midwest architecture community collaboration

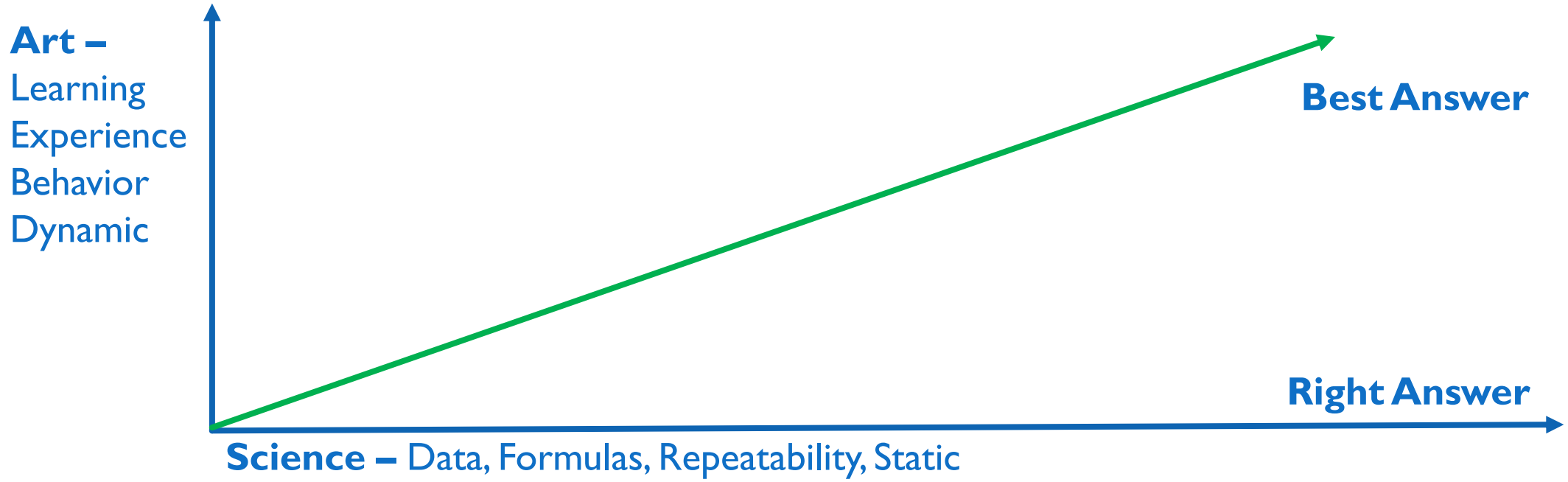
# LESSONS LEARNED USING AI TO IMPROVE NETWORK PERFORMANCE & SECURITY

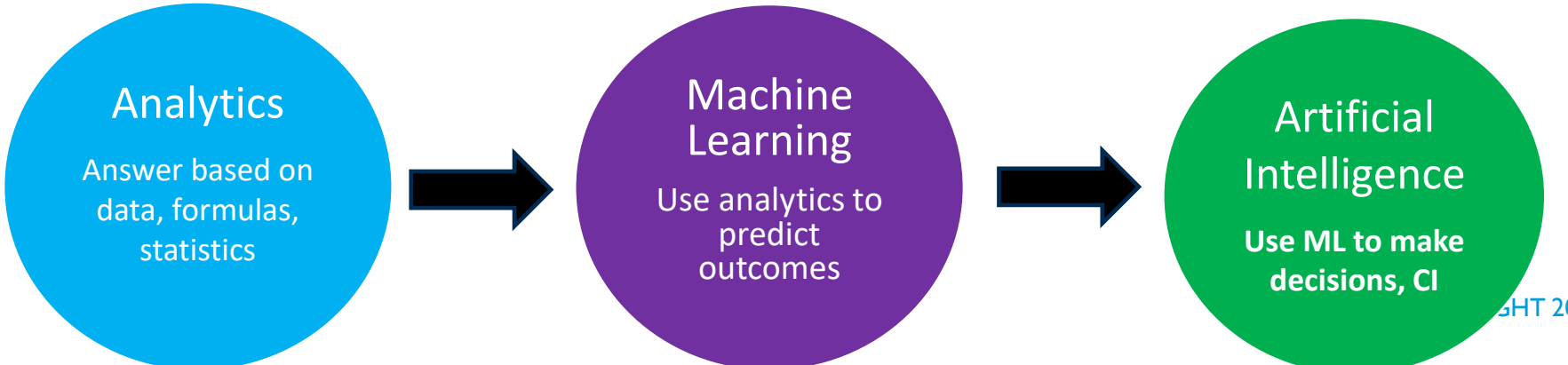
NOVEMBER 9, 2023

SORELL SLAYMAKER
PRINCIPAL CONSULTING ANALYST
TECHVISION RESEARCH

COPYRIGHT 2023 MACC

# AI LEVEL SET – THE RIGHT ANSWER VERSUS THE BEST ANSWER



# LESSON #1 – USE AI TO DO THE BASICS WELL

**Use Case:** Global Manufacture Needing Additional Operational Technology (OT) Security

**Business Drivers:** Cyber-security risk management and keeping cyber-insurance costs in-line which had gone from $20M to $30M in the past year

**Process:** Bring in 3rd party consultants/experts, gather requirements, go to RFP, select vendor, pilot, rollout, and continuously improve including measuring and managing results.

**Why AI** – Dynamic environment with limited resources so needed a system to help prioritize projects and keep the enterprise risk score up to date in near real-time.

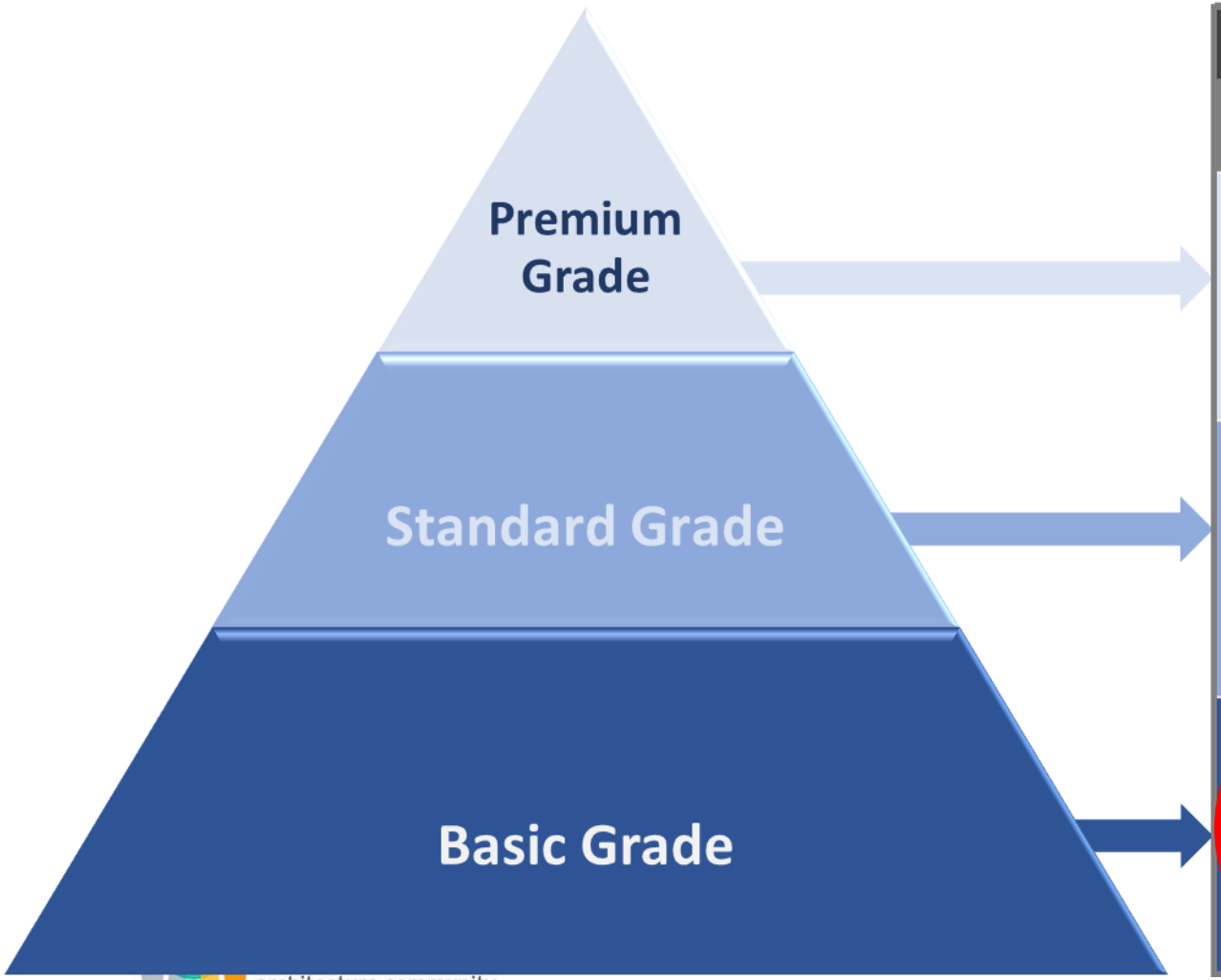
**Lessons Learned:** While AI-Ops and SOC are maturing, using AI to do foundational work such as building an active inventory and real-time risk assessment still has a ways to go. If you do not do the basics well, the fancy stuff and the value are minimized.



midwest architecture community collaboration

COPYRIGHT 2017 MACC

# LESSON #1 – USE AI TO DO THE BASICS WELL - CONTINUED




| Characteristics for each Security Tier | | | | | |
|---|---|---|---|---|---|
| Inventory | Network | UTM | SPAN | IAM | SIEM |
| LPA | Zero Trust | Proxy, DLP | Active | MFA (6x) | AI/ML Baseline, Anomaly Detection |
| Dynamic | Micro-Segments | IPS | Passive E-W | NAC | Event ID, Classifica-tion |
| Static | OT Segment | Firewall | Passive N-S | MAC | Logging |



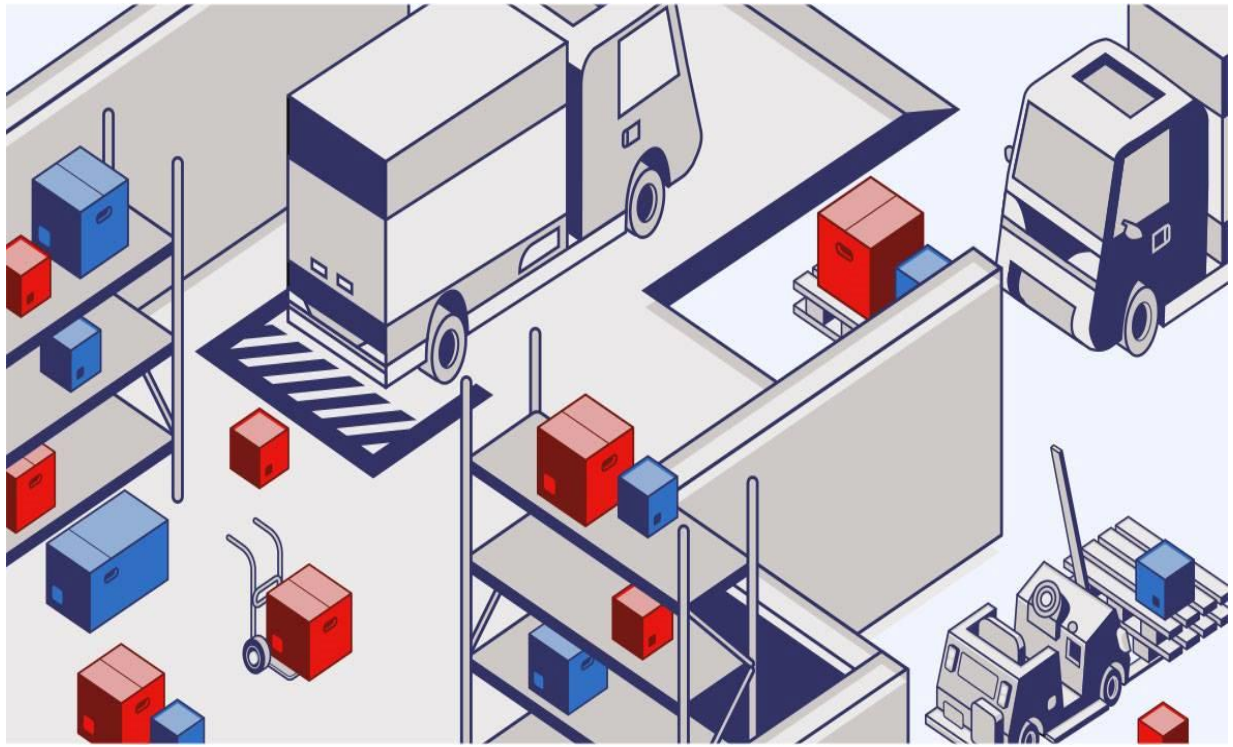
architecture community collaboration

COPYRIGHT 2017 MACC

# LESSON #1 – USE AI TO DO THE BASICS WELL - CONTINUED

## Inventory Management

1) **Identify everything connected**
   a) Device manufacture & function
   b) OS and patch version
   c) Protocols used
   d) Criticality
2) **Sort who is talking to what**
   a) IP addresses and TCP/UDP Ports
   b) Sessions and volumes
3) **Identity and access management**
   a) Local
   b) Remote
4) **Risk Score**





midwest architecture community collaboration

COPYRIGHT 2017 MACC

# LESSON #1 – USE AI TO DO THE BASICS WELL - CONTINUED

**Detect insider threats**

- Analyze behavior of users with access to sensitive data
- Detect unusual activities

**Natural next step in threat detection**

- Signatures → Correlation → ML
- All are needed to mitigate modern threats

**Higher fidelity risk scoring**

- Risk assignment based on deviation instead of static rules or event count

**Intuitive analysis of alarms**

- Generalized behavior profiles enable rapid response
- Alarms natively include user and entity context



midwest architecture community collaboration

 © 2023 AT&T Intellectual Property - AT&T Proprietary (Internal Use Only)

COPYRIGHT 2017 MACC

# LESSON #2 – UPGRADE TO PRECISION TIME PROTOCOL

**Use Case:** Large Financial Institution Driving Down Fraud

**Business Drivers:** Cyber-security thieves are getting smarter and the amount they are stealing is growing by double digits per year.

**Process:** Bring in 3rd party consultants/experts, gather requirements, go to RFP, select vendor, pilot, rollout, and continuously improve including measuring and managing results.

**Why AI** – The ability to tracking a transaction across 100+ systems and identify anomalies and risks in near-real time and automatically keep tuning to minimize false positives.

**Lessons Learned:** When dealing with applications that span hundreds of systems, upgrading from Network Time Protocol (NTP) which is accurate to 20-30ms to Precision Time Protocol which is accurate to 10-15 micro-seconds helps with event correlation and shotgun attacks.





COPYRIGHT 2017 MACC

# LESSON #3 – CORRELATION BETWEEN SYSTEMS YIELDS RESULTS

**Use Case:** Large U.S. Retailer

**Business Drivers:** Improve WiFi experience for shoppers and track their behavior within a physical store while also helping reducing theft

**Process:** Bring in 3rd party consultants/experts as a trusted advisor to help optimize investment

**Why AI** – Merging video data with network data provided business insights not seen before.

**Lessons Learned:** Tons of data and being able to anonymize the data while also tracking patters could predict things like flash theft in ways not see before. End-to-end monitoring provided a more consistent end user experience.





COPYRIGHT 2017 MACC

# LESSON #4 – ITS ALL ABOUT THE DATA

**Use Case:** All clients that I have worked with in the past few years

**Business Drivers:** Better return on technology investment to help drive measurable business results in a dynamic digital economy.

**Process:** Bring in 3rd party consultants/experts as a trusted advisor to help optimize investment

**Why AI** – The next evolution in processing data

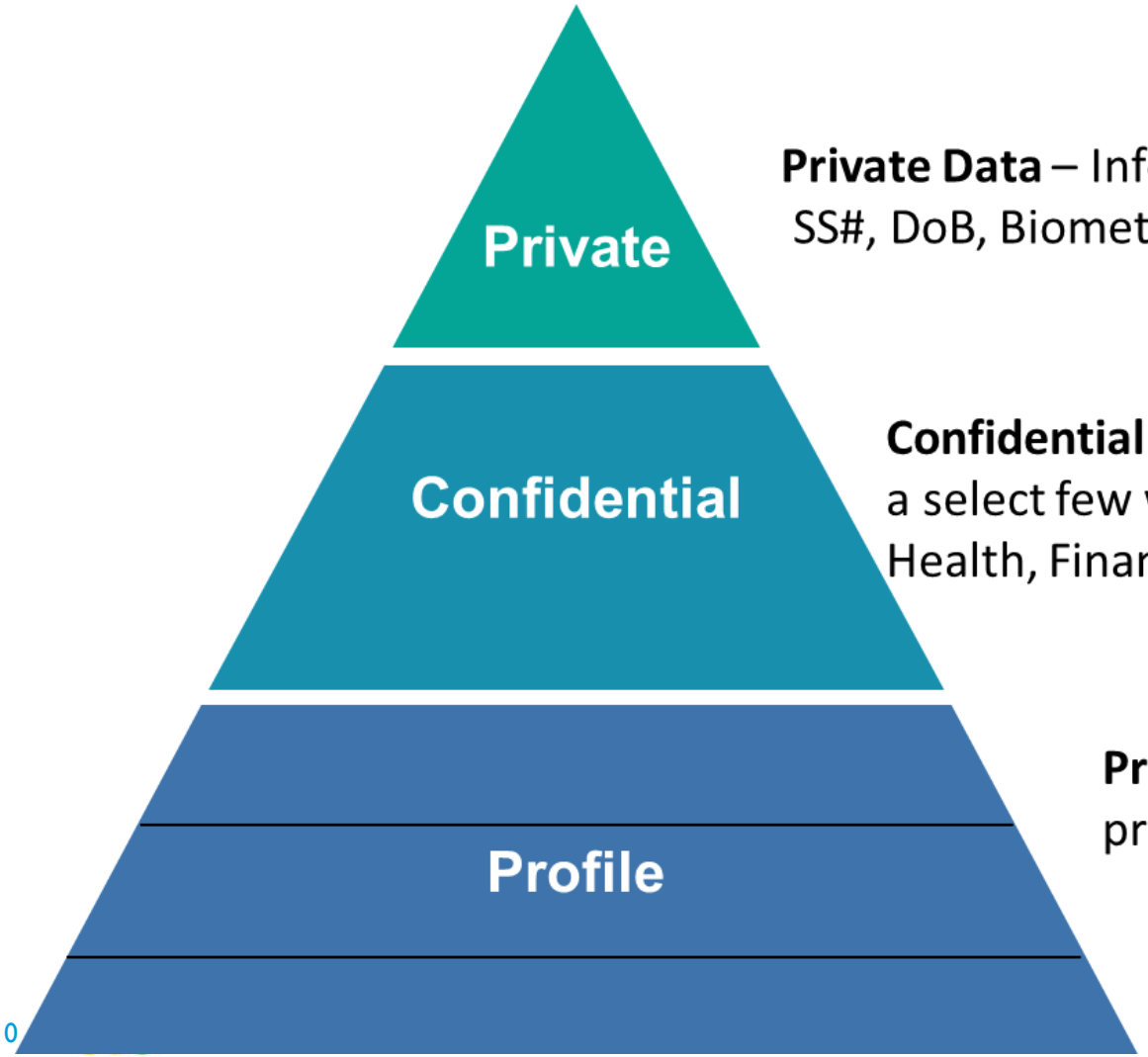
**Lessons Learned:** Tons of data and being able to anonymize the data while driving outcomes is half science and half art. It is amazing how much data can be collected.





COPYRIGHT 2017 MACC

# LESSON #4 – DATA CONTINUED – DATA CLASSIFICATION



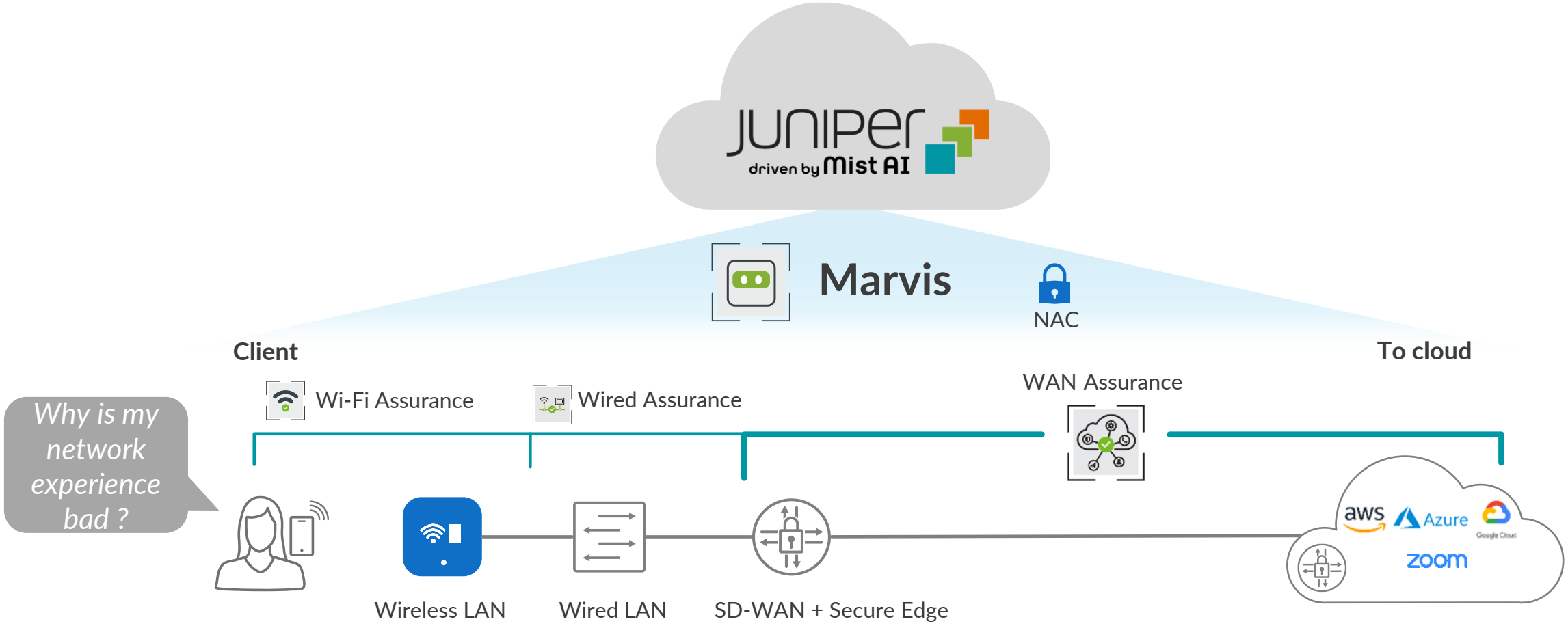

**Private Data** – Information used to personally identify someone.
SS#, DoB, Biometrics, Username/password

**Confidential Data** – Information that is secret, yet shared with a select few with express consent of the individual.
Health, Financial, Legal

**Profile Data** – Information about someone's preferences, location, history, connections


COPYRIGHT 2017 MACC

# MY JOURNEY WITH AI – STARTED WITH JUNIPER MIST

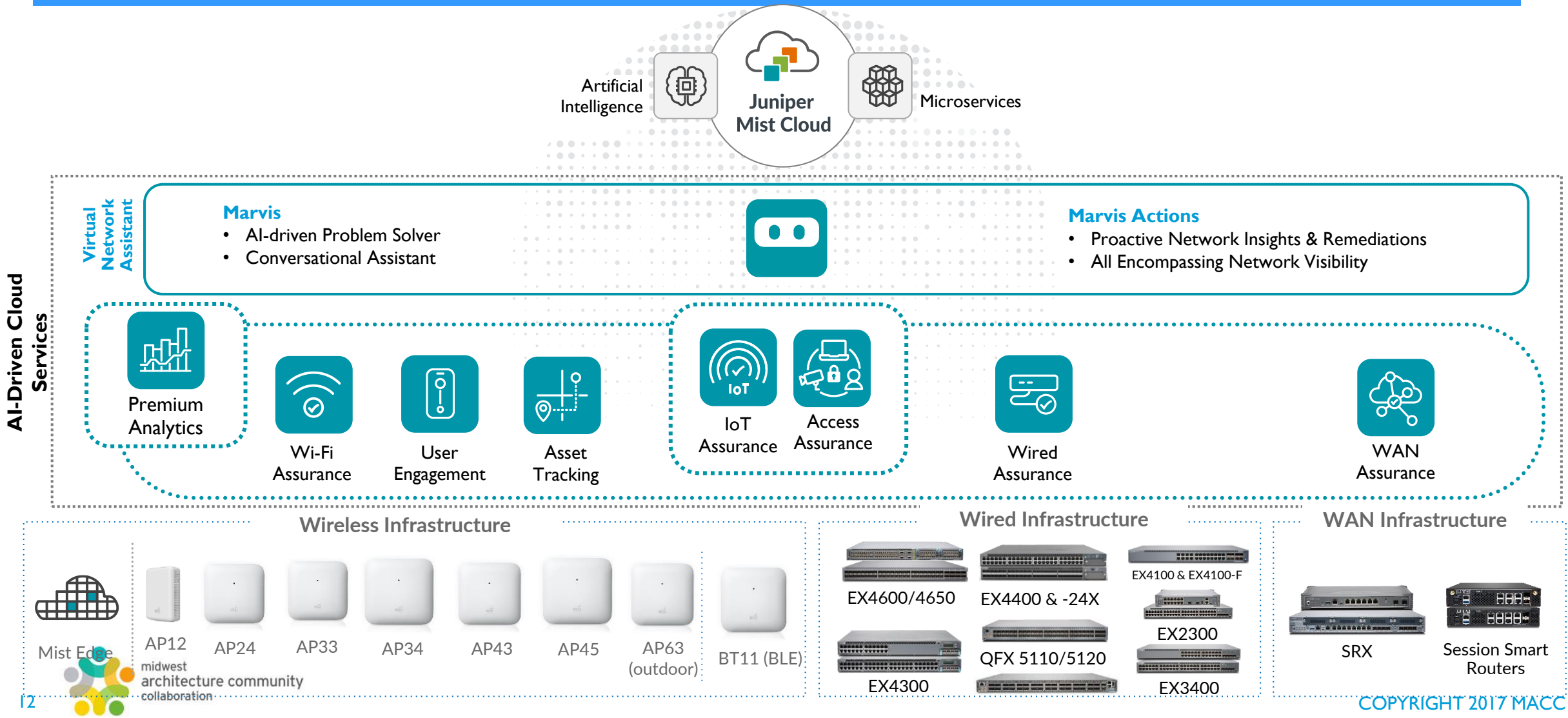





midwest architecture community collaboration

COPYRIGHT 2017 MACC

# MY JOURNEY WITH AI – STARTED WITH JUNIPER MIST - CONTINUED




midwest architecture community collaboration



COPYRIGHT 2017 MACC

# MY JOURNEY WITH AI – STARTED WITH JUNIPER MIST - CONTINUED

Marvis Client: Android, Windows

3rd Party

Graph DB

WAN-Marvis

Graph ML

NLP/ NLU

*(natural language processing/understanding)*

User Sentiment

WAN Self Healing

WAN Self Optimization

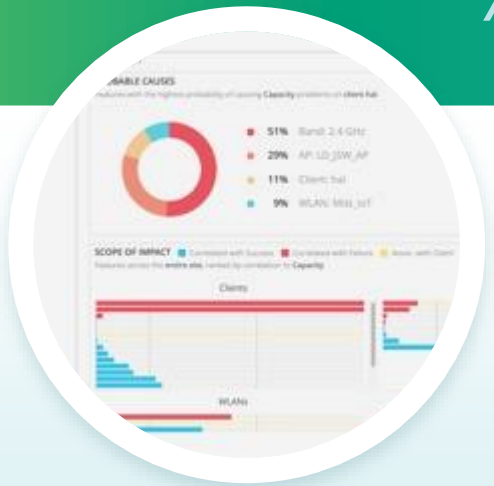
Data

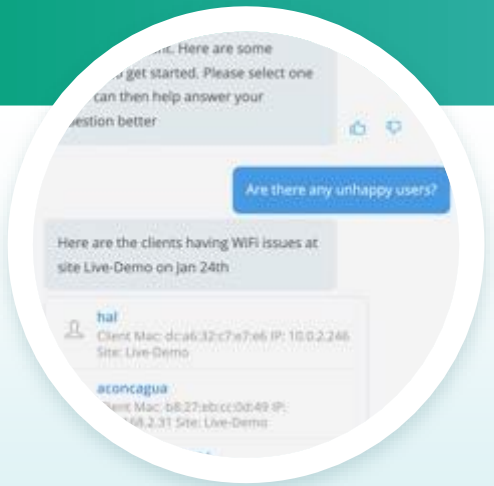
AI Primitives Event Timeline

Data Science Toolbox

Conversational Assistant

Self Driving Action Framework





CLIENT / WIRED / WIRELESS / WAN / SECURITY / MIST EDGE / 3RD PARTY

DISTRIBUTED SOFTWARE ARCHITECTURE



collaboration

COPYRIGHT 2017 MACC

# WHAT IS NEXT? – USING AI AS A COACH & AUTOMATE CONFIGS

AI is automation that can do tasks on par with human domain experts that requires cognitive skills.

## DEEP LEARNING

**LSTM- Neural Network**
Time Series Anomaly Detection, NLP, Geo-Spatial Analysis.

**Unsupervised Learning**
Location

**GAI / LLM / Transformer**
Marvis Conversational Assistant.

**Shapley**
Feature assessment.

**Reinforcement Learning**
RRMv

## ARTIFICIAL INTELLIGENCE

## MACHINE LEARNING

**K-Means Clustering**
Environment Learning.

**XGBoost / Decision Tree**
Throughput Prediction.

**Domain Expertise Classification**
Service Level Metrics, Event Timeline.

**Decision Tree**
AP / Switch Health, DHCP Health, Coverage Hole, bad cable.

**Probabilistic Graphical Models**
Root Cause Analysis.

**Mutual Information**
Feature Discovery.

**Online ARIMA**
Time Series Anomaly.

**Logistic Regression**
AP / Switch Health.

**Temporal Correlation**
Root Cause Analysis.

**Bayesian Inference**
Persistently Failing Clients, Auto Placement of AP.



midwest architecture community collaboration

COPYRIGHT 2017 MACC



midwest architecture community collaboration

COPYRIGHT 2017 MACC