Machine Learning and Security

By

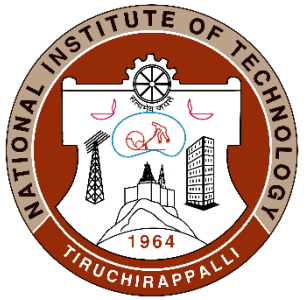
Dr. B. Janet


INTERCONNECTED WORLD

COMPLEX ORGANIZATIONS

DEMANDING USERS

Machine Learning?



"Learning is any process by which a system improves performance from experience."

- Herbert Simon

Definition by Tom Mitchell (1998):

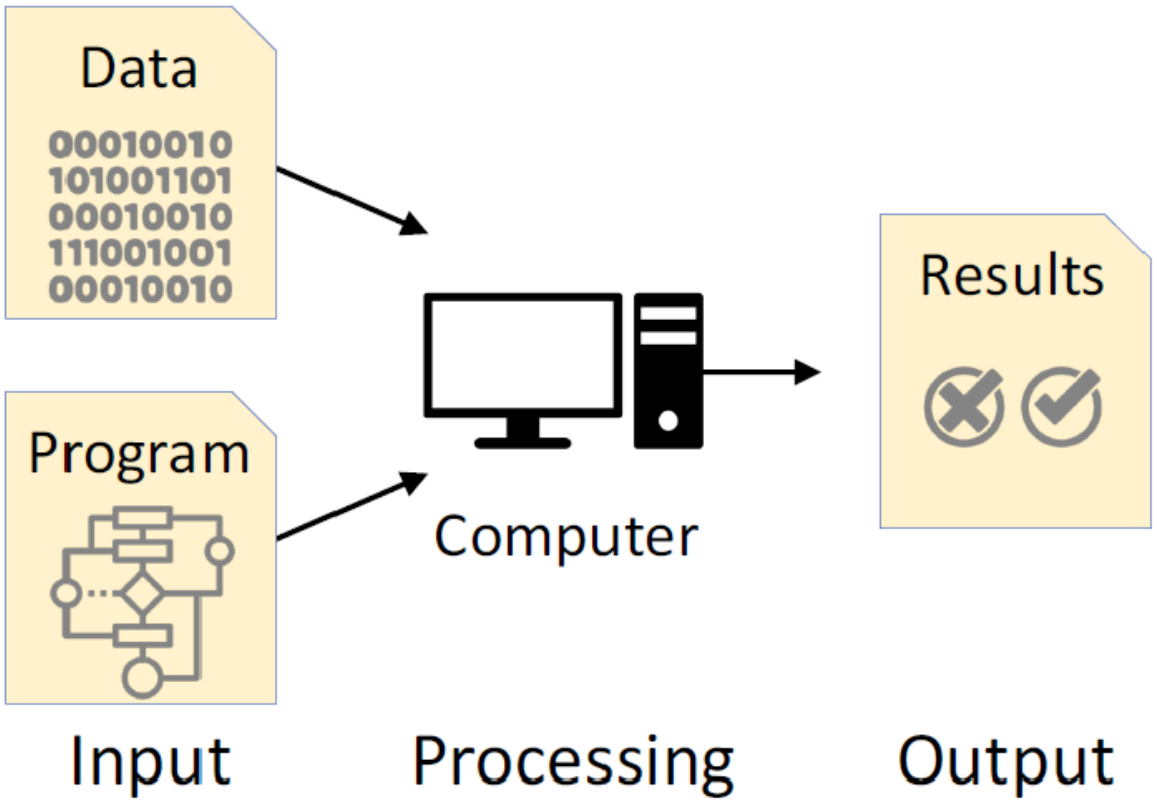
Machine Learning is the study of algorithms that

- improve their performance P
- at some task T
- with experience E.

A well-defined learning task is given by <P, T, E>.

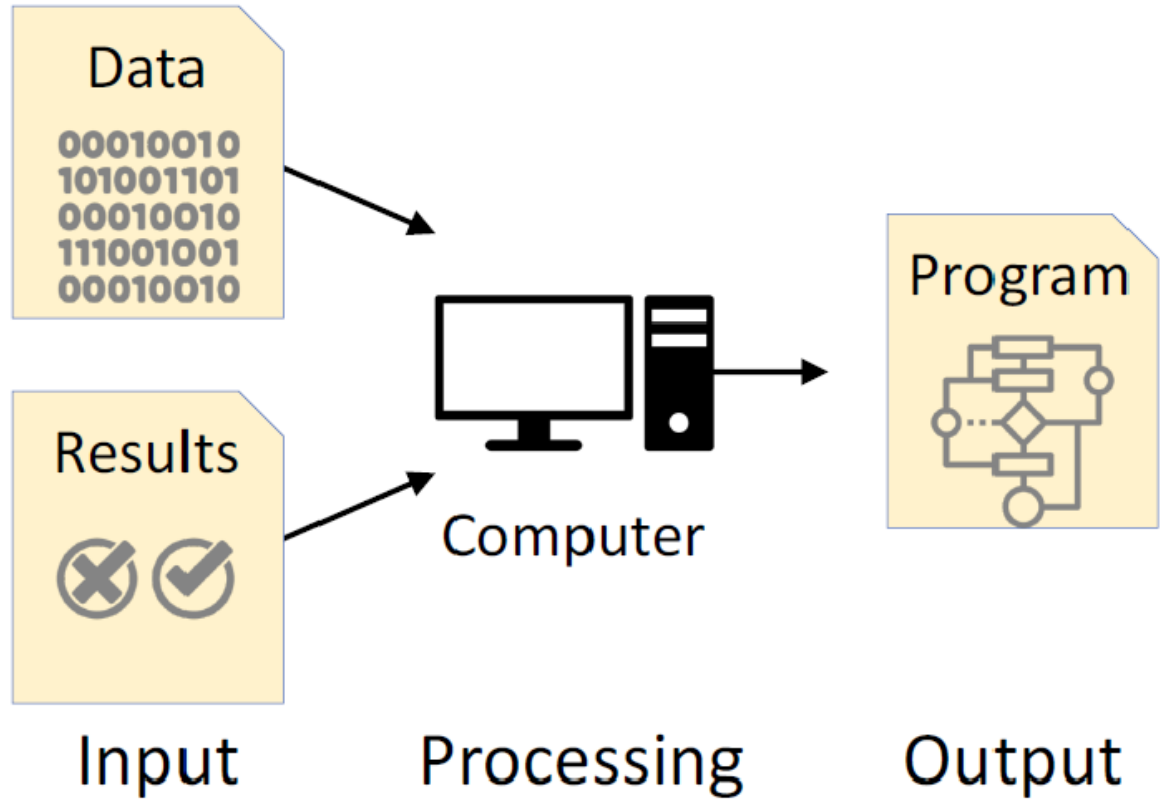
Traditional Programming

Works well when we know how to specify the program



Machine Learning

Needed when we don't know how to specify the program

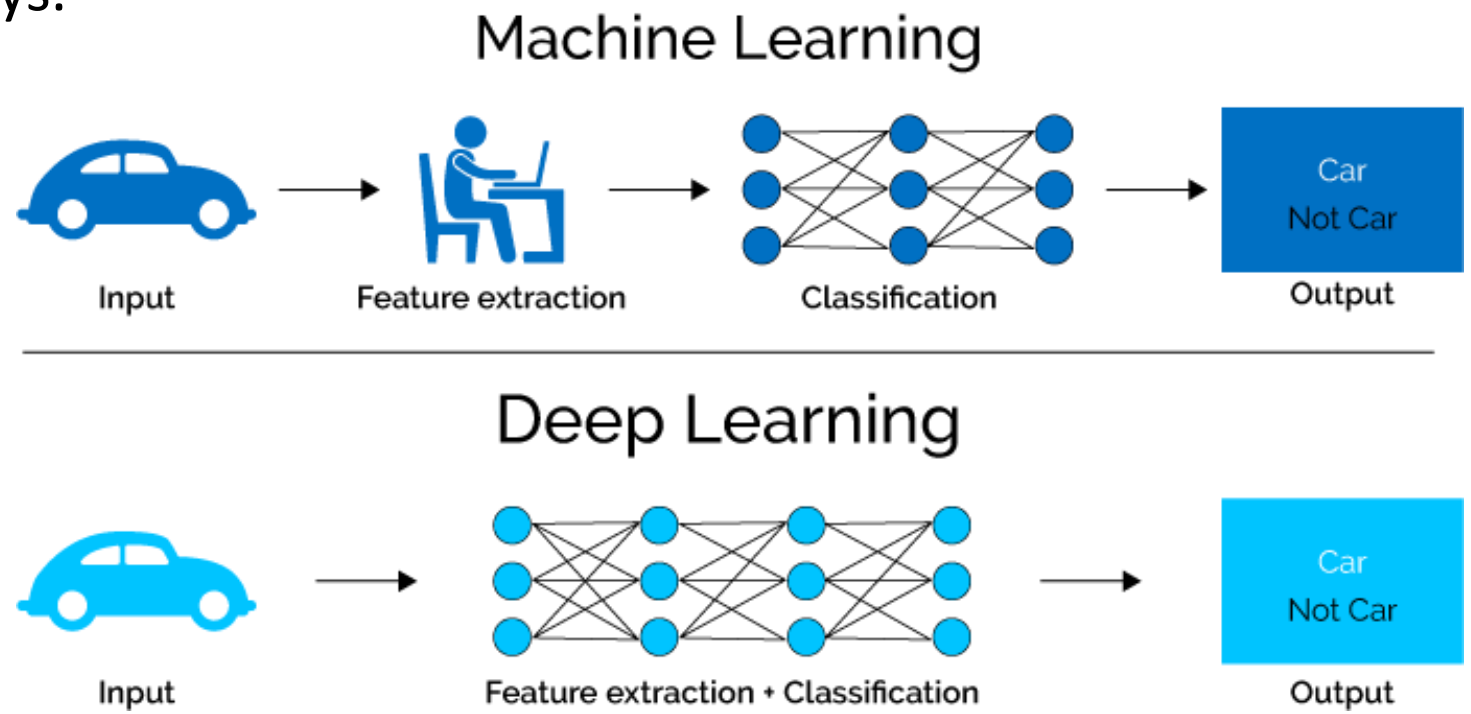


Deep Learning

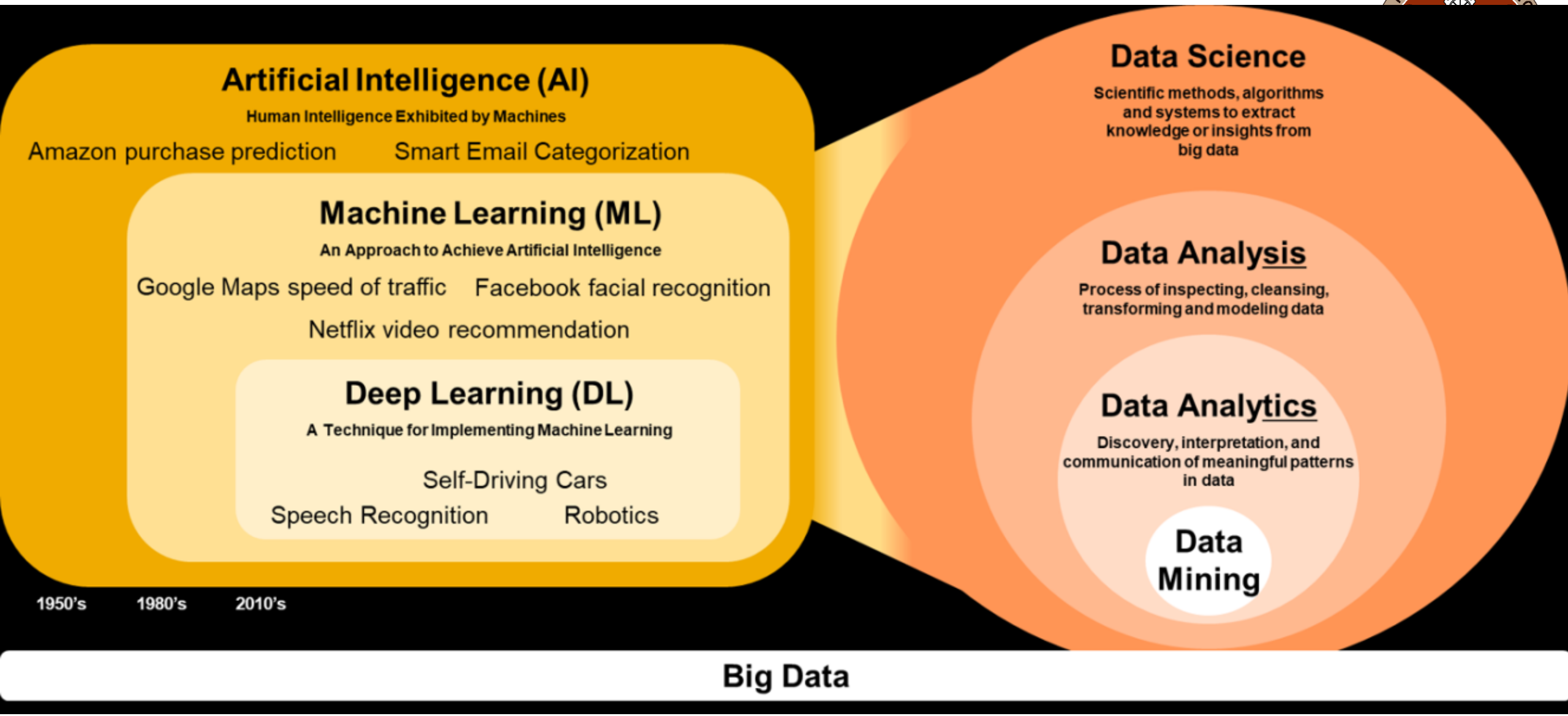
A machine learning subfield of learning **representations** of data. Effective at **learning patterns**.

Deep learning algorithms attempt to learn (multiple levels of) representation by using a **hierarchy of multiple layers**

If you provide the system **tons of information**, it begins to understand it and respond in useful ways.



https://www.xenonstack.com/blog/static/public/uploads/media/machine-learning-vs-deep-learning.png


Artificial Intelligence (AI)
Human Intelligence Exhibited by Machines
Amazon purchase prediction
Smart Email Categorization
Machine Learning (ML)
An Approach to Achieve Artificial Intelligence
Google Maps speed of traffic
Facebook facial recognition
Netflix video recommendation
Deep Learning (DL)
A Technique for Implementing Machine Learning
Self-Driving Cars
Speech Recognition
Robotics
1950's
1980's
2010's
Data Science
Scientific methods, algorithms and systems to extract knowledge or insights from big data
Data Analysis
Process of inspecting, cleansing, transforming and modeling data
Data Analytics
Discovery, interpretation, and communication of meaningful patterns in data
Data Mining
Big Data

IoT scope

- Smart parking
- On-board diagnostic systems
- Sharing information on the road
- ...

- Smart farming
- Preparing the soil
- Monitoring optimal conditions for planting
- ...

- Smart bulbs
- Smart domotic systems
- ...

- Payment & ticketing
- Information exchange
- Location services
- ...

- Smart clothes (Wearables)
- Smart appliances
- Relaxing time
- ...

- Environmental monitoring
- Energy management
- Security services
- ...

- Activity trackers
- Biomedical sensors
- Diseases monitoring
- ...

Data Center IoT Solutions

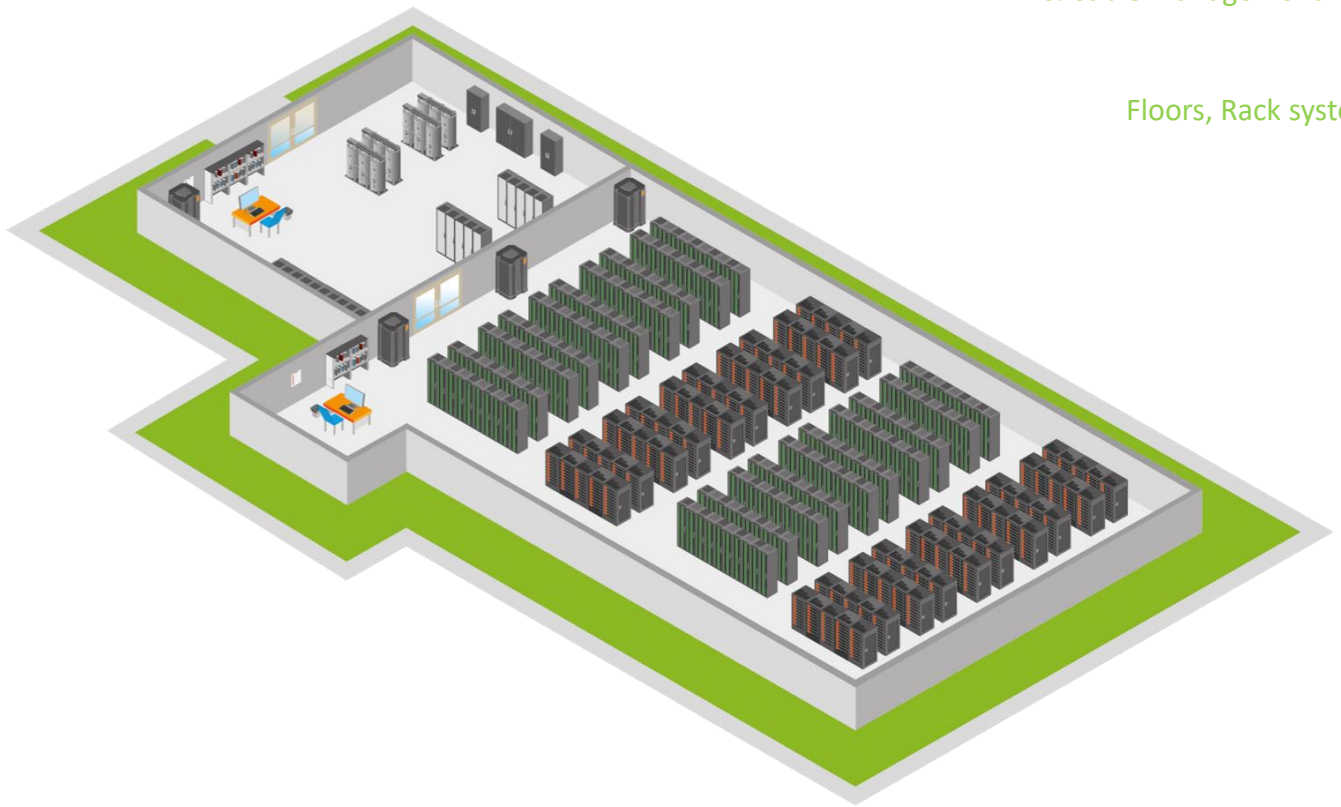
HV/MV & MV / LV
Transformers

MV and LV
Switchboards
& Switchgears

Modular
UPS

Sensors &
Meters

Busway



Network connectivity
& Cable management

Floors, Rack systems

Flexible Air
Containment

Room / Row / Rack
precision cooling

Indirect Free
Cooling

Chillers

Cooling VSD &
Control

Row
Modular
UPS & PDU

Lighting
Control

Access
Control, CCTV

Life Is On Schneider Electric

Industry IoT Solutions

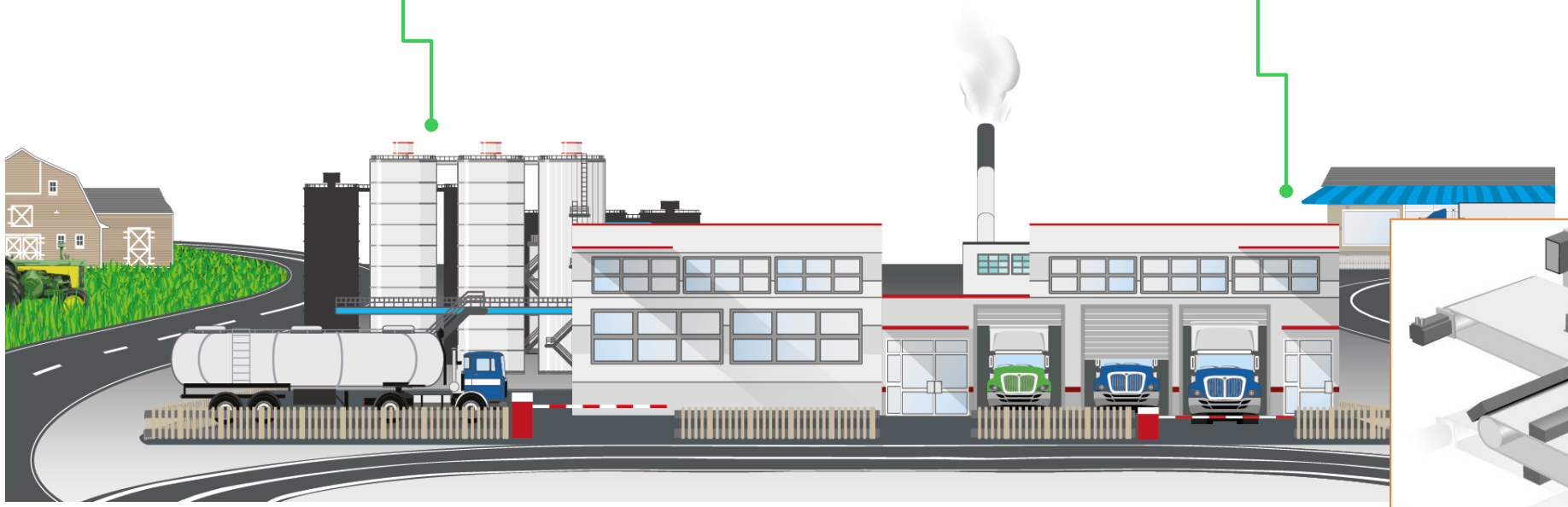
From **design** to **maintenance**, we **improve sustainability & efficiency** of your operations

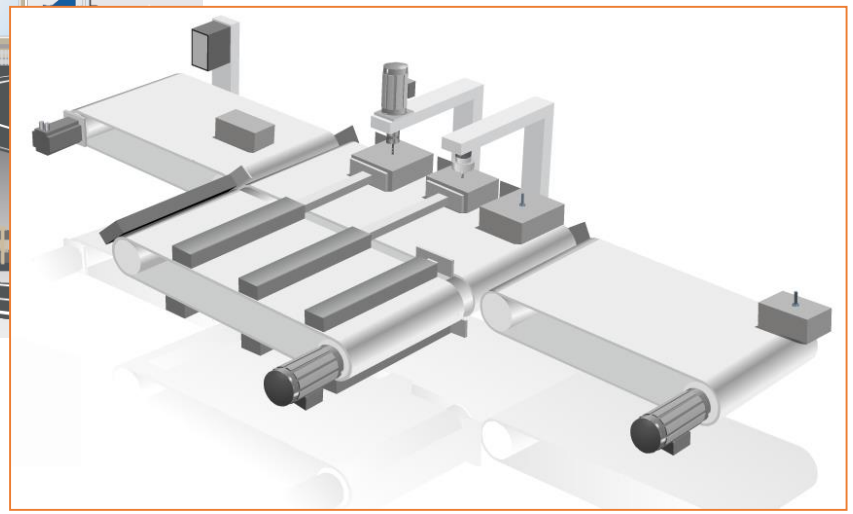
Energy and Sustainability

Improve the sustainability of your operation and reduce your energy bill by 30%.

Process Management

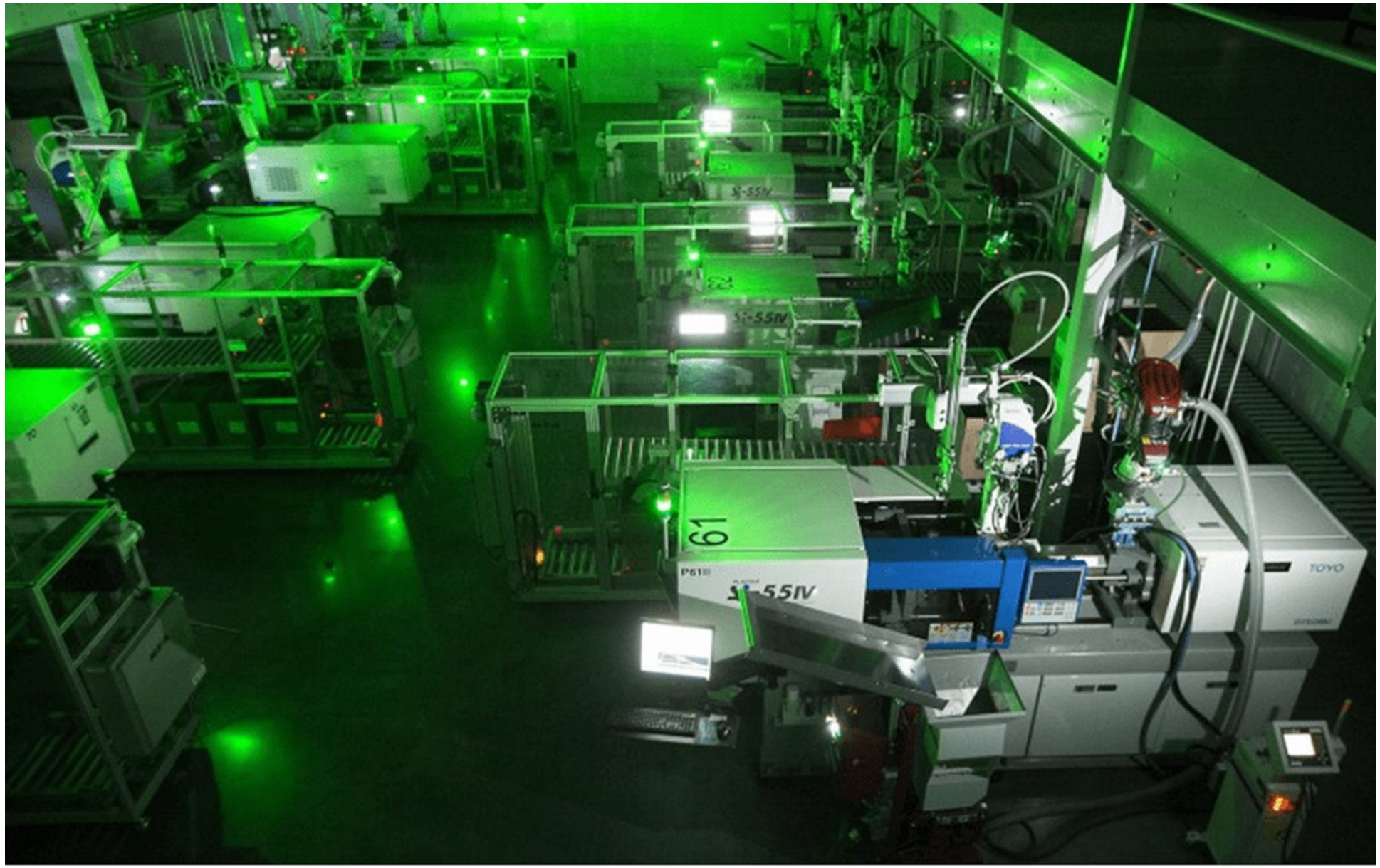
Strive for zero waste while increasing the flexibility on your plant floor.





Life Is On Schneider Electric

Factories


61
TOYO

Smart Grid & Smart City IoT Solutions

Smart Grid Operator
"IT/OT integration from field to control center to enterprise"

Smart Generator
"Producing power efficiently"

Energy Services Provider
"Bridging supply & demand"

Renewable Operator
"Making renewables dispatchable"

- Smart Buildings & Homes
- Smart Energy
- Smart Water
- Smart Mobility
- Smart Public Services
- Smart Data Center
- Smart Integration

Building & Homes IoT Solutions

Buildings:

Smart Electrical Distribution Panels

Building Management System

Energy & Power Management

Power Meters

Homes:

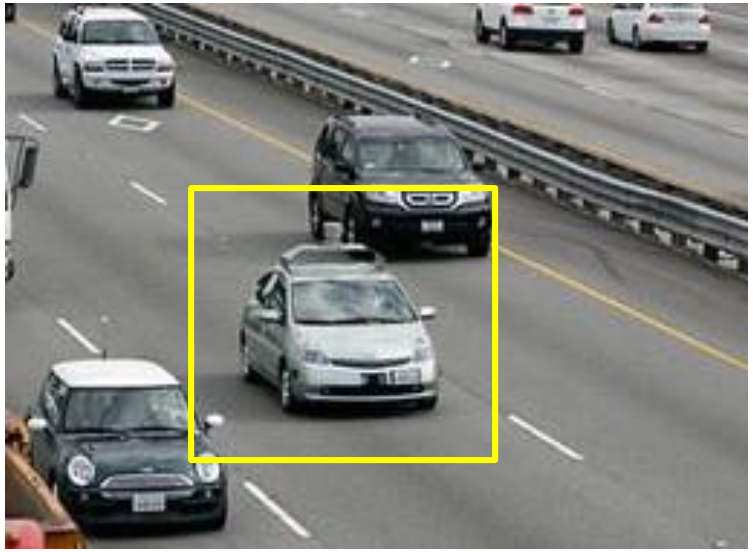
Connected Home System

Home Automation

Lighting & Temperature Control

Life Is On | Schneider Electric

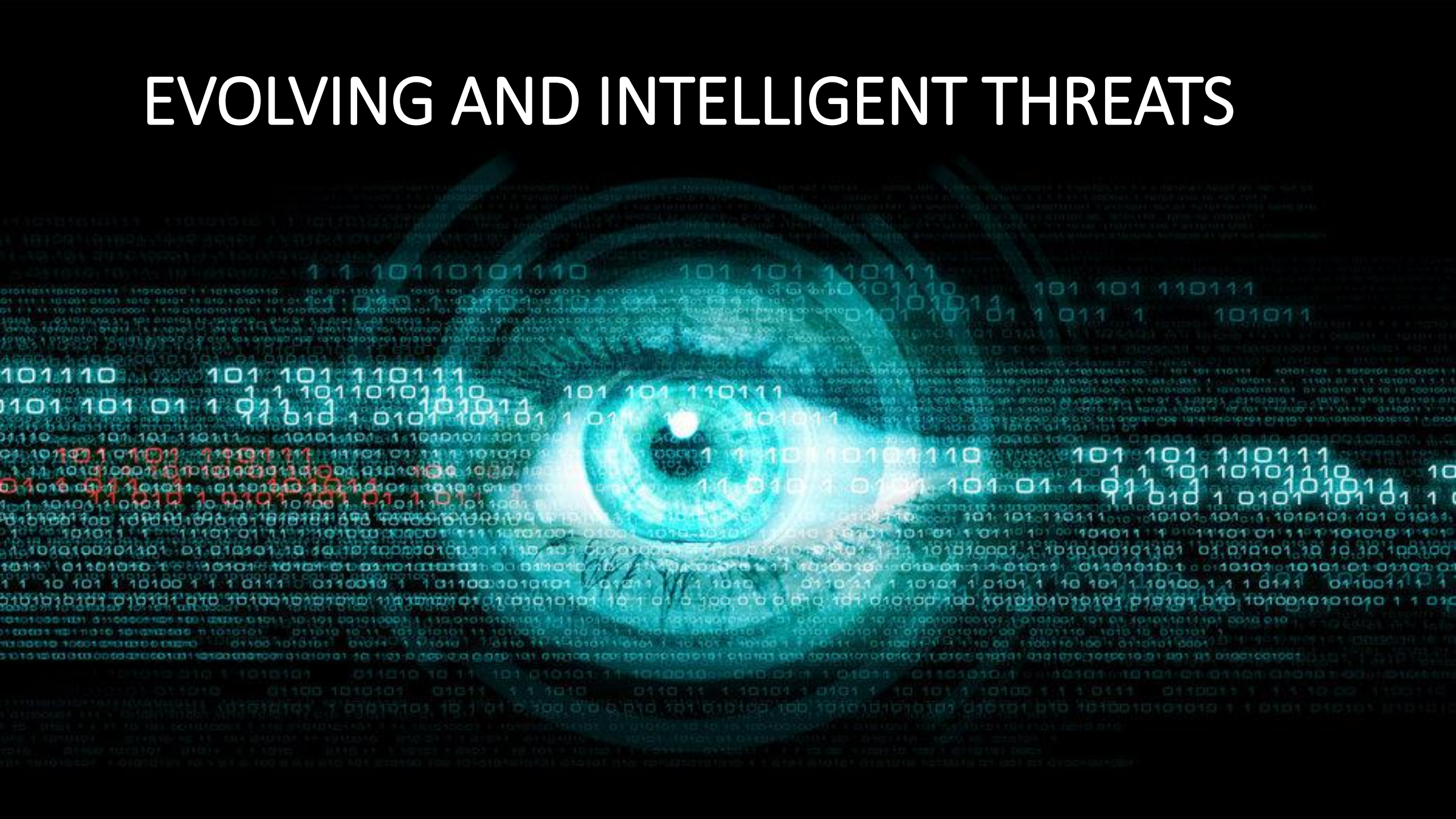
Autonomous Cars



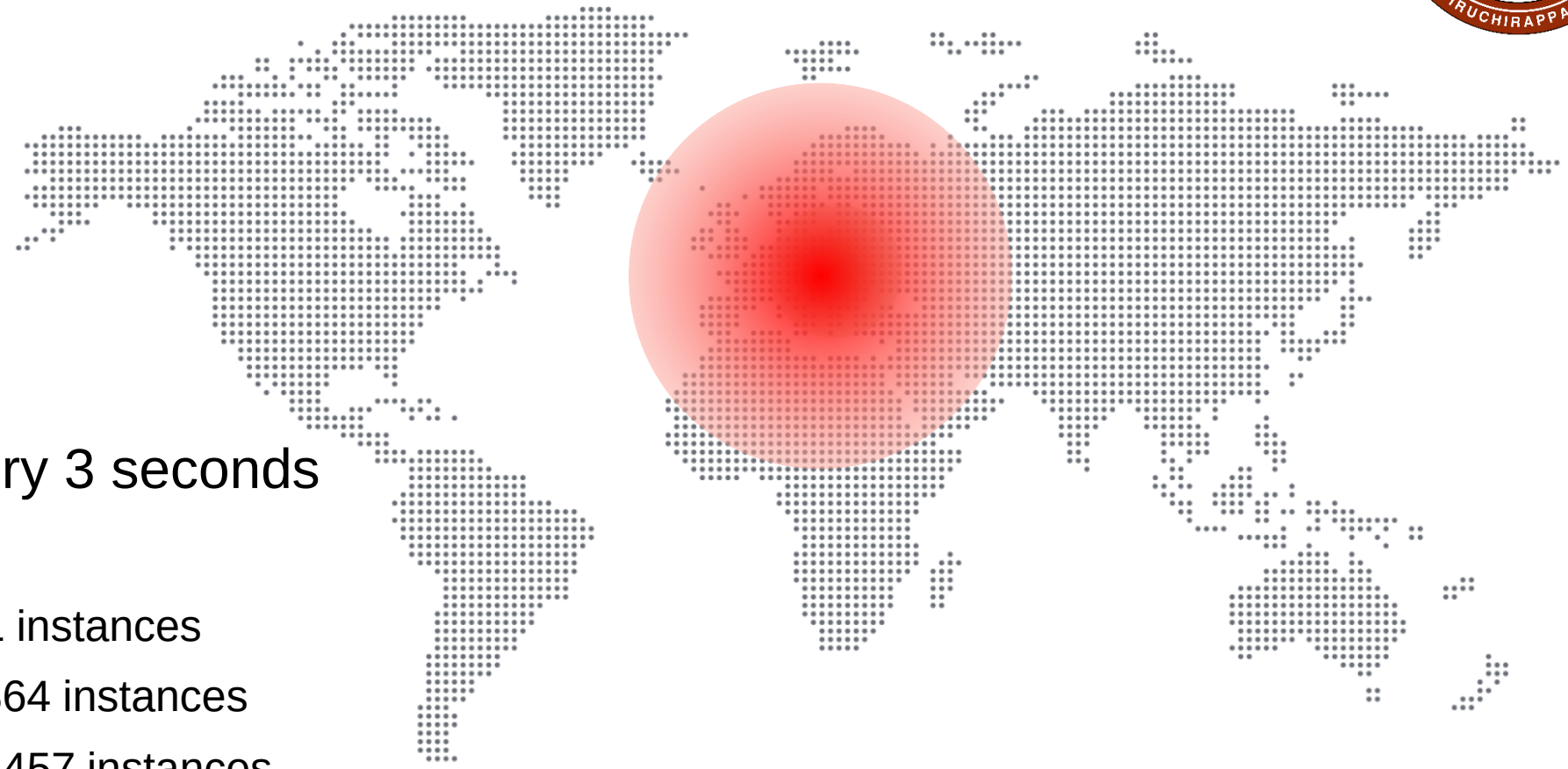
- Nevada made it legal for autonomous cars to drive on roads in June 2011
- As of 2013, four states (Nevada, Florida, California, and Michigan) have legalized autonomous cars

Penn's Autonomous Car →
(Ben Franklin Racing Team)

EVOLVING AND INTELLIGENT THREATS



SOPHISTICATED MALWARE SPREADING



New infection every 3 seconds
After….

1 minute = 2,021 instances

15 minutes = 9,864 instances

30 minutes = 45,457 instances

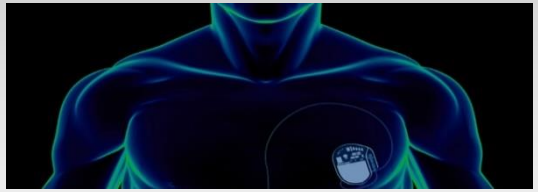
HIGHLY AUTOMATED ADVERSARIES

IoT risk and security awareness is increasing … and highlighting the need for security research and development.

Vehicle Hacking

http://bit.ly/1s0m4Hv
http://bit.ly/1TOt2h5

Global Positioning System Spoofing



Healthcare Device & Information Hacking

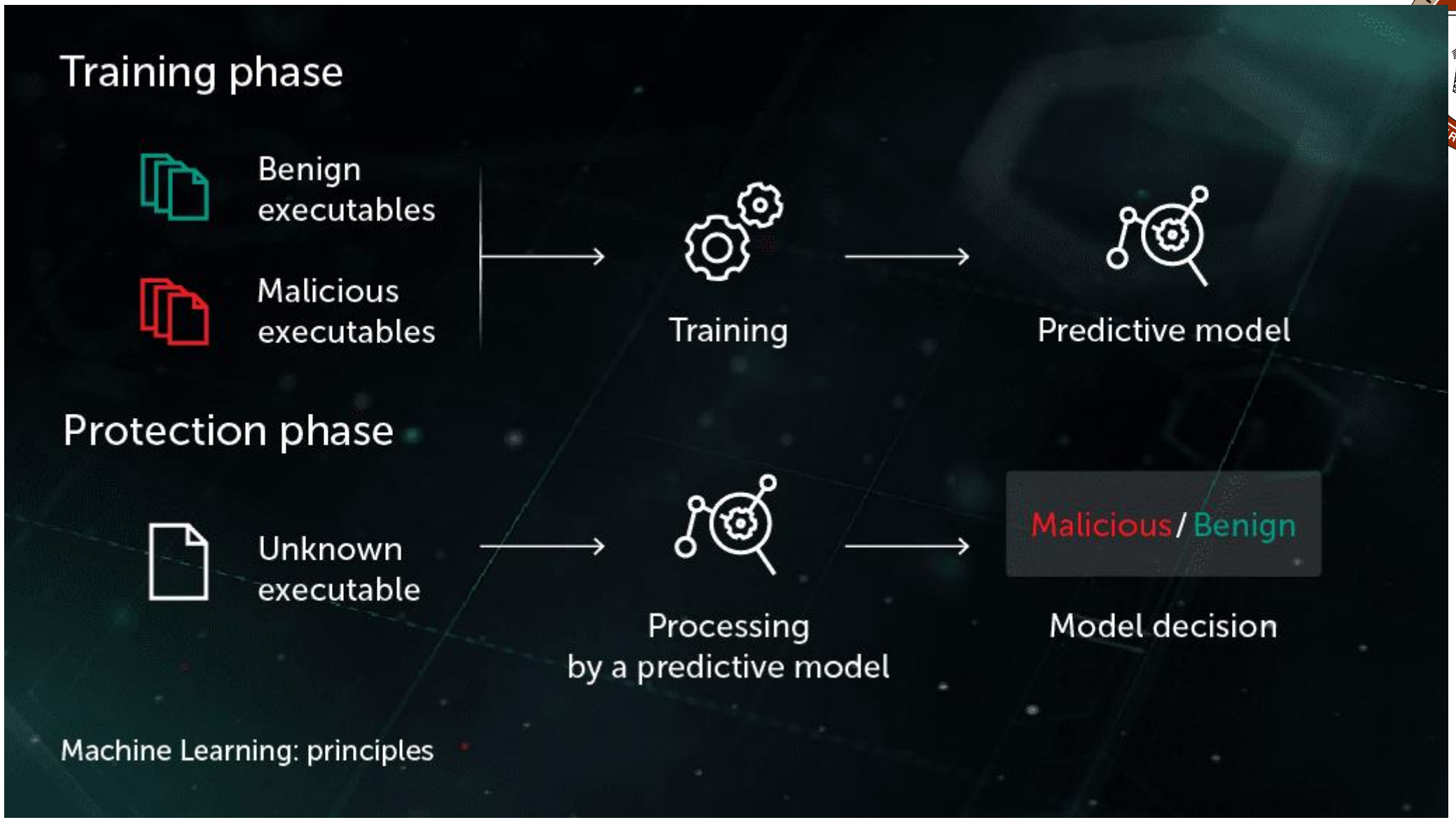
http://bit.ly/1EJnTjv

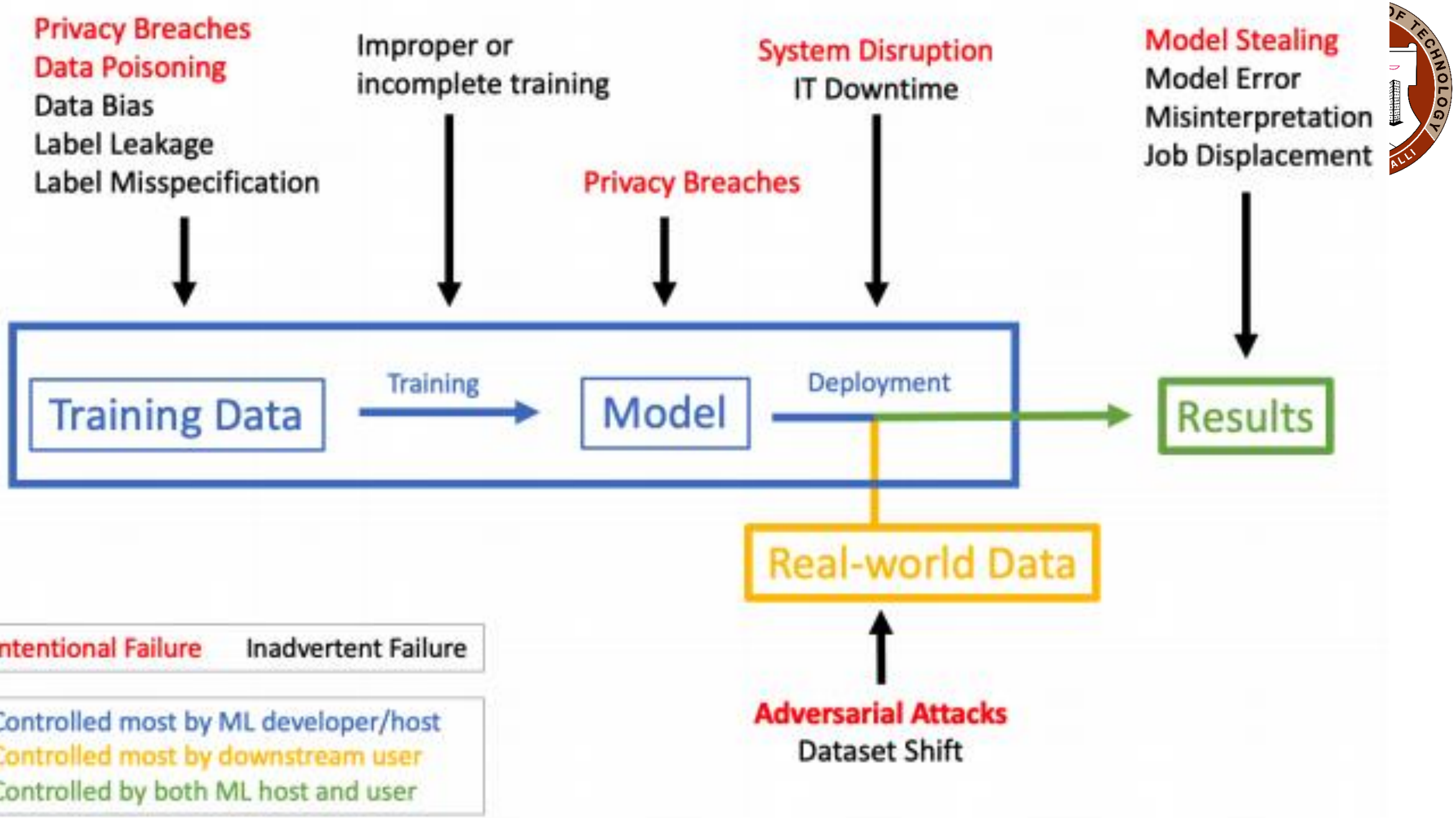
Industrial Hacking

Smart Home Hacking

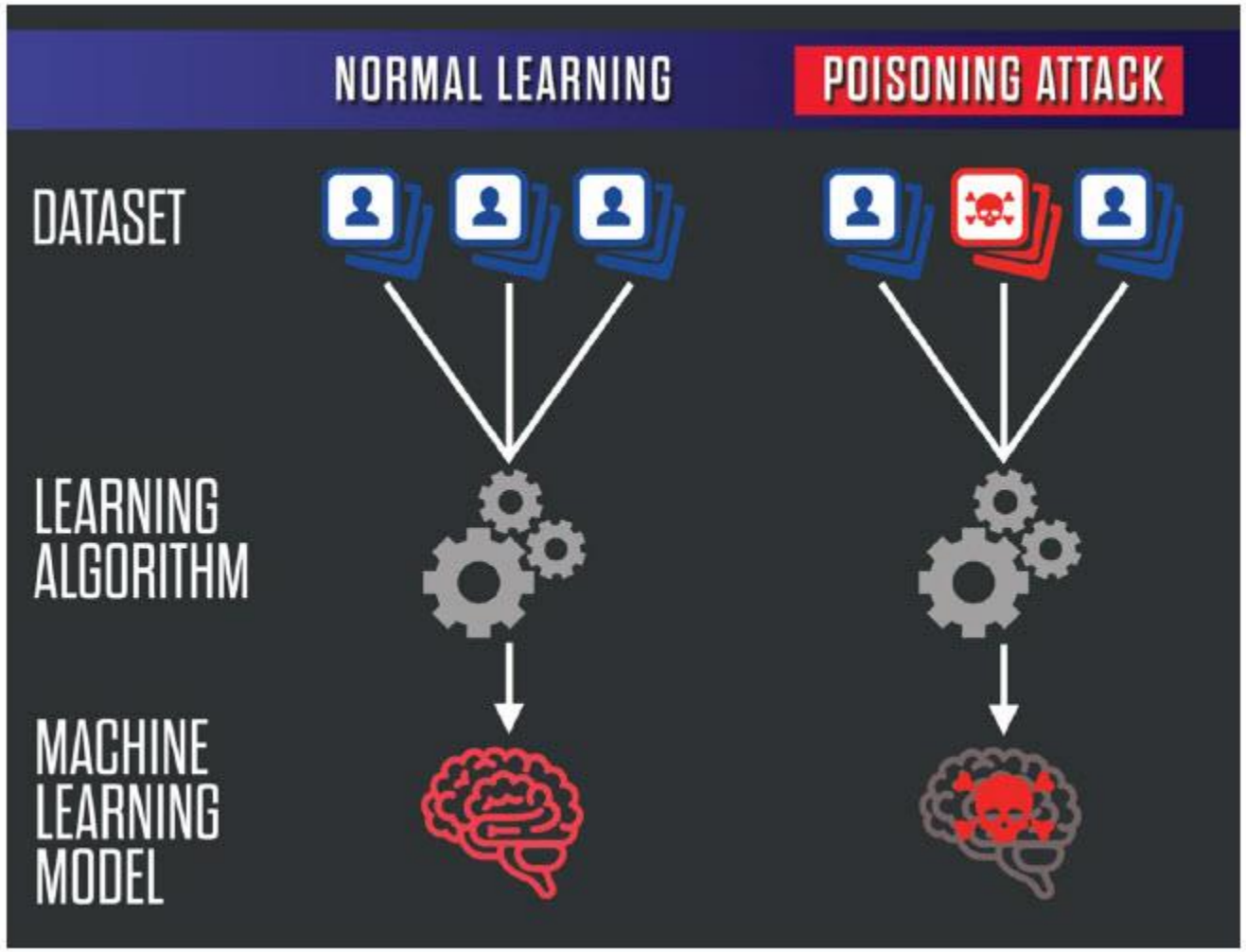
National Transportation Safety Board Connected-Car Mandate

Sources: npr.org; thehackernews.com; spectrum.ieee.org; cnn.com; technologyreview.com; politico.com.


Training phase
Benign executables
Malicious executables
Training
Predictive model
Protection phase
Unknown executable
Processing by a predictive model
Malicious / Benign
Model decision
Machine Learning: principles


Privacy Breaches
Data Poisoning
Data Bias
Label Leakage
Label Misspecification
Improper or
incomplete training
Privacy Breaches
System Disruption
IT Downtime
Model Stealing
Model Error
Misinterpretation
Job Displacement
Training Data
Training
Model
Deployment
Results
Real-world Data
Adversarial Attacks
Dataset Shift
Intentional Failure
Inadvertent Failure
Controlled most by ML developer/host
Controlled most by downstream user
Controlled by both ML host and user

Model poisoning



After AI: New Threats and Security Measures

Threat Vector

Human
Error, Social Engineering, Compromise

System Penetration
Vulnerability, Exploit

Query attacks
Challenge/Response

Malicious Inputs or Pertubations
Digital, Physical (behavior)

New Attack Types

Model Theft
Counterfeit functionality of target ML Model

Model Inference
For Subsequent Manipulation

Model Outcome Manipulation
e.g. via inversion, malicious training, altered business rules

Data Poisoning

Security Measures

Human focus
Security Awareness, Responsible AI; Anti-Phishing; Good UX for data entry

Enterprise Security
Network, Endpoint Security, User & Entity Behavior Analytics, Authenticate

AI Model Integrity
Trustworthy AI, Validation Checks

AI Data Integrity
Data Poisoning Detection, Protection

Pre-existing

New to AI

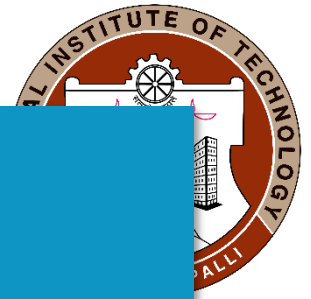
As AI Enters the Enterprise, Threats Naturally Follow

Organizational Risks of AI Implementations

Security	Liability	Social
More reliance on AI	Customer Protection	Data Rights
More opportunities for Errors	Compliance Requirements	Human Rights
More incentives for attackers	Financial Loss	Ethics
More serious consequences	Reputation Loss	Transparency, Accountability

Examples of Failures

- Bug in AI model of self driving car leads to fatal accident
- Incorrect AI credit scoring hinders consumers from securing loans
- Bank home loans in major U.S. city biased against certain race



TP Threat Prevention

UF URL Filtering

WF WildFire

AF AutoFocus

LS Logging Service

Magnifier

MM MineMeld

CLOUD-DELIVERED SECURITY SERVICES

NETWORK SECURITY

GP cloud service

GP

ADVANCED ENDPOINT PROTECTION

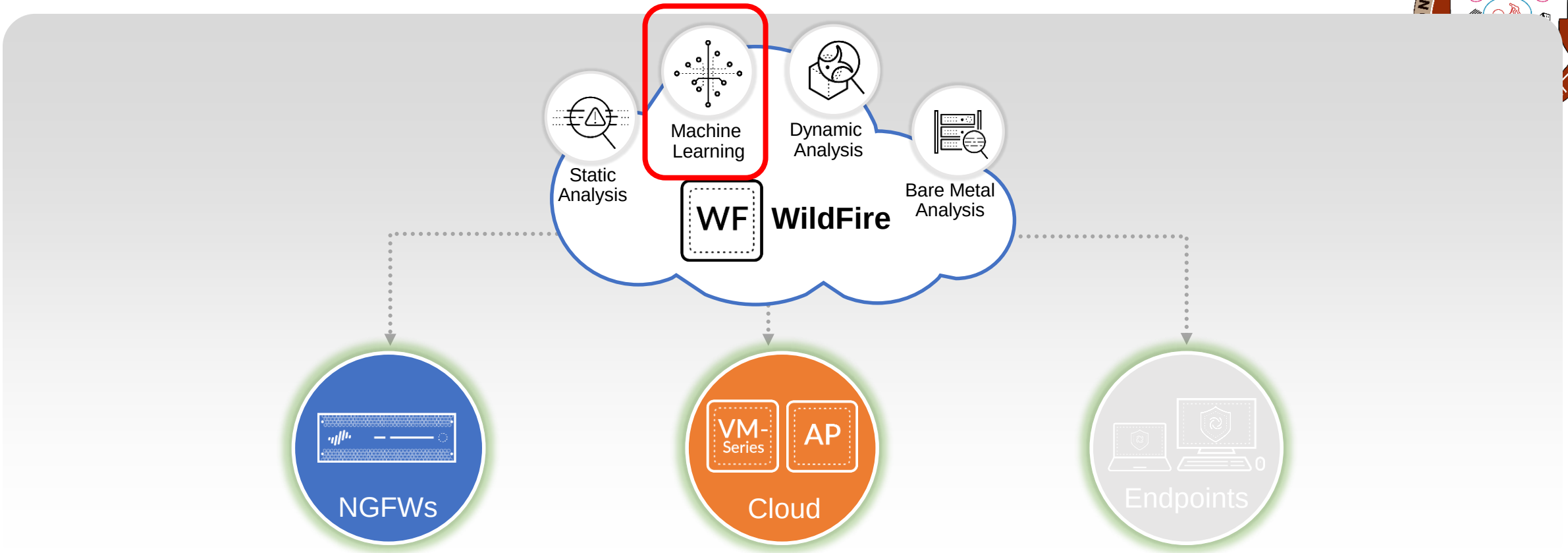
TR

CLOUD SECURITY

VM-Series

AP

WILDFIRE



1

NGFWs, Aperture, and Traps send unknowns or suspicious files and links to WildFire

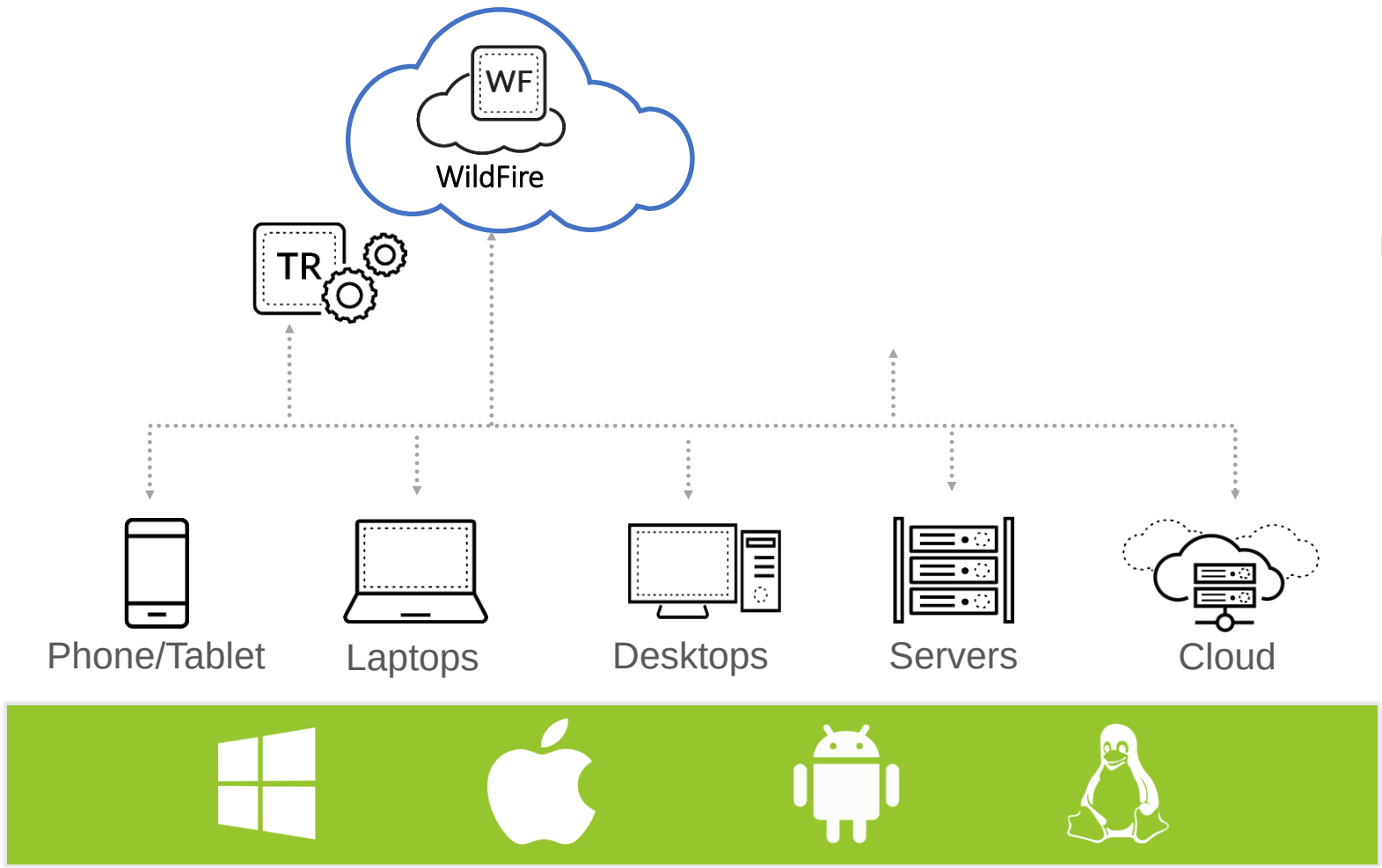
2

WildFire analyzes the unknown, renders a verdict, and shares threat intelligence

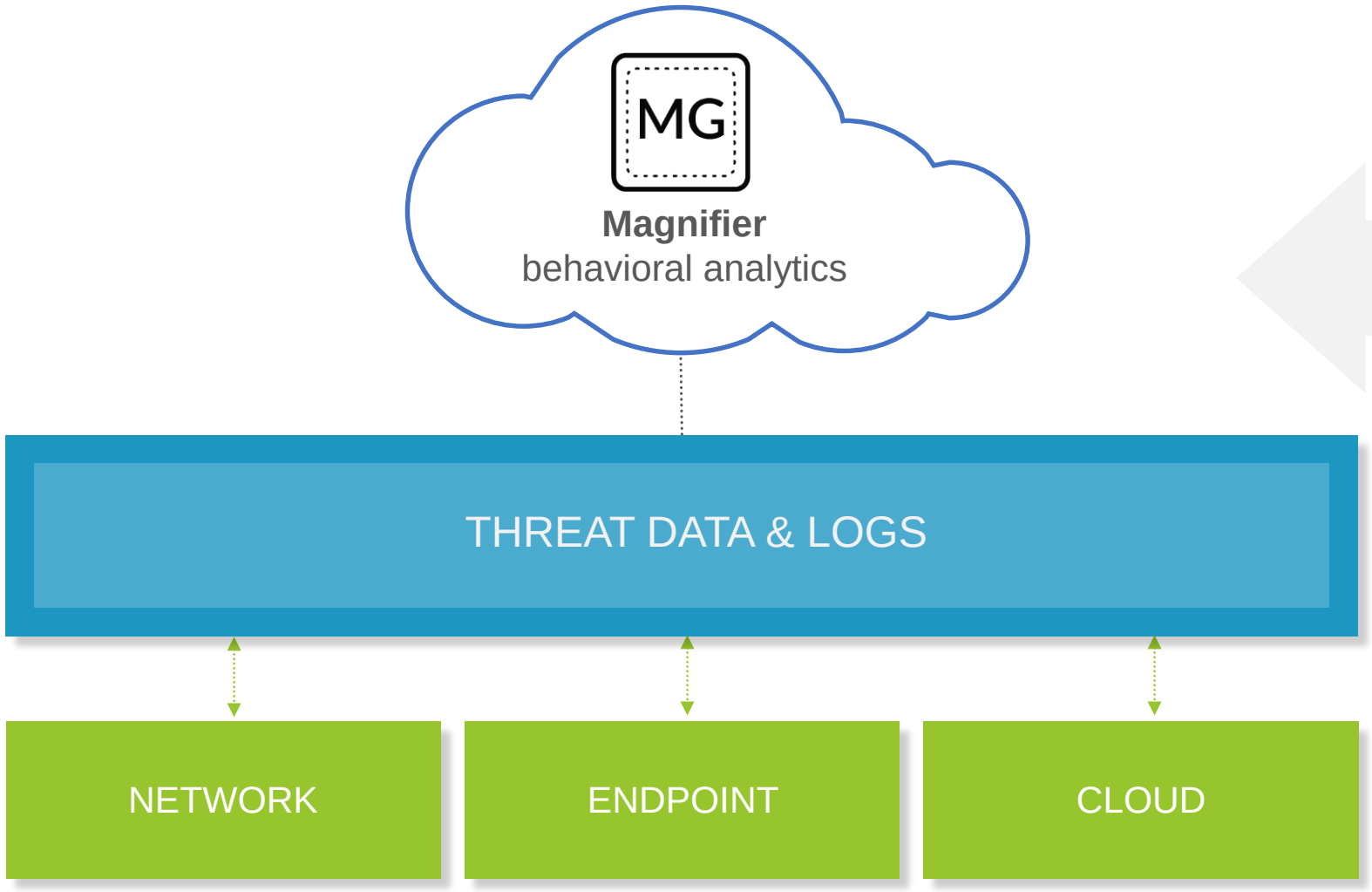
3

Automatically reprogram NGFW and endpoints to protect against new threat

TRAPS

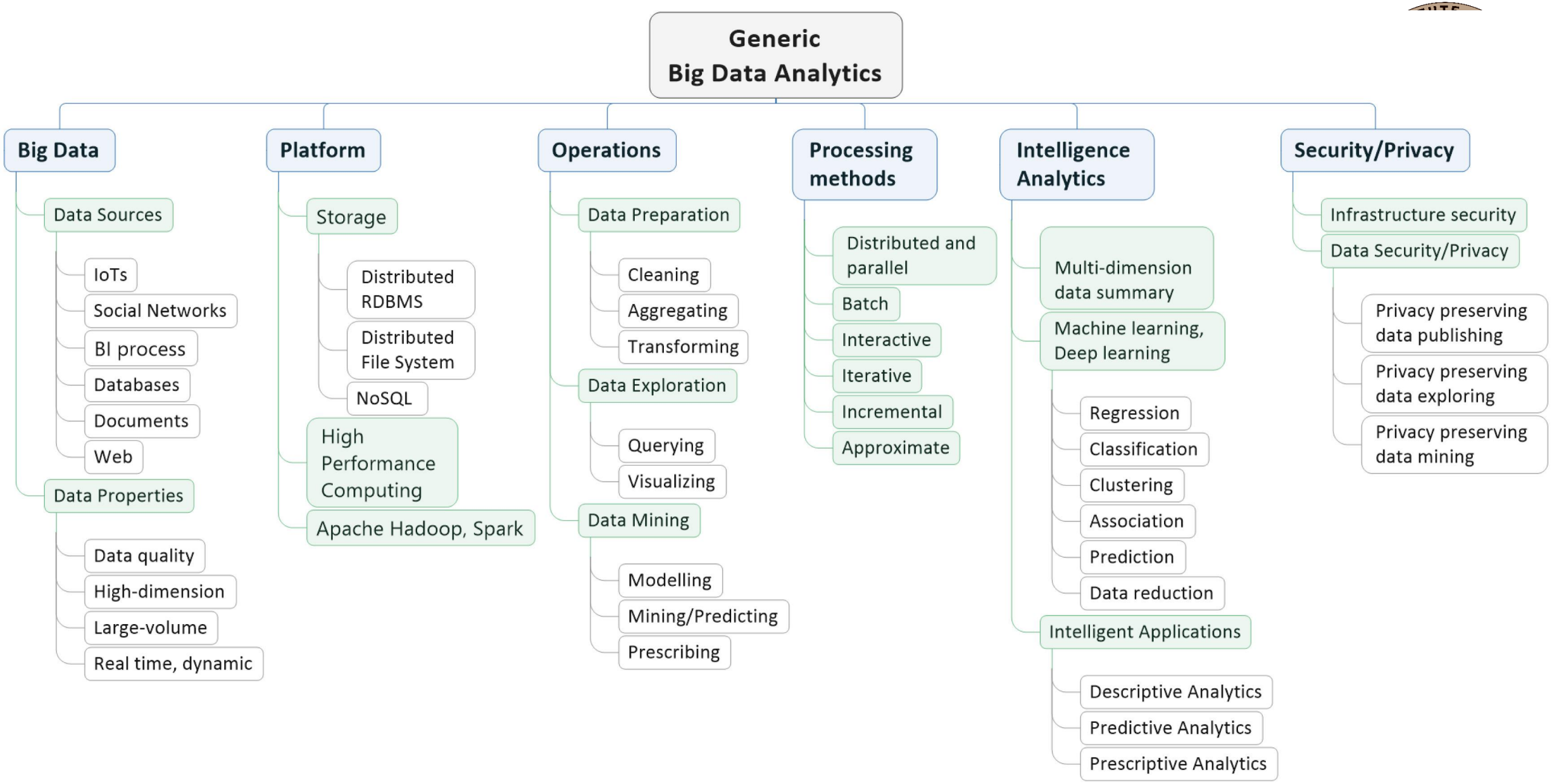


MAGNIFIER



MACHINE LEARNING

- Save analyst time
- Speed insight
- Find stealthiest threats


Generic
Big Data Analytics
Big Data
Data Sources
IoTs
Social Networks
BI process
Databases
Documents
Web
Data Properties
Data quality
High-dimension
Large-volume
Real time, dynamic
Platform
Storage
Distributed RDBMS
Distributed File System
NoSQL
High Performance Computing
Apache Hadoop, Spark
Operations
Data Preparation
Cleaning
Aggregating
Transforming
Data Exploration
Querying
Visualizing
Data Mining
Modelling
Mining/Predicting
Prescribing
Processing methods
Distributed and parallel
Batch
Interactive
Iterative
Incremental
Approximate
Intelligence Analytics
Multi-dimension data summary
Machine learning, Deep learning
Regression
Classification
Clustering
Association
Prediction
Data reduction
Intelligent Applications
Descriptive Analytics
Predictive Analytics
Prescriptive Analytics
Security/Privacy
Infrastructure security
Data Security/Privacy
Privacy preserving data publishing
Privacy preserving data exploring
Privacy preserving data mining