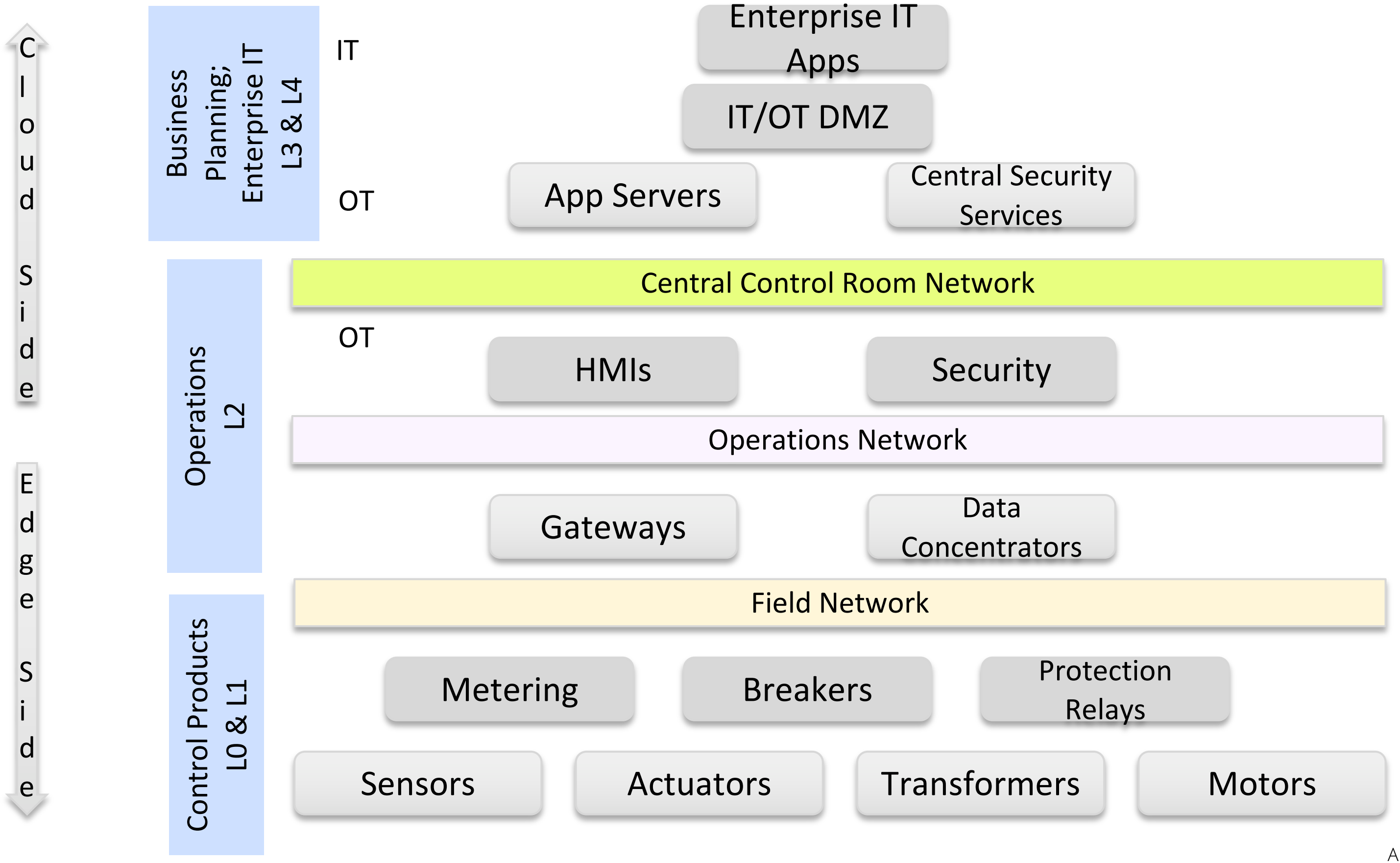
AmberFlux

Cyber Security Offerings
For
ER&D NIPP Pitch Session
Schneider Electric Challenge

AmberFlux EdgeAI Pvt Ltd, India
Scalarr Inc., USA

The energy sector IT/OT Infrastructure

Adapted from Schneider Electric Presentation



Cloud Side

Edge Side

Business Planning; Enterprise IT L3 & L4

IT

Enterprise IT Apps

IT/OT DMZ

OT

App Servers

Central Security Services

Operations L2

Central Control Room Network

OT

HMIs

Security

Operations Network

Gateways

Data Concentrators

Control Products L0 & L1

Field Network

Metering

Breakers

Protection Relays

Sensors

Actuators

Transformers

Motors

but...connected devices are prone to security threats

- Many OT devices are not equipped to handle security. Highly vulnerable to threats
- OT/IT convergence – Fraudsters leverage IT techniques to target OT
- If the internet fails, operations may halt
- Legacy systems connecting to OT/IT and to IoT
- Heterogeneous systems, multi-vendor environments, lack of adherence to standards
- Lack of skills, evolving business processes

Use of EdgeAI for OT/IT security can help

EdgeAI is about enabling AI on the device or near to the device that is generating the data

IOT, 5G driving the need for placing compute, analytics and storage closer to where the data is getting generated

EdgeAI speeds up decision making, makes data processing secure, improves user experience & lowers costs

EdgeAI delivers direct value in threat detection, incident management etc.

OT cyber security requirements

OT Visibility & Asset Management

Visibility into all IT, IOT, IIOT assets, processes and connections

Network Segmentation

Visibility and automatic mapping of network zones

Threat and Anomaly Detection

Asset profiling, traffic weeding, anomaly detection, realtime alerts

Vulnerability Management

Common Vulnerability Exposure data; identify, prioritize and remediate vulnerabilities

Remote Incident Management

Incident detection, remediation

Data Management & Controls

Scalable data management, access and other controls, analytics reports, realtime actuation

AmberFlux

AmberFlux EdgeAI software offers deep, differentiated & valuable technology suite to lead EdgeAI adaptability

Technology backed by several years of R&D and patents (3 granted in US & 1 Granted in India and a few more under examination)

EdgeAI Products

Purpose specific EdgeAI products that can be deployed & managed directly on edge devices securely

Integration with IT/OT

Enterprise integration with existing IT/OT infrastructure

Hardware & Network Agnostic

Supports multiple Edge, IOT, SOC hardware; Works for any edge cloud service

AmberFlux EdgeAI Product Bundles

AmberFlux Opus

EdgeAI software that runs on devices/equipment

Sense, learn & act at the edge

AmberFlux Concerto

Edge & Cloud enterprise containers and APIs for integration with IT/OT

Data & Protocol transformations

Opus Dashboard

Orchestration & Visualization software to manage millions of edge devices.

Remote deployment, updates & operations for EdgeAI

AmberFlux Market Recognition

Since incorporation in Aug 2020

EDGE COMPUTING WORLD

Selects AmberFlux as a finalist at Start Up of the Year 2020 competition

(Oct 2020) - www.edgecomputingworld.com

STL PARTNERS

Names AmberFlux as one of the 60 Edge Computing Companies to Watch in 2021

(Apr 2021) – www.stlpartners.com

CYBERSECURITY CENTRE of EXCELLENCE

Selects AmberFlux for its incubation center

(Sep 2021) - https://ccoe.dsci.in/

DEEP TECH hello tomorrow PIONEERS

Shortlists AmberFlux as one of the deep tech pioneers for Industrial IOT

(Sep 2021) - https://hello-tomorrow.org/

T-AIM

Selects AmberFlux to Telangana AI Mission Revv Up Accelerator

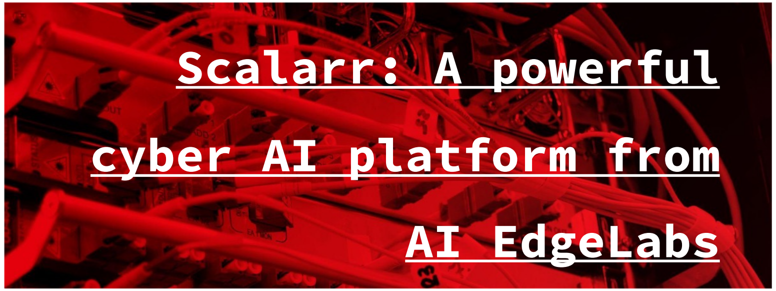
(Apr 2022) - https://ai.telangana.gov.in/revv-up/

Intel® Network Builders

Selects AmberFlux as Intel Network Builders Winners' Circle Member & Partner Alliance Gold Level

(Apr 2022) - https://networkbuilders.intel.com/ecosystem

AmberFlux is bringing a comprehensive cyber security solution in partnership with Scalarr Inc, a US company



Scalarr: A powerful cyber AI platform from AI EdgeLabs

Threat detection & Incident Management

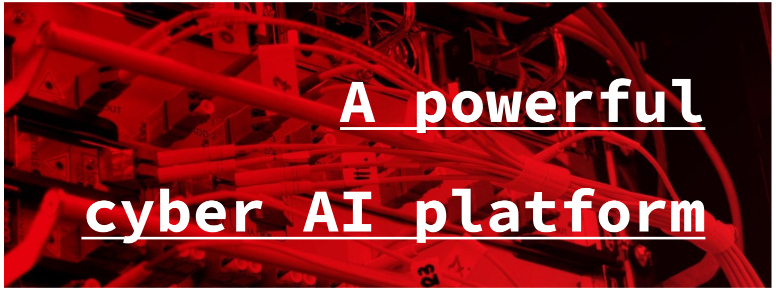
+

AmberFlux

Opus Dashboard

Visualization & Orchestration

What is AI EdgeLabs?



A powerful cyber AI platform

that brings advanced network visibility, early threat detection and automated incident response and remediation for Edge/IoT

Shell zynga Yandex iFarm JOOM

AI EDGE
LABS

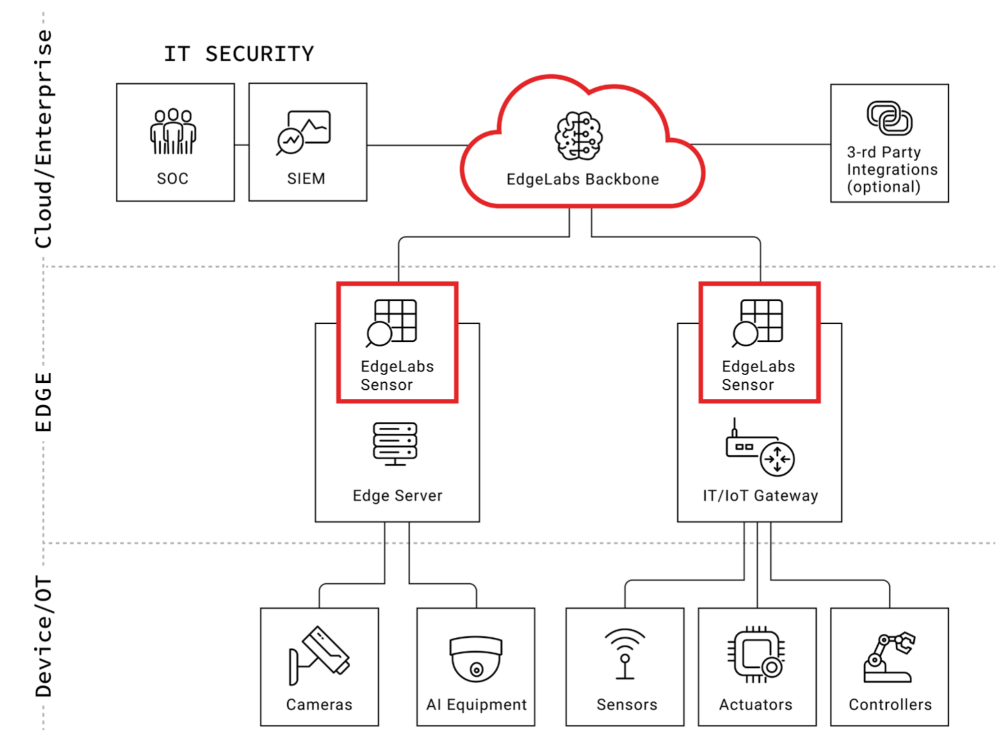
Detect and respond to Edge and connected IoT security threats in real-time with **99% accuracy**

SCALARR
Powered by Scalarr

AI EdgeLabs features

- **Edge/IoT Threats Detection:** DDoS, Botnets, Hacking, Malware and other threats and attacks detection.
- **Edge/IoT Threats Prevention/ Autonomous Cyber AI:** Dynamic firewalling, blocking, automated shutdown protocols.
- **AI-Based Anomaly Detection:** Reinforcement Learning approach for 0-day threat and attacks detection.
- **IoT / OT Assets Discovery:** Agentless discovery of the connected assets.
- **Network Visibility & Observability:** Dashboard and integration with SIEM systems.

Integration Structure

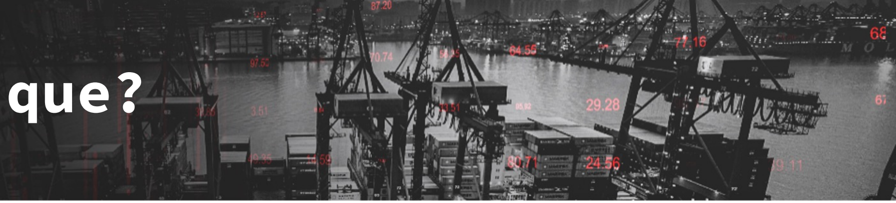


Network Functions

On-premise / MEC security
Eg. private LTE/5G network, SD WAN/universal CPE services, API gateways, etc

Cloud-edge compute infrastructure security
Eg. distributed core and RAN network functions, virtual CMTS, etc

What Makes AI EdgeLabs Unique?



1. Edge-Focused Design & Performance:

- Autonomous lightweight (**less than 100mb**) Rust-based agent deployed on the Edge/on-Prem workload.
- **High performance with low OS footprint: only 5% of CPU is used.**
- Ready for unstable connectivity and offline work including AI models.
- Possibility to deploy inside enterprise without data transfer externally.

2. Advanced Cyber AI Detection

- A mix of **reinforcement learning**, supervised, unsupervised machine learning algorithms and rule sets → **99% of accuracy, ultra-low false positives rate.**
- Optimized Edge RL **we are able to zero-day attacks and threats with highest accuracy possible.**
- **‘Cold start’ models** to analyze data and provide with the outputs right away.
- Self-learning algorithms to ensure personalized level of security.

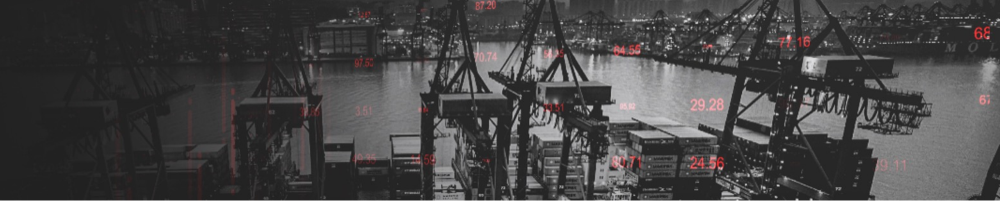
3. Autonomous Cyber AI. Security as an embedded flawless feature

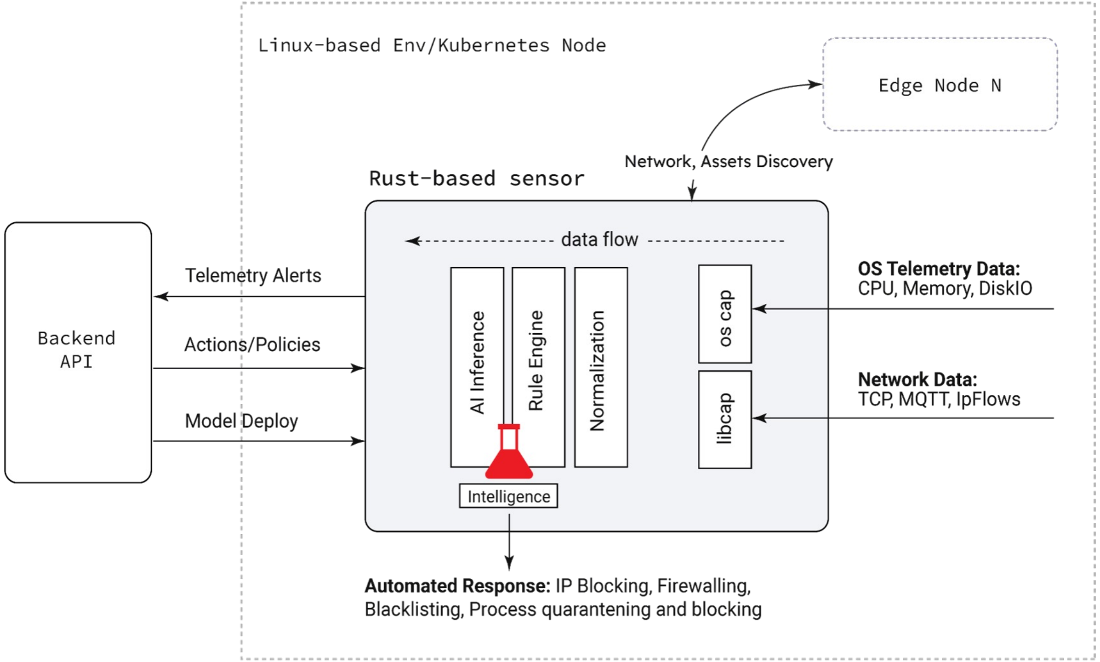
- Early threat prevention.
- Automated incident response and remediation.
- **Automated shutdown protocols & policies.**

4. Simple solution to protect complex systems & critical infrastructure

- **Linux-native, container-based or K8S deployments.**
- Real-time visibility across your network.
- Robust reports and posture.
- ‘Smart’ alerting.

The AI.Sensor





Linux-based Env/Kubernetes Node

Edge Node N

Network, Assets Discovery

Rust-based sensor

data flow

AI Inference

Rule Engine

Normalization

os cap

libcap

Intelligence

Backend API

Telemetry Alerts

Actions/Policies

Model Deploy

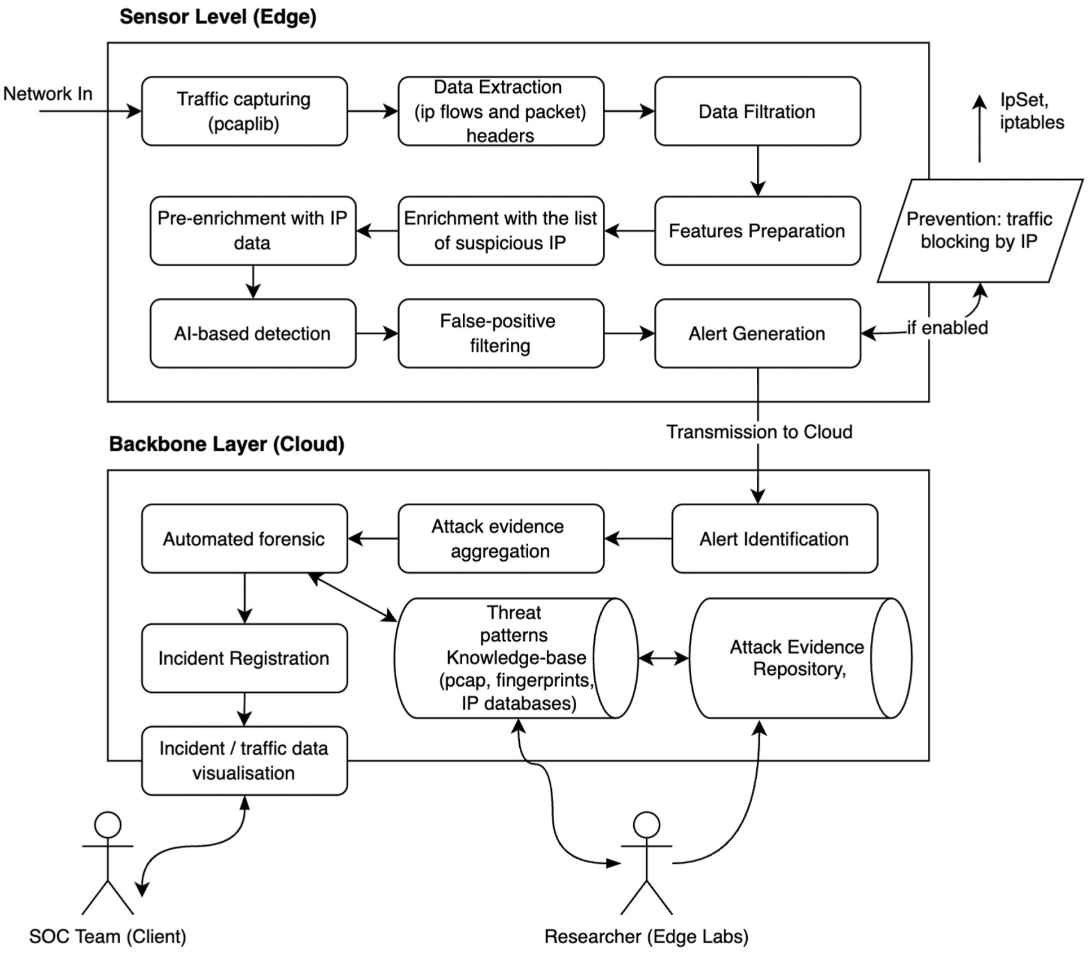
OS Telemetry Data: CPU, Memory, DiskIO

Network Data: TCP, MQTT, IpFlows

Automated Response: IP Blocking, Firewalling, Blacklisting, Process quarantening and blocking

Requirements and Limitations

1. AI Inference and processing should be **lightweight** (Rust, ONNX compression)
2. Ready for offline work and **unstable connectivity** (buffering and autonomous models)
3. Should have a **simple integration** (Linux, Kubernetes support)
4. Should work to **unique traffic picture** on the client side node (RL, Autoencoders)



Sensor Level (Edge)

Network In

Traffic capturing (pcaplib)

Data Extraction (ip flows and packet) headers

Data Filtration

Features Preparation

Enrichment with the list of suspicious IP

Pre-enrichment with IP data

AI-based detection

False-positive filtering

Alert Generation

if enabled

Prevention: traffic blocking by IP

IpSet, iptables

Transmission to Cloud

Backbone Layer (Cloud)

Alert Identification

Attack evidence aggregation

Automated forensic

Incident Registration

Incident / traffic data visualisation

Threat patterns Knowledge-base (pcap, fingerprints, IP databases)

Attack Evidence Repository,

SOC Team (Client)

Researcher (Edge Labs)

DETECTION WORKFLOW

Sensor Level (Edge):

- Traffic data extraction (Rust),
- Feature preparation (Rust),
- Compressed AI-models
- Prevention stack
- Alert escalation

Backbone Level:

- Incidents registration,
- Core API,
- Enrichment Pipeline;
- Patterns Knowledge Base
- Dashboard;

AmberFlux
Opus Dashboard
Security

Visibility into connected devices

Drill downs

Orchestration rules and policies

Orchestration controls

Response controls

Security Features/Functions

Device Visibility

- Device attributes
- Device recognition
- Logs and logs tally
- Managed, unmanaged assets

Anomaly & Risk Assessment

- Vulnerability mapping
- Multi threat assessment
- Device risk scores
- Regulatory compliance assessments

Policy Enforcements

- Behavior segregations (trusted/untrusted)
- Multi-list (blocked, allowed, unknown, suspected)
- Automatic updates
- Random checks & escalations management

Proactive/Reactive Threat Prevention

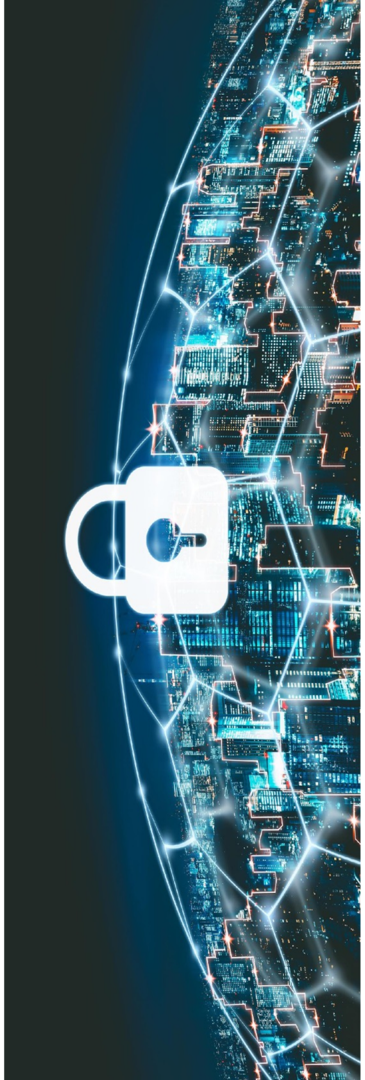
- Detection of threats (known, unknown via payloads)
- Device risk group categories
- Command & control theft management
- Fast detection, response

Orchestration

- Workflow, deployment management
- Order management

3rd Party integrations

- Inbound/outbound APIs
- Component/micro-product approach



AmberFlux

Thank You!

Contact:

Muralidhar Goparaju, CEO, AmberFlux, GoparajuM@amberflux.com
Raghavendra Rao Gudipudi, COO, AmberFlux, Raghu@amberflux.com
Isaiah Arias, AI EdgeLabs, Isaiah.arias@edgelabs.ai