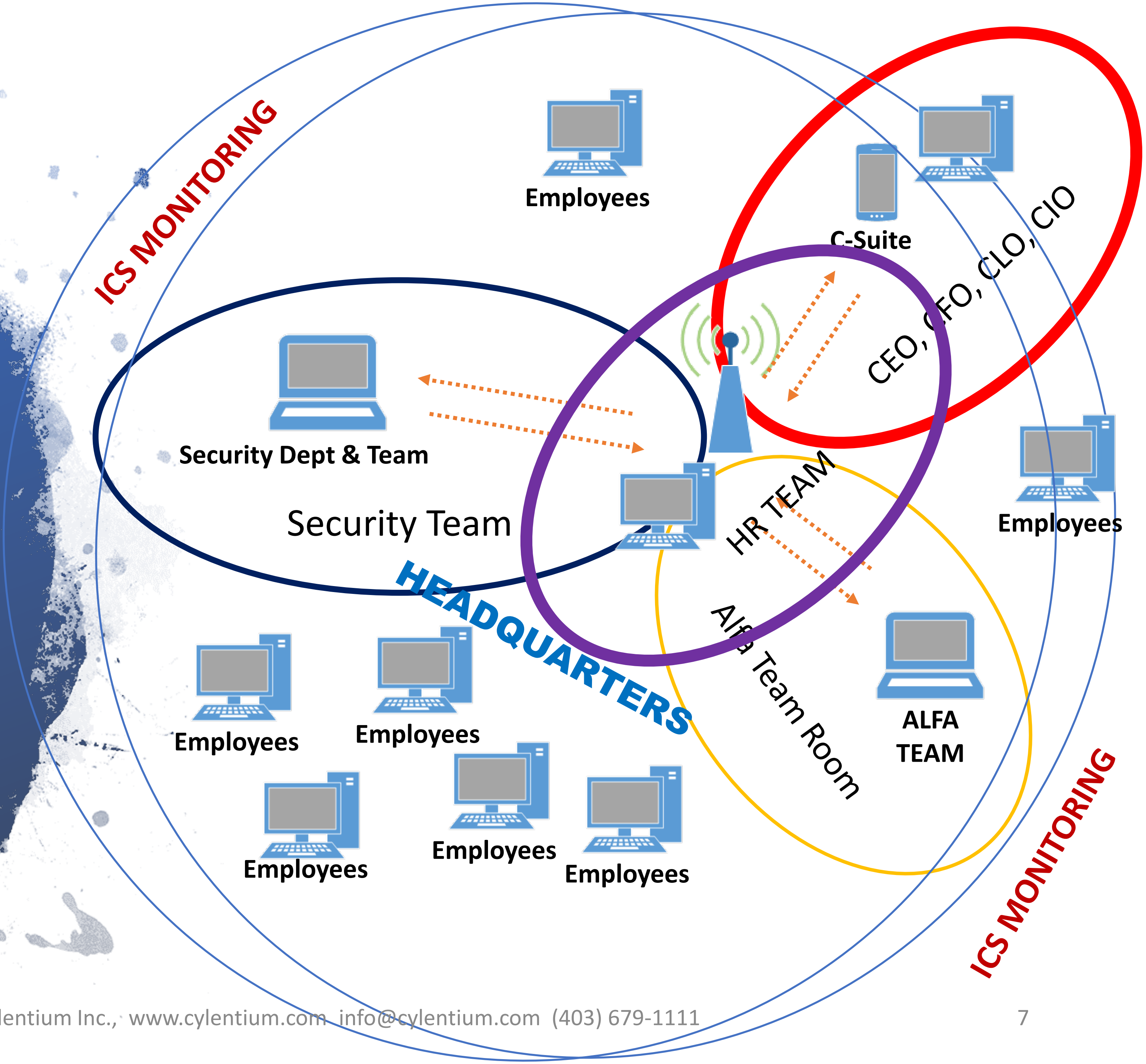
Redundant Access Controllers provide high availability

Client provides End-to-End uniform, strong security and enforces end point connection rules. This ensures that devices that are infected or do not meet policy standards are not allowed on the secure network

Components and encryption are vendor & protocol agnostic and supports existing and forthcoming standards


Service Provider
Cloud Server
Master Access Controllers and Policy Server maintaining policies, authentication and authorization for all users and devices
Customer
Intermediate Access Controllers providing p2p bridging
Fog Server 1
Fog Server 2
Fog Server 3
Home Mini Access Controllers providing P2p access for IOT devices and meters
Smart Meter

Who is Cylentium WirelessWall?



Cylentium Core Competency

A SYSTEM-LEVEL SOLUTION FOR CENTRALIZED MANAGEMENT AND DISTRIBUTED ENFORCEMENT OF WIRELESS LAN SECURITY POLICIES

MUTUALLY AUTHENTICATED LAYER 2 AES-BASED SECURITY

SEAMLESS SUBNET (LAYER 3) ROAMING

TIGHT INTEGRATION WITH EXISTING IDENTITY MANAGEMENT SOLUTIONS

SIGNIFICANT FLEXIBILITY COURTESY OF COTS HARDWARE

THE ULTIMATE LEVEL OF RISK MITIGATION FOR UNCLASSIFIED WIRELESS LAN COMMUNICATION

Cylentium Wireless in Security

“Typical” 802.11 ranges

802.11b/g is typically ~300 feet (2.4 GHz)

802.11a/h is typically ~60 feet (5 GHz)

Radio waves penetrate building walls — impossible to define and enforce perimeter

Networks can be picked up 15 - 20 miles away with sufficient antennae

Creates an entirely new category of espionage — one extremely difficult to detect

Passive attacks capture data for offline analysis; active attacks compromise network real-time

Known Attacks on Wi-Fi Networks

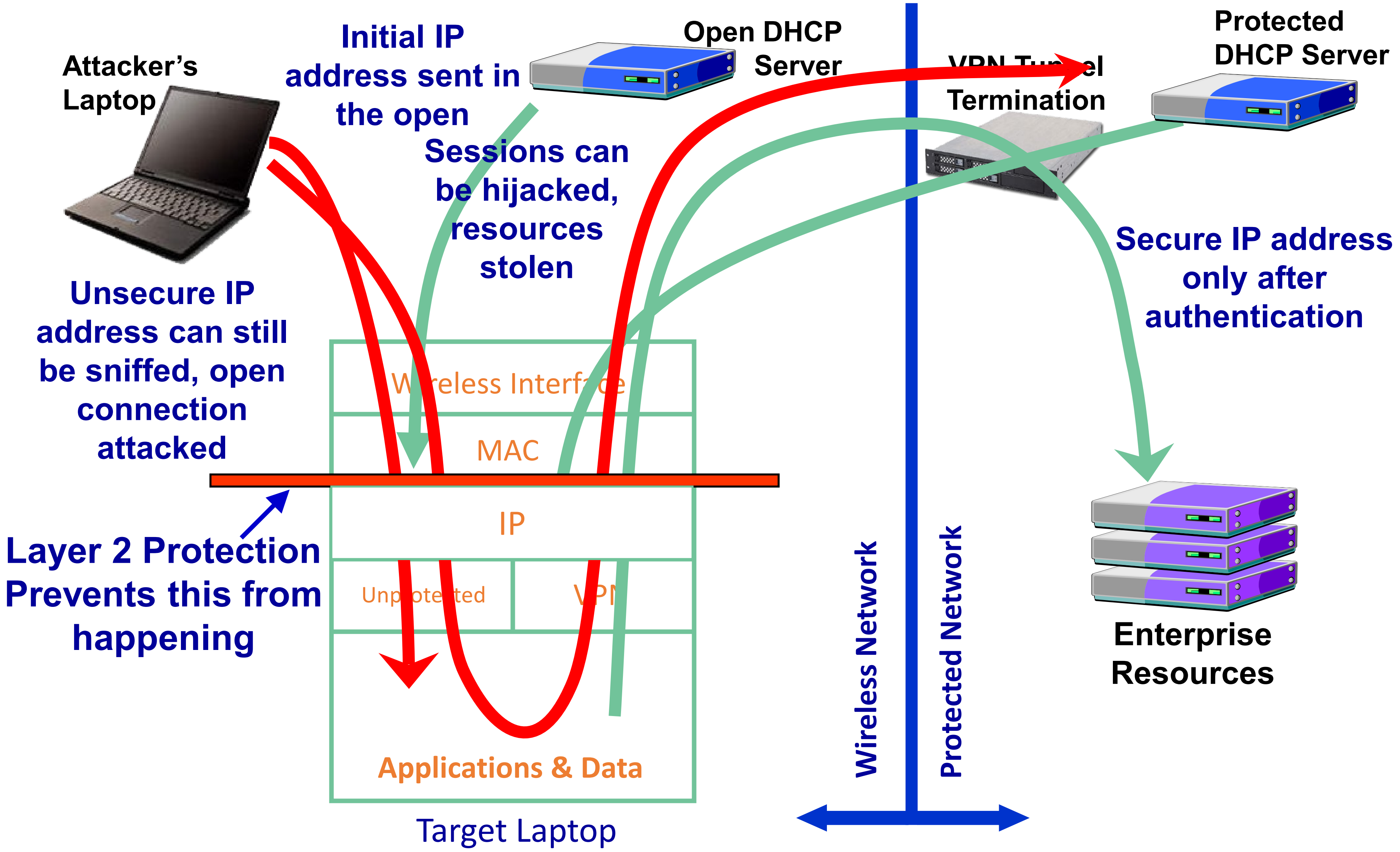
ATTACK	DESCRIPTION	EXPOSURE	**CYLENTIUM DEFENSE**
WEP Compromise/ Data Privacy	Poor implementation of RC4 algorithm results in weak Initialization Vectors	Complete compromise of network and data privacy	Totally different key derivation process; unique session keys per connection
Passive Dictionary	Age-old attack revitalized by proximity access to WLAN	Compromise user credentials to access network	Protect authentication exchanges with TLS tunnels
ARP Connection Redirection	Attacks corrupt network routing tables	Denial of Service of wireless and wired network resources	Layer 2 protection prevents unauthorized use of ARP messages
Access Point Spoofing	Devices can be tricked into thinking they are communicating with enterprise-sanctioned APs	Compromise credentials by responding to an attacker's password challenge	Client and WAC mutually authenticate each other at session initiation
Unauthorized Access	Mobile users can connect anywhere in the network, allowing them to connect to unauthorized network areas	Previously unavailable networks can be accessed by users, giving them access to unauthorized resources	Network resource access independent from connection location

Built on Standards

Where the Standards Fit

Wired Equivalent Privacy (WEP)	Part of the 802.11 standard, provides device authentication and encryption on WLAN access points and client cards; not FIPS-certifiable and widely recognized as flawed
Dynamic WEP	• Addresses weak IV issue by rotating WEP keys periodically • Ties users to a single vendor for all devices
Wi-Fi Protected Access (WPA)	WEP with periodic key rotation & 802.1x for authentication • Uses Temporal Key Integrity Protocol (TKIP), which is a ‘quick-fix’ patch • Does not support requirements for secure roaming • Interim security solution — will be obsoleted in 2004 by 802.11i • Not FIPS certifiable
802.11i	Station-to-station security standard for AP and peer-to-peer applications • Addresses privacy, integrity, authenticity of data between devices • Does not address system-level management, security, mobility issues •Not FIPS certifiable with interoperability
802.1x	IEEE standard for authentication only; supports multiple authentication modes for wired and wireless networks • Does not specify a secure communication channel between ‘supplicant’ (user) and ‘authenticator’ • Does not address system-level security, mobility, management issues
802.11f	Describes inter-AP communications among multi-vendor systems • Specifies fast handoff between APs • Only addresses roaming within the same subnet

WHY CYLENTIUM? VPNs Don't Protect the Network


Attacker's Laptop
Initial IP address sent in the open
Open DHCP Server
VPN Tunnel Termination
Protected DHCP Server
Sessions can be hijacked, resources stolen
Unsecure IP address can still be sniffed, open connection attacked
Secure IP address only after authentication
Wireless Interface
MAC
IP
Unprotected
VPN
Applications & Data
Target Laptop
Layer 2 Protection Prevents this from happening
Wireless Network
Protected Network
Enterprise Resources

Cylentium Completes the Picture

Mechanism	Management	Security	Mobility
WEP	NO	Widely recognized as flawed Being replaced with WPA	NO
WPA WPA2	NO	Improvement over WEP	NO
802.11i	NO	Device level only	NO
802.1x	NO	Authentication only	NO
802.11f	NO	NO	Between APs on same subnet only
Cylentium WirelessWall	YES	Network level security Strong authentication AES encryption	Robust roaming across Micro Segmentation subnets
Cylentium Wireless Wall Manager	YES	Enforces enterprise wide security policies	Policy enforced while roaming

Why is Wireless *insecure*

“Typical” 802.11 ranges

802.11b/g is typically ~300 feet (2.4 GHz)

802.11a/h is typically ~60 feet (5 GHz)

Radio waves penetrate building walls — impossible to define and enforce perimeter

Networks can be picked up 15 - 20 miles away with sufficient antennae

Creates an entirely new category of espionage — one extremely difficult to detect

Passive attacks capture data for offline analysis; active attacks compromise network real-time

Common Concerns Addressed

Attacks on Wi-Fi networks

- WEP compromise
- Credential compromise (dictionary attacks)
- ARP cache poisoning (Man-in-the-Middle)
- Access point spoofing (Man-in-the-Middle)
- Unauthorized access

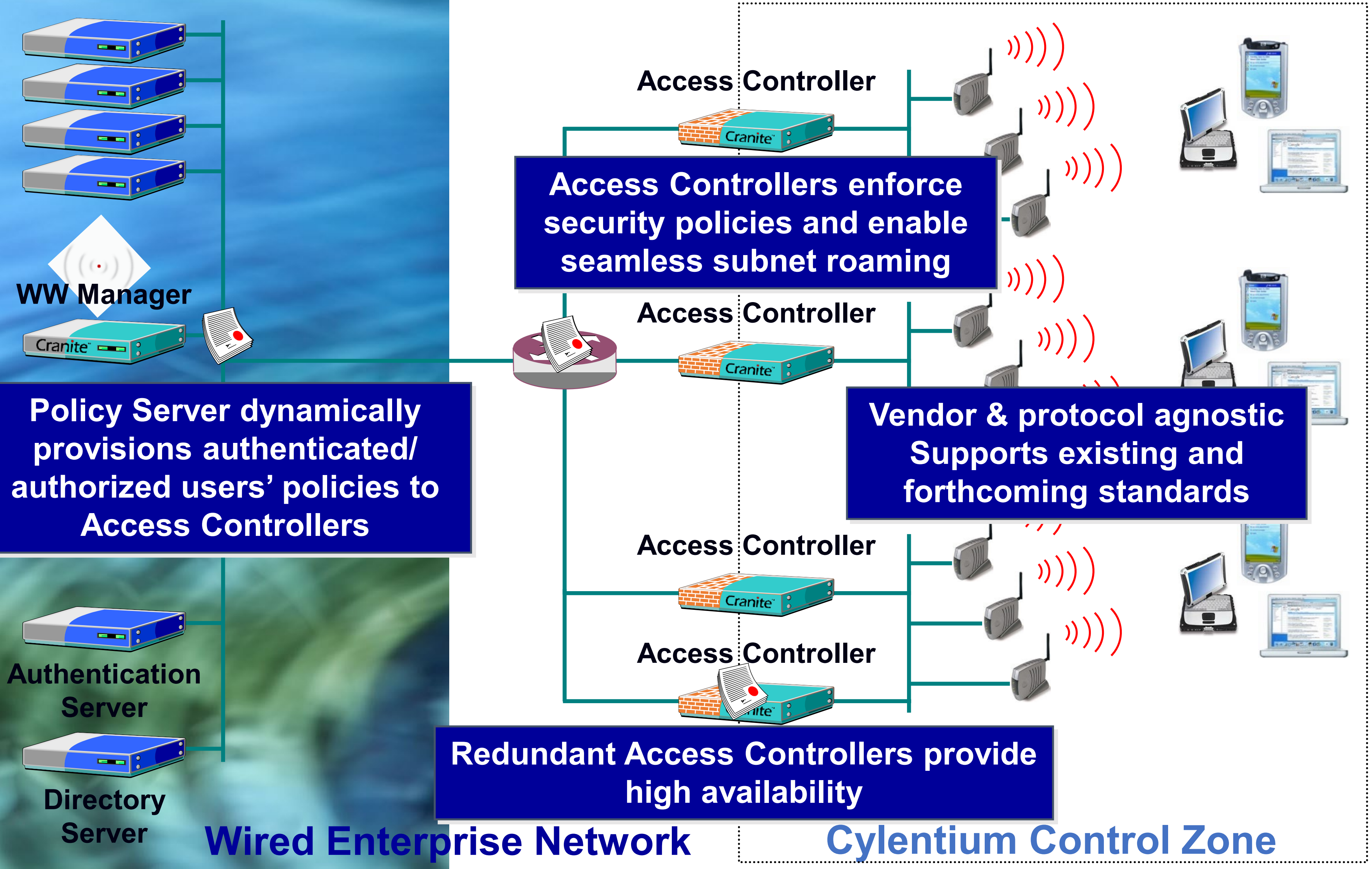
Mobility challenges

- Low latency handoffs across Layer 2 and Layer 3 boundaries
- Seamless Layer 3 roaming without need to re-authenticate while maintaining network integrity

Management challenges

- Identity management integration
- Role-based access control

WirelessWall – How it Works



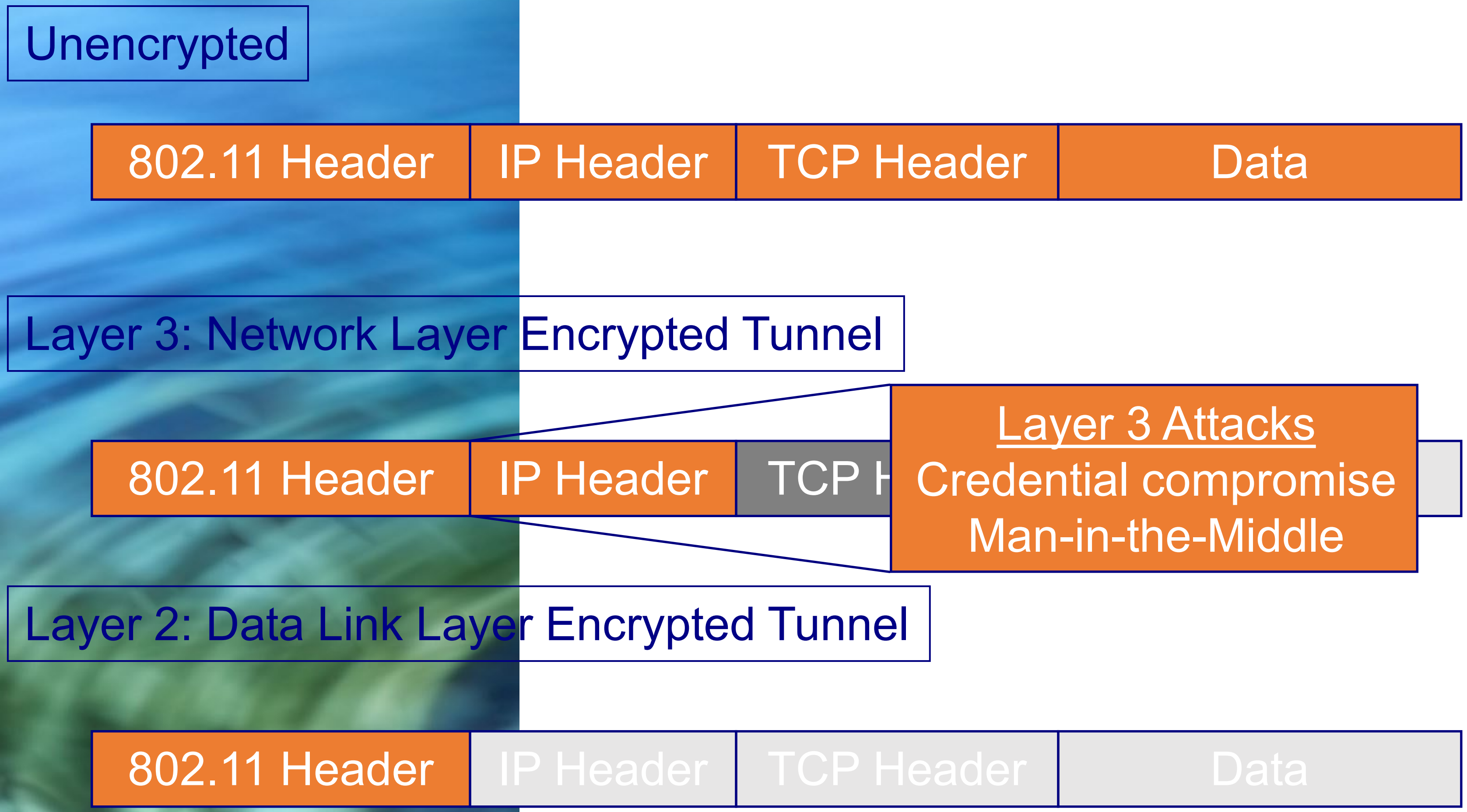
Access Controllers enforce security policies and enable seamless subnet roaming

Policy Server dynamically provisions authenticated/ authorized users' policies to Access Controllers

Vendor & protocol agnostic Supports existing and forthcoming standards

Redundant Access Controllers provide high availability

Securing Data and Network Layers



Unencrypted

802.11 Header | IP Header | TCP Header | Data

Layer 3: Network Layer Encrypted Tunnel

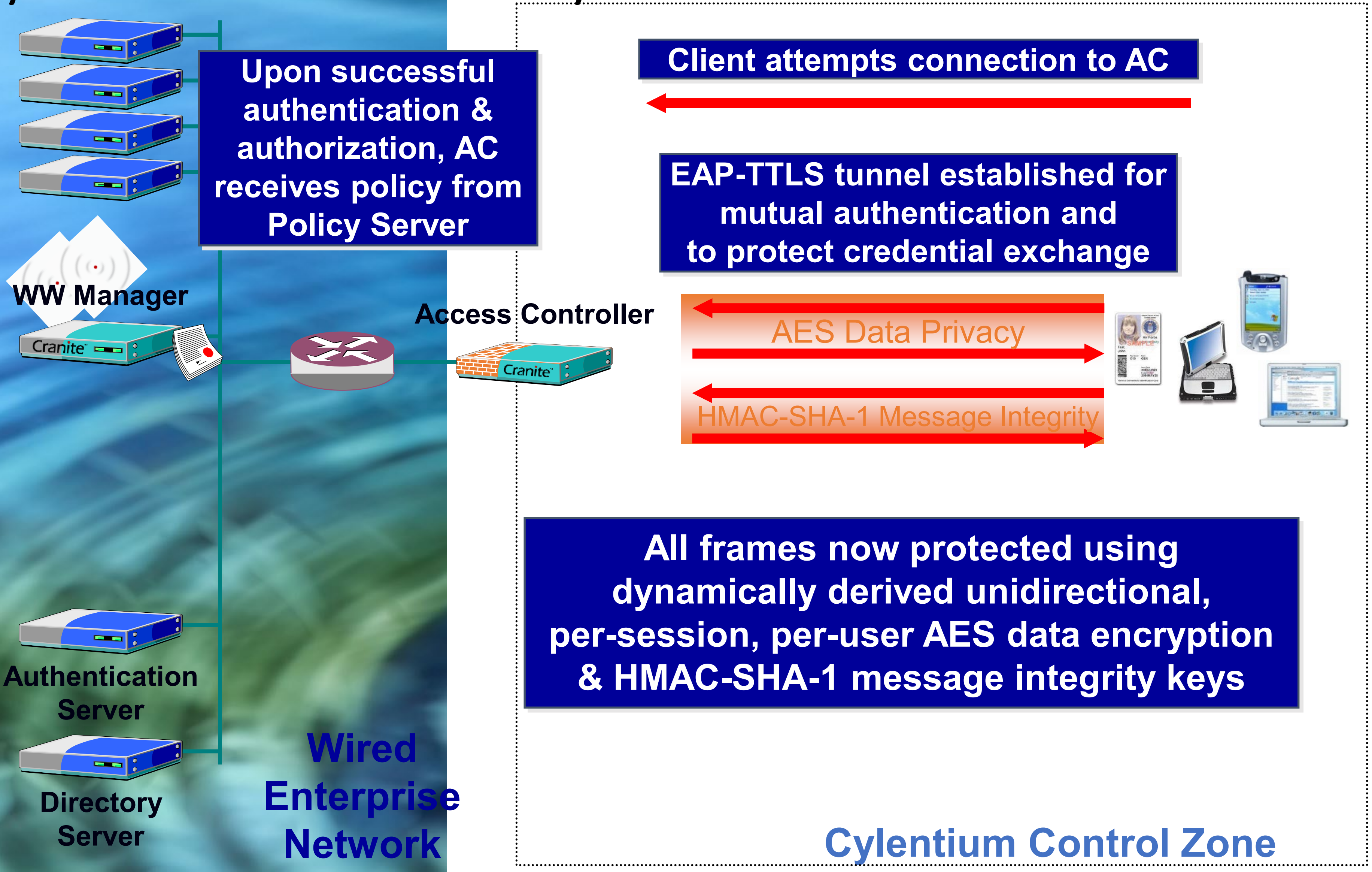
802.11 Header | IP Header | TCP H

Layer 3 Attacks
Credential compromise
Man-in-the-Middle

Layer 2: Data Link Layer Encrypted Tunnel

802.11 Header | IP Header | TCP Header | Data

Layer 2 Data Security



Upon successful authentication & authorization, AC receives policy from Policy Server

Client attempts connection to AC

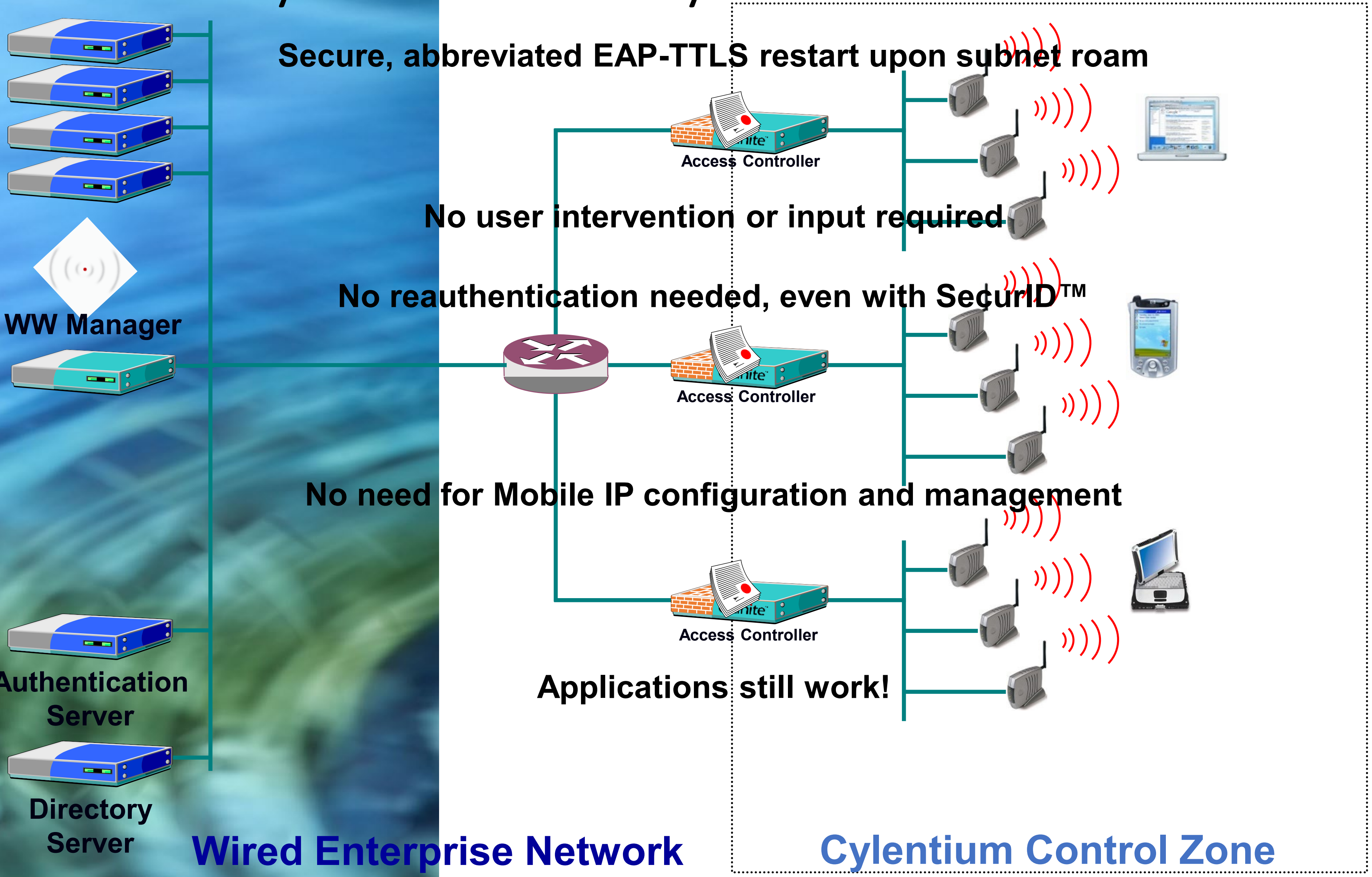
EAP-TTLS tunnel established for mutual authentication and to protect credential exchange

AES Data Privacy

HMAC-SHA-1 Message Integrity

All frames now protected using dynamically derived unidirectional, per-session, per-user AES data encryption & HMAC-SHA-1 message integrity keys

Seamless Layer 3 Mobility



Secure, abbreviated EAP-TTLS restart upon subnet roam

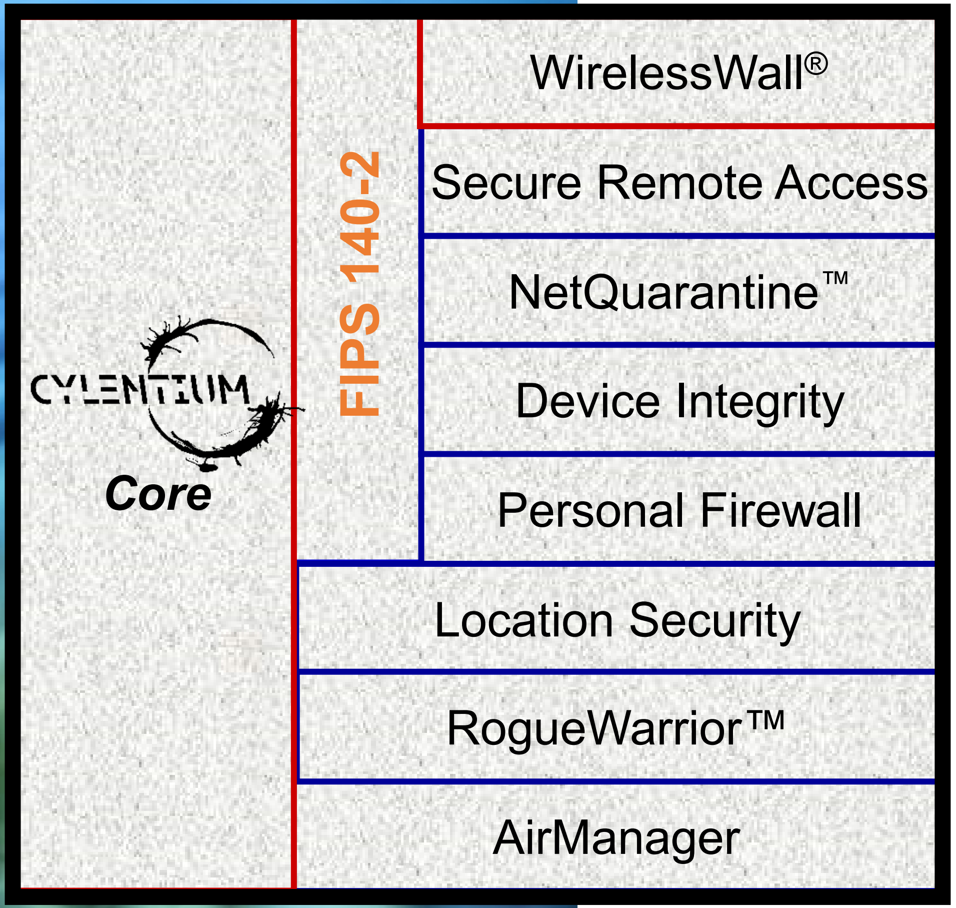
No user intervention or input required

No reauthentication needed, even with SecurID™

No need for Mobile IP configuration and management

Applications still work!

Cylentium Core: Integrated WLAN Security Platform



CYLENTIUM

Core

FIPS 140-2

WirelessWall®

Secure Remote Access

NetQuarantine™

Device Integrity

Personal Firewall

Location Security

RogueWarrior™

AirManager

Layer 2 Security with Mobility

Traverse WAN @ Layer 2

Isolate Non-compliant Devices

Remote Device Protection

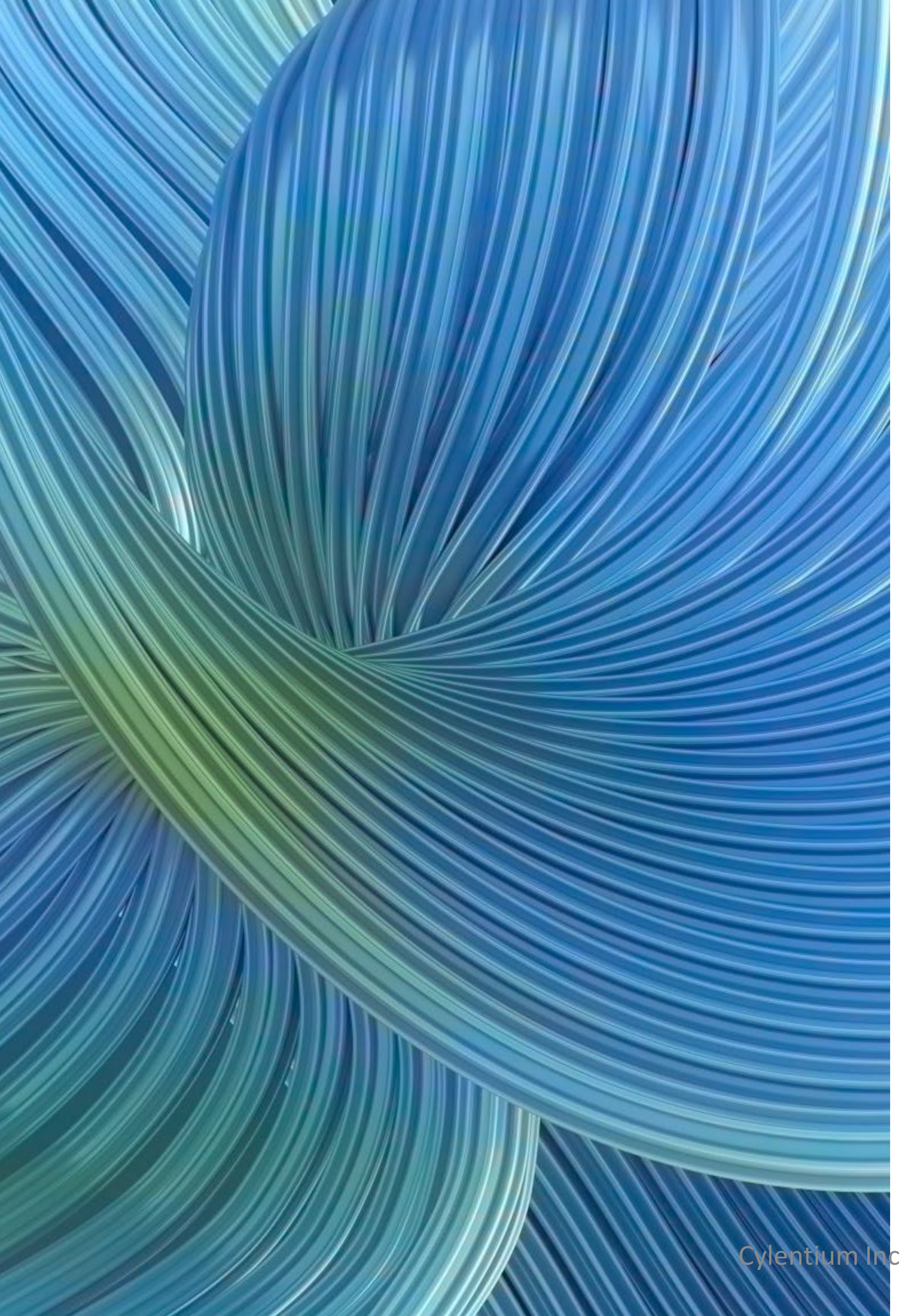
Dynamic Access Control

Location-based Access Control

Detect, Locate, Kill Rogue APs

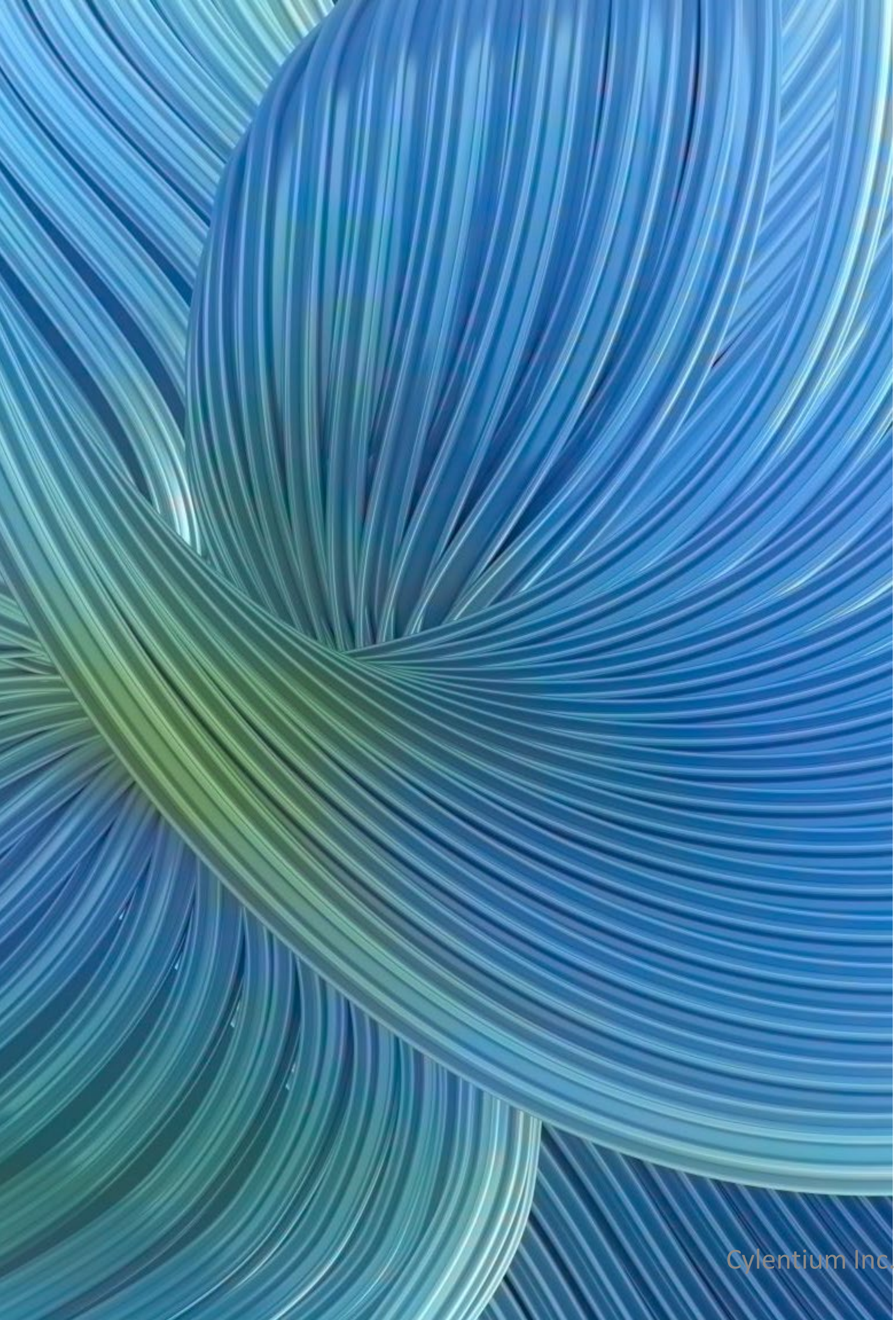
AP Management

CYLENTIUM VPN



Remote Access Problems

- 🔓 Feature-rich and complex IPsec forced to share market with browser-only SSL VPNs
- 🔒 SSL VPNs fail in application interoperability
- ⚠ Neither addresses evolving security threats



Better Remote Access

Feature-rich and complex IPsec forced to share market with browser-only SSL VPNs

SSL VPNs fail in application interoperability

Neither addresses evolving security threats

Cylentium SafeConnect *"combines ease of use of SSL…with the end-to-end applications interoperability of IPsec"*

Better Remote Access

For customers unhappy with IPsec *and/or* frustrated by SSL VPN limitations

Cylentium's SafeConnect is *proven* superior

- Much more secure than IPsec or SSL
- *All* network applications work out of the box
- 10x-20x throughput improvement over SSL
- 2x-3x throughput improvement over IPsec
- Simplicity leads to significant TCO savings

Current and Legacy Clients

CURRENT / LEGACY CLIENTS

- Savannah River Nuclear Site
- NSA – National Security Agency
- Defense Information Systems Agency (DISA)
- United States State Department
- United States Special Operations Command (SOCOM)
- United States Naval Academy
- Army Safety Command
- Naval Sea Systems Command
- Canadian Airforce Tactical Forces
- Naval Research Center
- Naval Warfare Systems Command (NAVWAR)
- United States Special Operations Command (SOCOM)
- US Marine Corps field operations Iraq

CURRENT / LEGACY CLIENTS

- NTT - Nippon Telegraph & Telephone
- New York City SWAT First Responders Teams
- Lockheed Martin (LMCO)
- Rockwell
- Sandia National Labs
- Booz Allen Hamilton Consulting
- US Army field operations Iraq
- US Army Field Mobile Handsets
- Army Medcom
- Naval-Marine Corps Intranet (NMCI)
- United States Joint Forces Command
- Madigan Army Medical Center
- Walter Reed Medical Center

U.S. Army Inspector General School

cisra

UTMB

RENTON
AHEAD OF THE CURVE

DETRICK
A Community of Excellence

U.S. Army Inspector
General School

Canada

Lawrence Livermore
National Laboratory

USAMRIID
United States Army Medical Research Institute of Infectious Diseases

Sandia National Laboratories

UNITED STATES NAVAL ACADEMY

MADIGAN ARMY MEDICAL CENTER

Walter Reed
Army Medical
Center