ENGARDE

YOUR GUARD WITHIN

Protecting the Network

EnGarde Technologies, Inc.

Military Grade Cybersecurity

Agenda

- The Challenge We Face
- Zero Trust and How We Get There
- Gaps to Address Zero Trust
- Sensor Vulnerabilities

All other Software Deals with Threats After they Enter the Network

The Challenge

The most serious challenges of cybersecurity for industry and government include the constant evolution of sophisticated cyber threats and attack vectors. Cybercriminals are increasingly employing advanced techniques, such as social engineering and ransomware, to exploit vulnerabilities and gain unauthorized access to sensitive data. Additionally, the growing interconnectedness of systems and devices in the digital age amplifies the risk of widespread attacks and potential disruptions to critical infrastructure. Moreover, the shortage of skilled cybersecurity professionals exacerbates the difficulty in effectively defending against and responding to cyber threats, leaving organizations and governments vulnerable to potential breaches and data breaches. Risks and costs increase every day. We are able to address these challenges now.

EnGarde Provides an Immediate Solution, Simple, and Low Cost

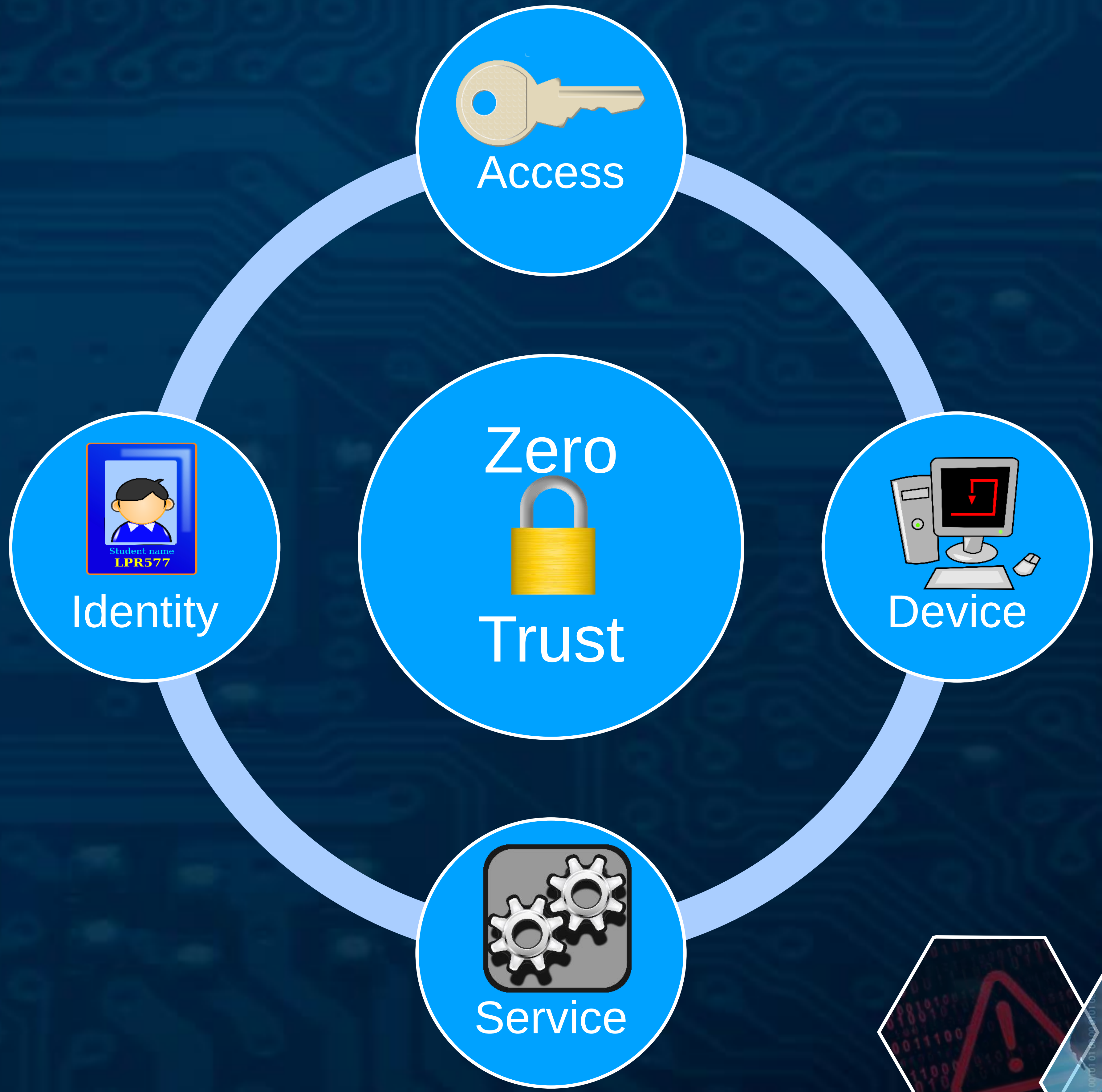
What is Zero Trust?

Never Trust, Continuously Verify: Device, User, and Data

Zero trust is the term for an evolving set of cybersecurity protocols that move defenses from static, network-based perimeters to focus on dynamic identity-based users, assets, and resources.

Zero Trust represents a shift in philosophy … from verify once at the perimeter to continual verification of each user, device, application, and transaction

Zero Trust places significant emphasis on stronger enterprise identity and access controls



Redefining Cybersecurity

We often define *cybersecurity* in terms of protection from external intrusions. But what about embedded issues? What about ransomware or malicious code hidden in chips or software? The definition needs expansion.

Cyber Incident

- **–The De facto IT definition**
  - **•Connected to the Internet, generally running Windows, and data is maliciously being manipulated or stolen - All about privacy**
- **–NIST/GAO definition**
  - **•Electronic communication between systems that affects Confidentiality, Integrity, or Availability**
  - **•Whether Unintentional or Malicious**

Common Gaps in Zero Trust

- We often do a reasonable job of protecting computer assets, but in the current world devices are much more than PCs or servers on a network.

- We often rely on continuous connections to the cloud to enforce security. But what if that connection is interrupted or what if a man-in-the-middle attack hijacks that traffic?

- We rely heavily on hub-and-spoke architectures for simplicity of administration.   But this gives the enemy an easy point to attack the systems.

- Continual verification is often tossed aside as too intrusive. But frame authenticity is required to prevent many attacks.

- Machine Learning is needed to understand patterns of life to prevent ransomware.

- Role based access controls are insufficient; policy based access controls need to cover all devices and nodes on the network.

- Some attacks (such as ARP poisoning) are just ignored as too hard to solve.

- Complexity in managing and maintaining multiple systems leads to potential errors.

EnGarde Technology

EnGarde develops Military Grade Cybersecurity software. Legacy versions have been utilized continuously for the past 18 years by the US Department of Defense (DoD) and the US Department of Energy (DoE) to protect their digital networks and physical assets such as ships, aircraft, military bases, missile sites and nuclear facilities—against cyber threats from bad actors with zero incidents. Our MVP (Latest version) will be available in Q4 2023 for government/military deployment. Recent testing and validation in 2023 with Navy Cyber, USSOCOM, and elements of the IC.

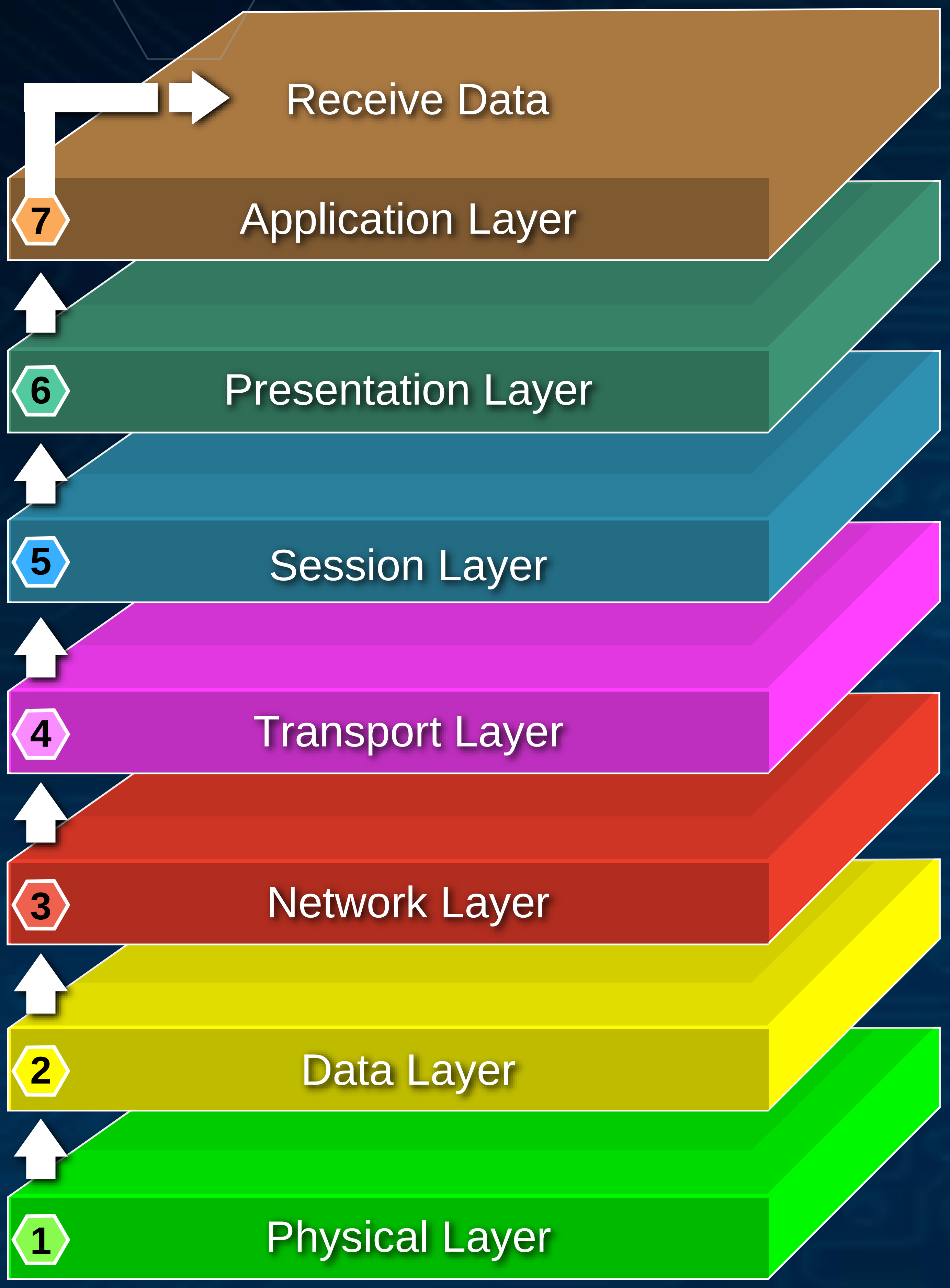
*Military-Grade Network Cloaking • 18 Years with **Zero Breaches***

The Key to our Software

- *The EnGarde cloaking technology is highly disruptive to the conventional cybersecurity process, providing a new paradigm vision for on-premises protection allowing safe network operations, navigating the IoT space. Our principle advantage is that EnGarde operates at OSI Layer 2 - the Data Link Layer, therefore preventing threats **before** they can penetrate the network.*
- *MACSec protocols provide frame-level encryption with highest security, min latency*
- *All other cybersecurity software works on the traditional model of: Monitor, Detect, and Mitigate threats **after** the threat enters the network, at OSI Layer 3.*

All other Software Deals with Threats After they Enter the Network

Operating at ***Layer 2*** *and works seamlessly with Layer 3 Environments*



Data Transmit and Receive Layers

Net Quarantine

- Insider Threat Detection
- Rogue Actor Intelligence Detection
- Anomalous Cyber Behavior Detection

3

Micro Segmentation

- Encryption enforced software
- User based access
- Firewalls

3

VPN

- Military Standards Encryption
- Remote Networking
- Controlled Access

3

EnGarde software uniquely operates traditional Layer 3 ıctions at Layer thereby achieving 100% network security 2

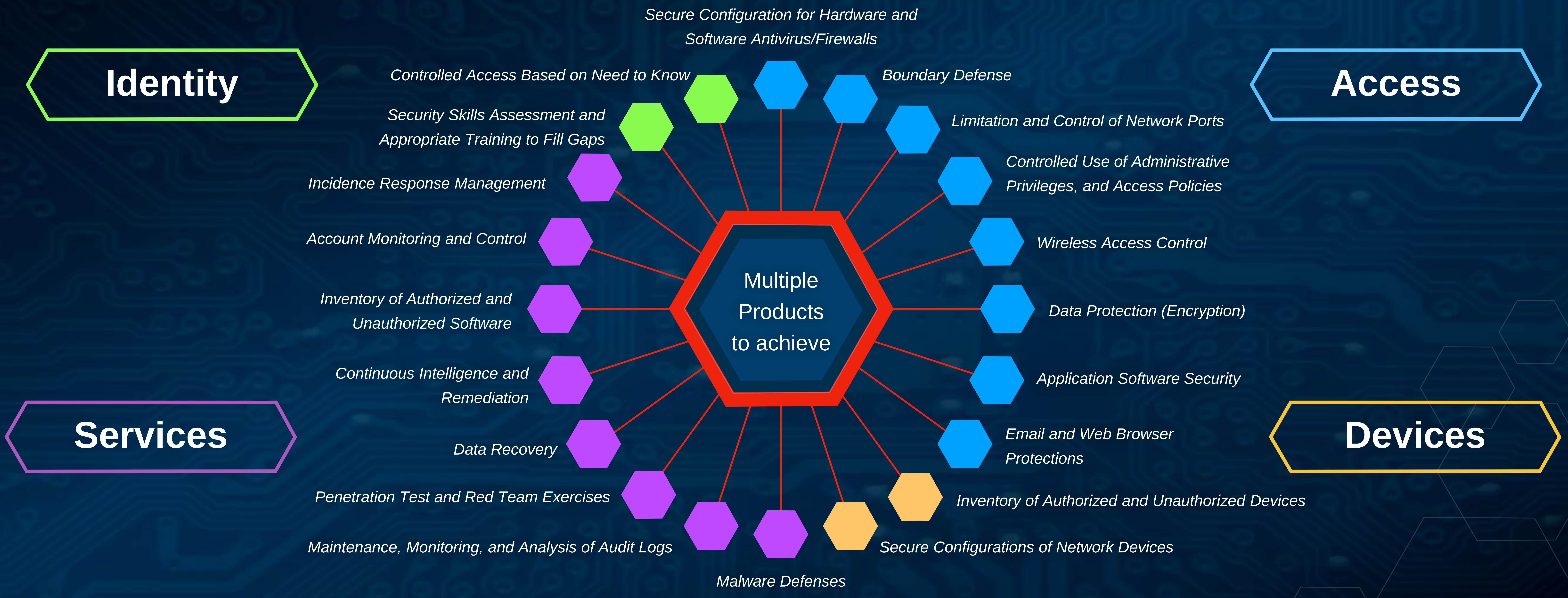
2

- Only Layer 2 IP Cloaking and Encryption Protocol Worldwide
- Uses FIPS 140-2 Protocols
- Dynamic key rotation
- Responsive policy-based access control
- Employed on FRONT END of data flow and network systems
- Obfuscation of IP addresses

EnGarde can Protect all Legacy applications and devices by assuring that each device meets policy standards **before** being granted access to the network

ENGARDE

Necessary functions to achieve Zero Trust at Layer 3



Multiple Products to achieve

Identity

- Controlled Access Based on Need to Know
- Security Skills Assessment and Appropriate Training to Fill Gaps

Access

- Secure Configuration for Hardware and Software Antivirus/Firewalls
- Boundary Defense
- Limitation and Control of Network Ports
- Controlled Use of Administrative Privileges, and Access Policies
- Wireless Access Control
- Data Protection (Encryption)
- Application Software Security
- Email and Web Browser Protections

Devices

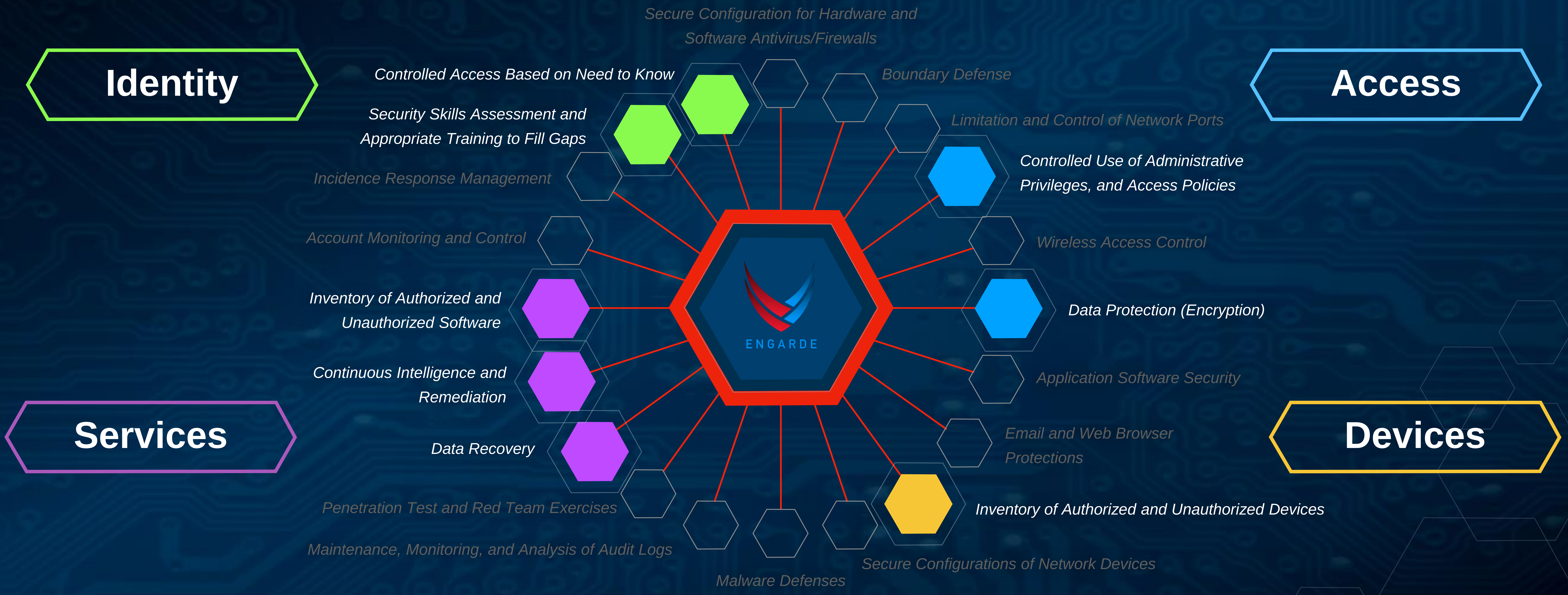
- Inventory of Authorized and Unauthorized Devices
- Secure Configurations of Network Devices

Services

- Malware Defenses
- Maintenance, Monitoring, and Analysis of Audit Logs
- Penetration Test and Red Team Exercises
- Data Recovery
- Continuous Intelligence and Remediation
- Inventory of Authorized and Unauthorized Software
- Account Monitoring and Control
- Incidence Response Management

Today's IT Security Paradigm: **Detect, Identify, Mitigate** *at* **Layer 3 and Above**

Benefits of a Layer 2 Solution - Flexibility



Identity

Access

Services

Devices

ENGARDE

Secure Configuration for Hardware and Software Antivirus/Firewalls

Controlled Access Based on Need to Know

Security Skills Assessment and Appropriate Training to Fill Gaps

Incidence Response Management

Account Monitoring and Control

Inventory of Authorized and Unauthorized Software

Continuous Intelligence and Remediation

Data Recovery

Penetration Test and Red Team Exercises

Maintenance, Monitoring, and Analysis of Audit Logs

Malware Defenses

Secure Configurations of Network Devices

Inventory of Authorized and Unauthorized Devices

Email and Web Browser Protections

Application Software Security

Data Protection (Encryption)

Wireless Access Control

Controlled Use of Administrative Privileges, and Access Policies

Limitation and Control of Network Ports

Boundary Defense

Layer 2 Cloaking Means: Far Less Costs in Software, Hardware and Personnel Operating at Layer 2

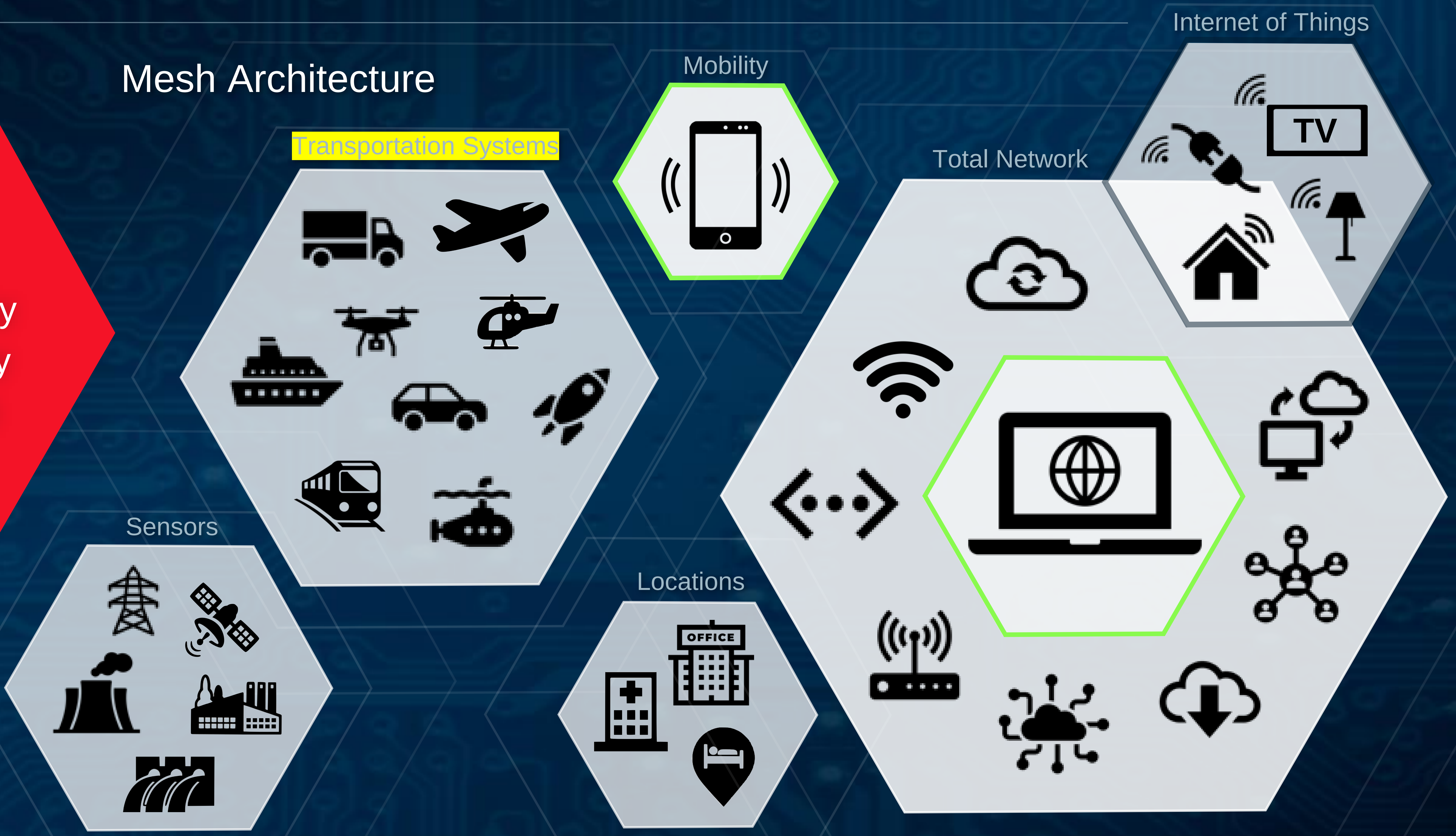
ENGARDE

We Protect the network and any connected device

We Protect Point-to-Point Data Communications from any Connected Device to Any Connected Device (IoT)

Total Trust

Prevents actors from operating inside or outside any network



Cloaking Cybersecurity Protection down to the often-overlooked Sensor Level

Assure *Data Integrity Down to the* ***Sensor*** *Level*

Limitation with a traditional VPN:

- **The tunnel is secure, but has the data been compromised, especially those coming from our network sensors? Vulnerabilities for Man-in-the-Middle attacks/DDOS**

EnGarde checks the integrity of every data packet sent

- **The data payload of *each* frame is encrypted and carries a separate integrity verification code**

The Threat to Internet-of-Things (IoT) Devices

- *25 billion IoT devices, 8 billion deployed within Enterprises*
- *24% of IoT devices utilize encryption when transmitting data, leaving 76% of IoT devices completely exposed*
- *Attacks on IoT devices have increased 700% since 2019*

EnGarde Ensures ***data*** *you receive from your sensor network is valid and trusted*

EnGarde Sensor Protection **Solution**

Infrastructure Example

Prior to 2006 there were Zero Chinese transformers – Sensors may be compromised in our inventory today

A typical electric power station can have more than 20k sensors to monitor site operations. Sourcing of these sensors are suspect and often untraceable as to authenticity or origin

EnGarde Ensures the data you receive from your sensor network is valid and trusted by authenticating every packet of data

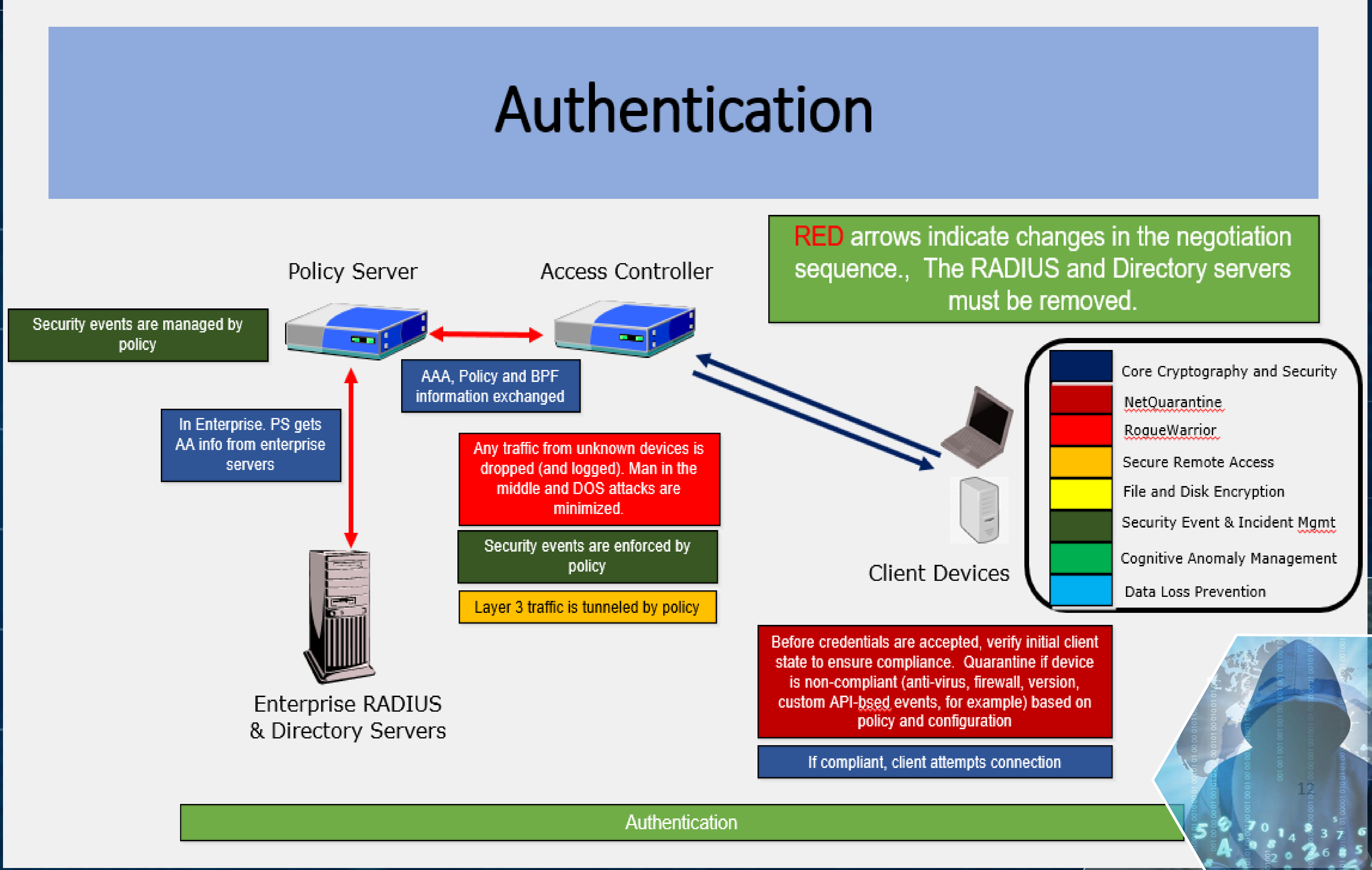
Industrial Organizations Reporting Sensor Issues/Concerns on Data

- **Massachusetts' Braintree Electric Light Department (BELD)**
- **Bechtel**
- **Fluor**
- **Florida Power & Light**
- **PacifiCorp**
- **Iberdrola**
- **Fortis**
- **Public Service Company of New Mexico**
- **NV Energy**
- **New York Power Authority (NYPA)**

Sacramento Municipal Utility District

EnGarde Security ***Protecting the Sensors***

- **Crypto-Enabled to secure the transfer of data between two devices *regardless of the intervening devices or network***
  - **Enhanced cryptography for more sensitive sections of the network (Quantum, AES 128, AES 256 and ECC)**
  - **Unauthorized changes to data cannot be made without being detected**
  - **A received frame is encrypted and guaranteed to have been sent by the authenticated IT / IoT device (Sensor). It cannot be intercepted by a man-in-the-middle attack and delayed by more than a few seconds without being detected**



Authentication

RED arrows indicate changes in the negotiation sequence., The RADIUS and Directory servers must be removed.

Security events are managed by policy

AAA, Policy and BPF information exchanged

In Enterprise. PS gets AA info from enterprise servers

Any traffic from unknown devices is dropped (and logged). Man in the middle and DOS attacks are minimized.

Security events are enforced by policy

Layer 3 traffic is tunneled by policy

Before credentials are accepted, verify initial client state to ensure compliance. Quarantine if device is non-compliant (anti-virus, firewall, version, custom API-bsed events, for example) based on policy and configuration

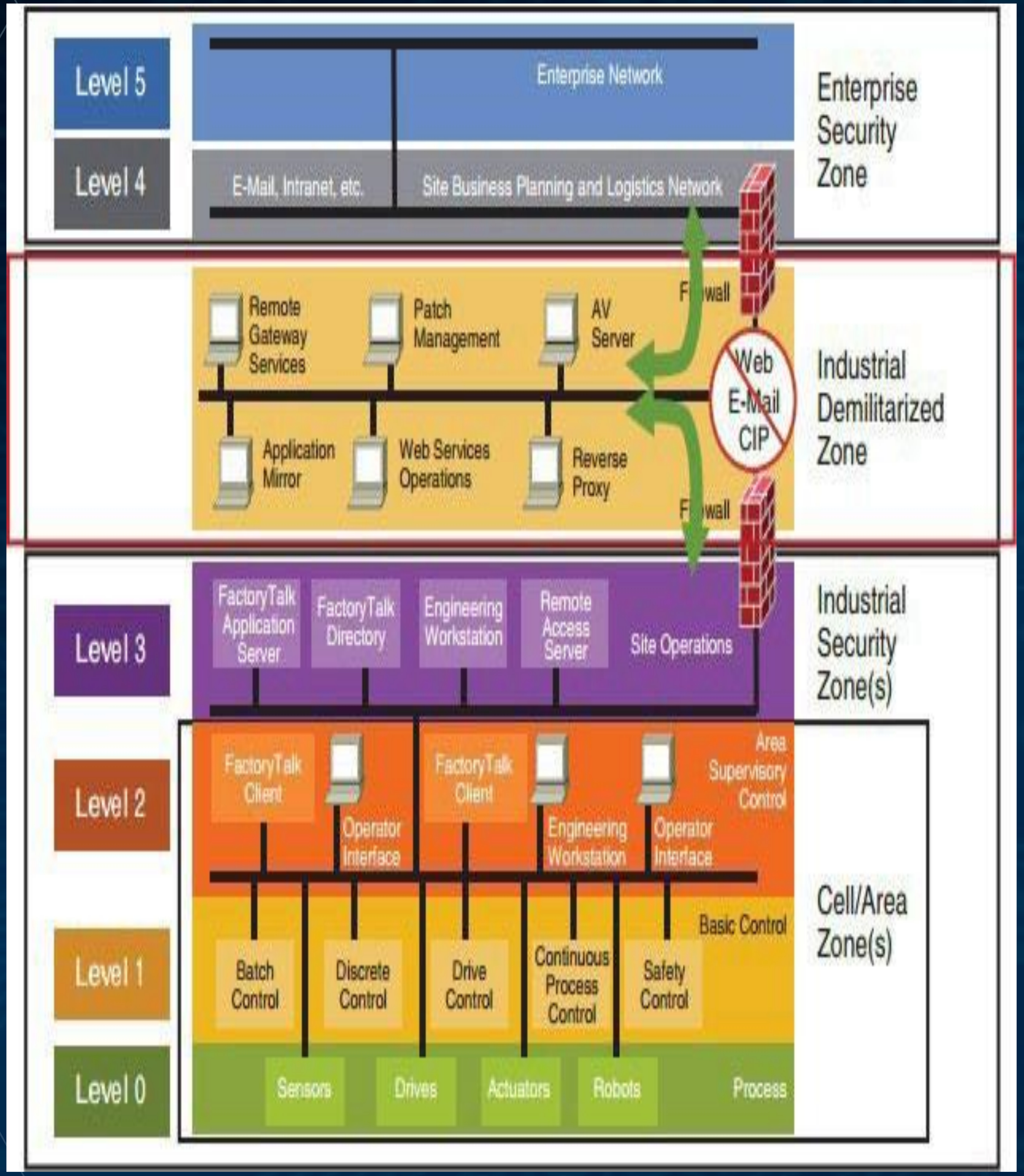
If compliant, client attempts connection

Authentication

🟦	Core Cryptography and Security
🟥	NetQuarantine
🟥	RogueWarrior
🟧	Secure Remote Access
🟨	File and Disk Encryption
🟩	Security Event & Incident Mgmt
🟩	Cognitive Anomaly Management
🟦	Data Loss Prevention

Authentication ***Demonstrations*** *both the Simplicity and Power of EnGarde*

The Purdue Reference Model (Real Time Sensors)



The process sensors at level 0 perform monitoring in real time

- Monitoring at level 3 or above can miss anomalous behavior of level 0 devices.

- Common operating systems, such as Windows, have latency characteristics that can miss aberrant behavior or even down time in these real time devices.

At Level 1 (Edge) EnGarde becomes the Sensor “Sentry” required to secure the Level 0 Sensors

Why are **Process Sensors so Vulnerable?**

Process Sensors:

- **Have no passwords, antivirus, authentication, keys**
- **Use insecure sensor networks (HART*, Profibus, etc.)**
- **Have no cyber certification, Factory Acceptance Test, or Site Acceptance Test criteria**

Reported Issues:

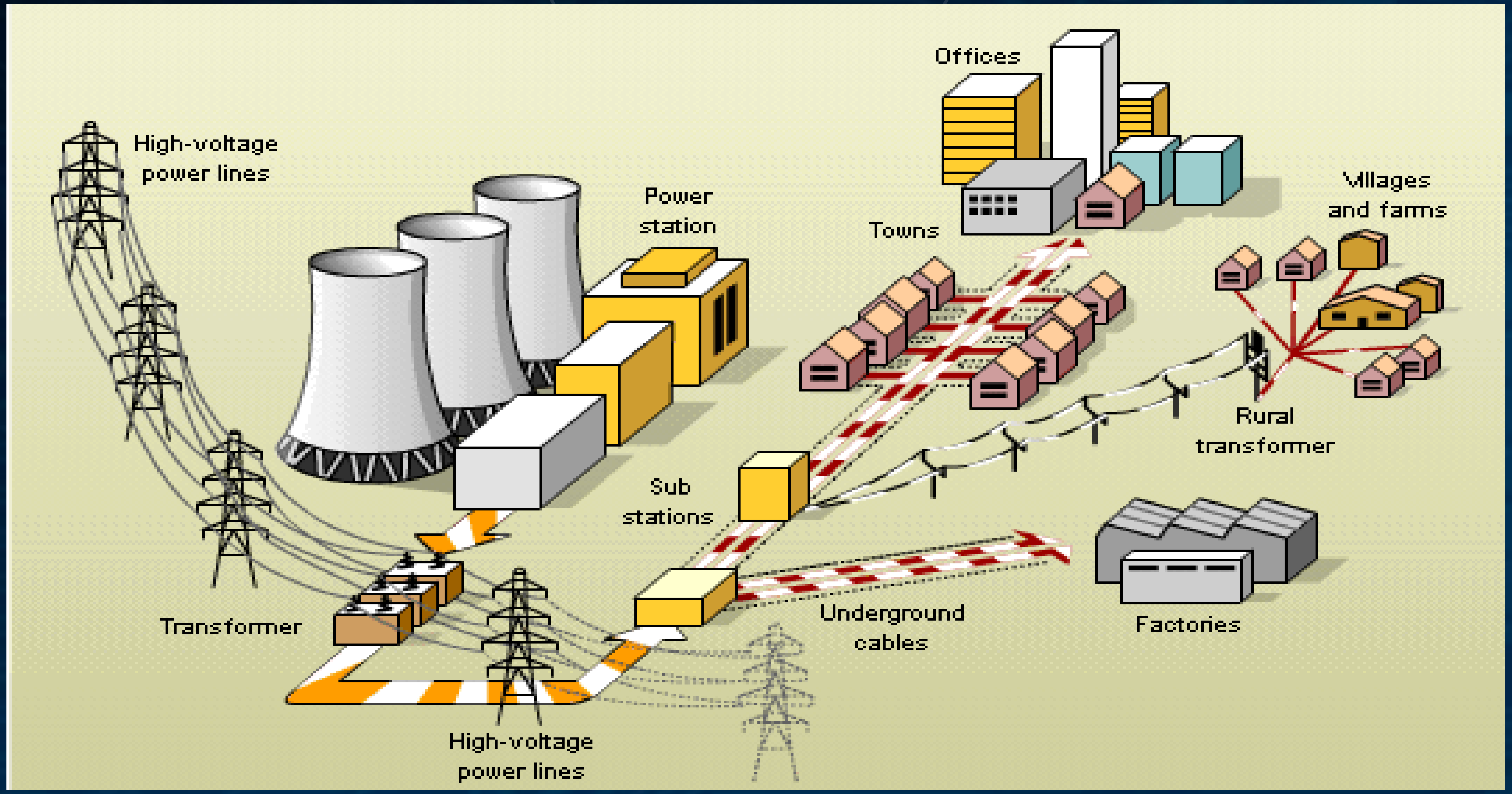
- **Command and Control Backdoors in IoT Sensors within foreign-sourced electrical transformers**

Sensors are the “Achilles Heel” of our critical infrastructure

Above Sources: Multiple Government and Industry Cybersecurity Reporting

* **Highway Addressable Remote Transducer**

Example Simple Power Grid



Example Power Network

- **Represents typical network**
- **Each element represents a subnetwork**
- **Each has unique characteristics and unique vulnerabilities within the system - especially the insecure process sensors**
- **Mobile networks linked to fixed networks**
- **Ultimately, it's about protecting the data as it moves throughout all networks**

EnGarde Protects Critical Infrastructure down to the Sensor Level

How Does Sensor Vulnerability Impact Industry?

Reported Events:

- Freeport LNG – Force Majeure / Human Error
- Colonial Pipeline

Implications - Cyber Insurance

- March 26, 2023 – Lloyds of London will no longer insure against Nation-State Attacks,

Reasoning:

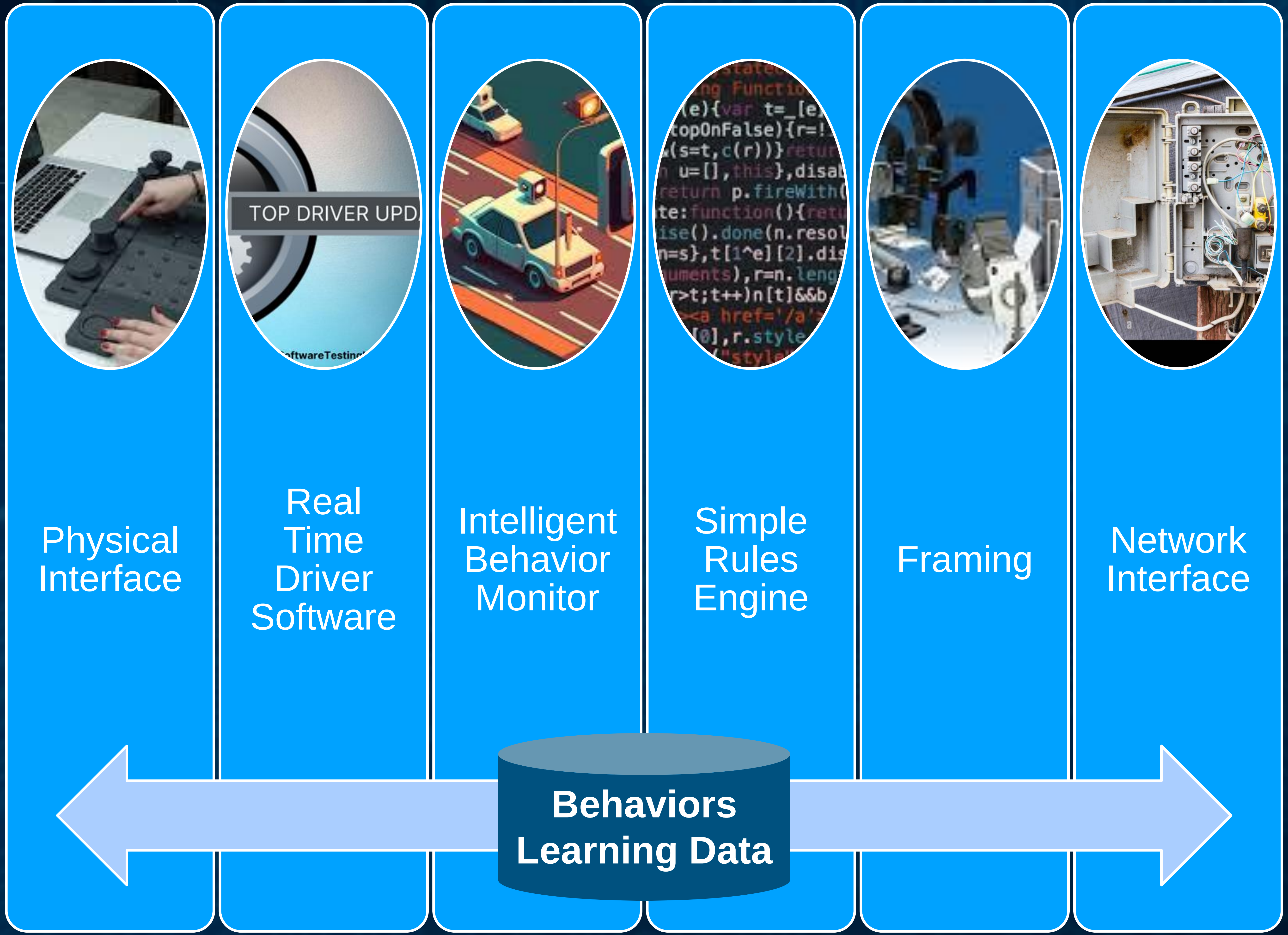
- Lack of security controls on IoT Sensors throughout industry

Not Protecting Sensors is Costly!

Above Sources: Multiple Government and Industry Cybersecurity Reporting

The EnGarde Simple Process Model
Next Steps to Incorporate Machine Learning

Sensor



Physical Interface

Real Time Driver Software

Intelligent Behavior Monitor

Simple Rules Engine

Framing

Network Interface

Behaviors Learning Data

Network Monitoring/ Controller

Real-Time Processing in Memory for Real-Time Monitoring

ENGARDE

Value Propositions and Final Thoughts

- *It all comes down to protecting data and the network…beyond encryption (Zero Trust)…it's authenticity of data, devices, and users*
- *Simplicity of design with minimal manager and user intervention (alerts, updates, etc.)*
- *Current hub and spoke design is not meeting achieving optimum network defense*
- *Mesh design/deployment with MACSec protocols with machine learning will fundamentally change how we do network security*
- *We designed our products so your network can protect you, not you having to protect your network*

- *QUESTIONS…*

*Military-Grade Network Cloaking • 18 Years with **Zero Breaches***

ENGARDE

YOUR GUARD WITHIN

Contact:
EnGarde Technologies Inc.
6671 S. Las Vegas Blvd.
Building D, Suite 210
Las Vegas Nevada, 89119

Phil Klevorick (Co-CEO)
Phil@EnGardetech.com
808.800.7253

100% American Made 100% American Owned Veteran Led