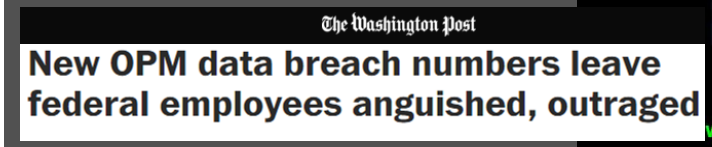
Deep Machine Learning Meets Cybersecurity

The Problem



* Malware growing exponentially
  * Over 100K malware variants created every hour
* Cyber defense is a big data problem
* Bad actors embraced automation
  * Create large amounts of malware
* Good actors have not kept pace
  * Still construct malware detection rules manually

The Solution:

Deep Machine Learning Applied to Cybersecurity

Training Data Sets:
Repository of
Billions of Malware

+ theano +

Deep Learning

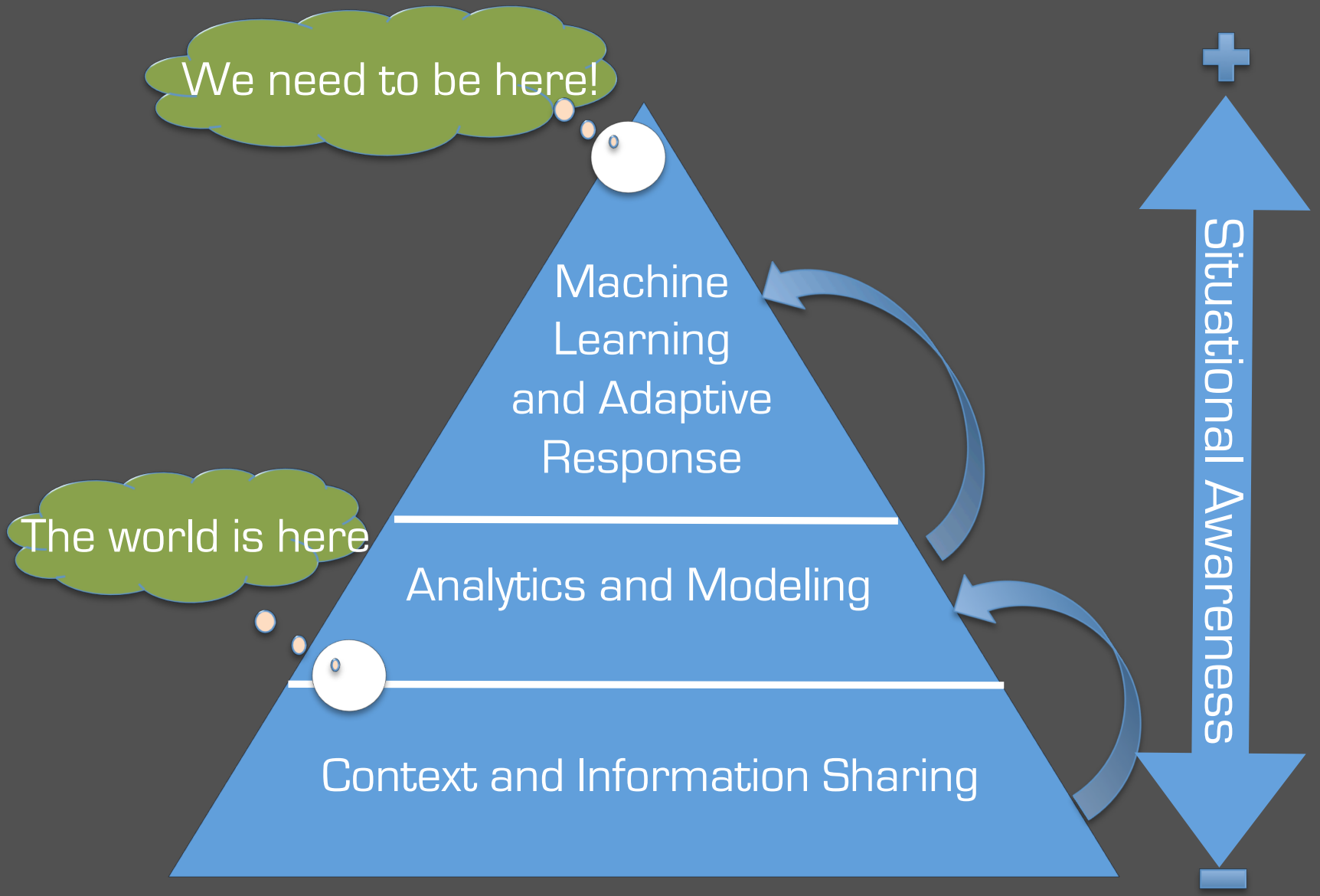
amazon web services

High-Performance
Cloud Computing

=

Cyber
Analytics

Gartner's View on Cybersecurity

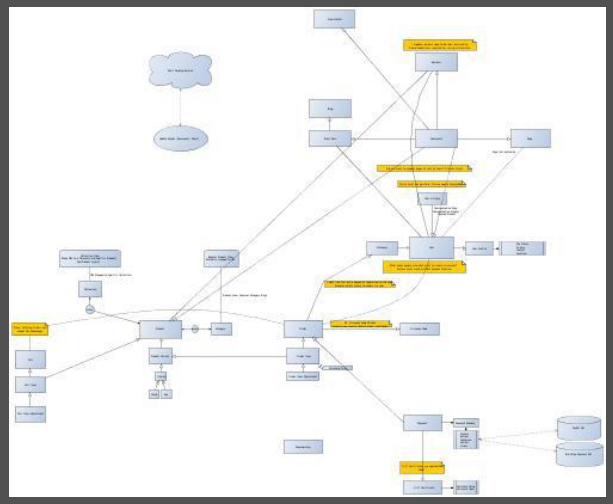


Gartner report: "Intelligent and Automated Security Controls Impact the Future of the Security Market", Oct 2015

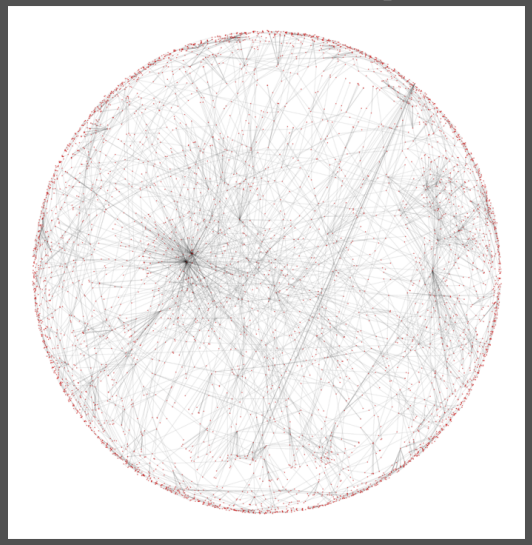
Graphical Expression of Files

Binary Input

Control Flow Graph



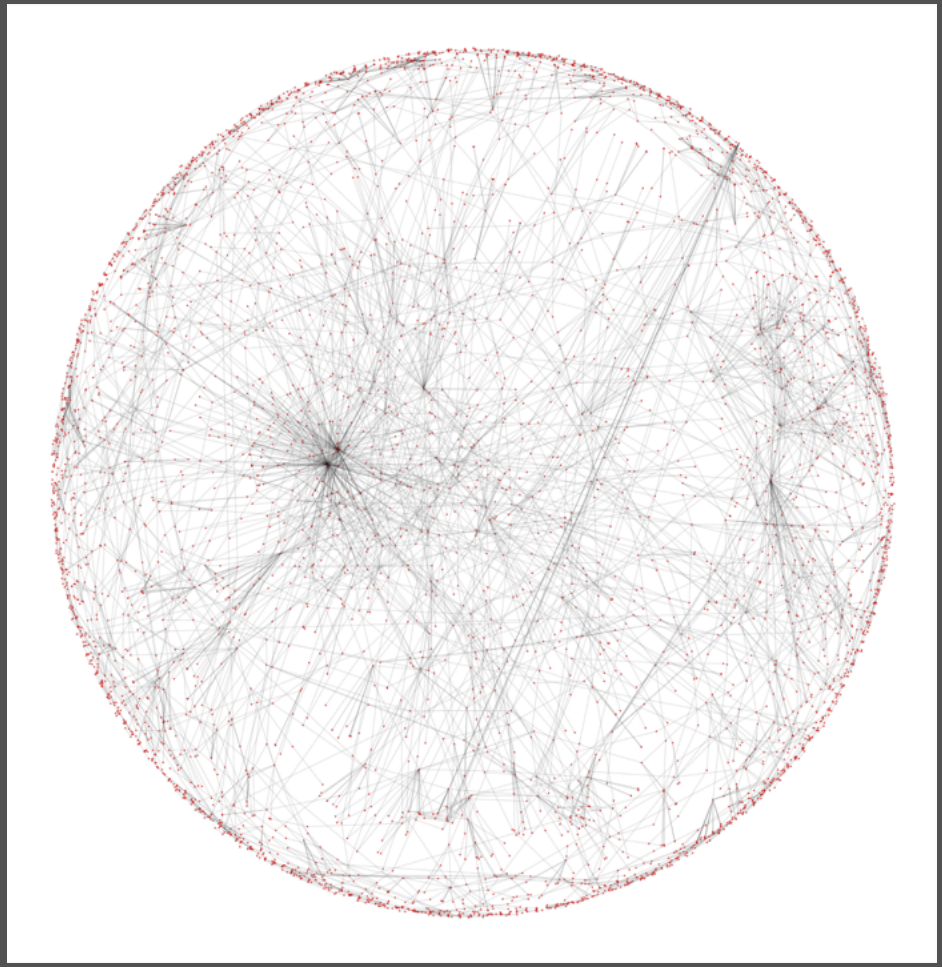
DNN Graph



Step 1:

- Malware has one thing in common with all files: it is composed of code
- Software code is best expressed as a graph
- We characterize malware as a graph then feed it into our Deep Learning engine

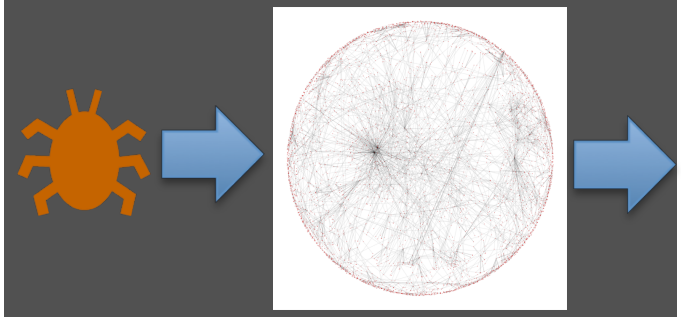
Graphical Characterization of Malware

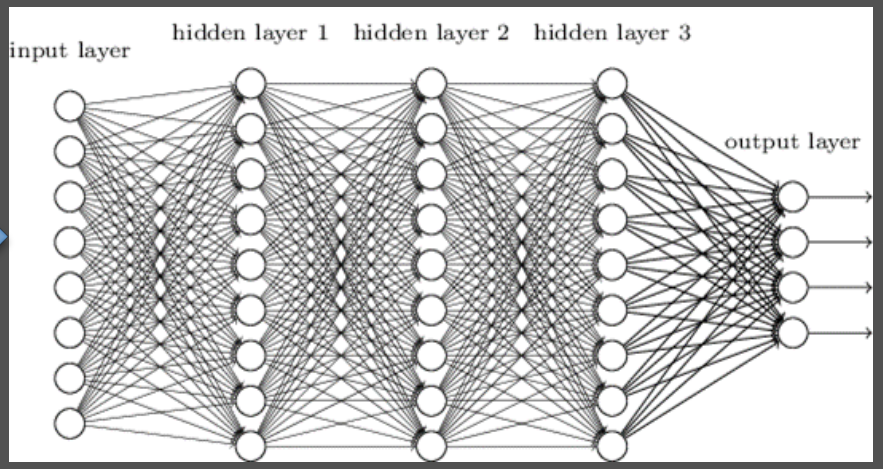


Big Data & Deep Learning Platform in the Cloud

Input

Output





Malware?
What Family?
Capabilities?

Graph-Based Malware Features

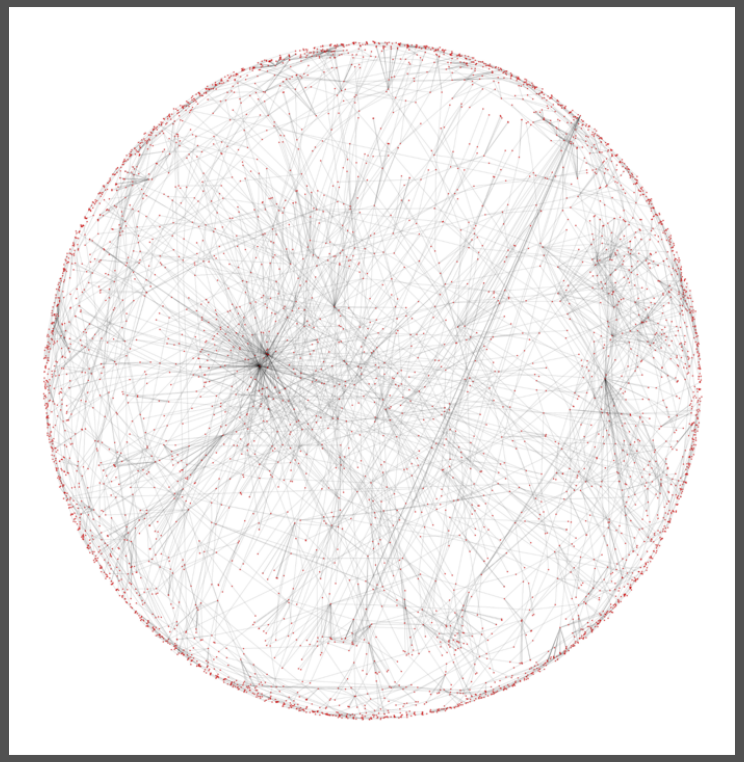
Cloud-Based Deep Learning Neural Network

Step 2:

- Our Deep Learning engine predicts malware with precision and real-time speed

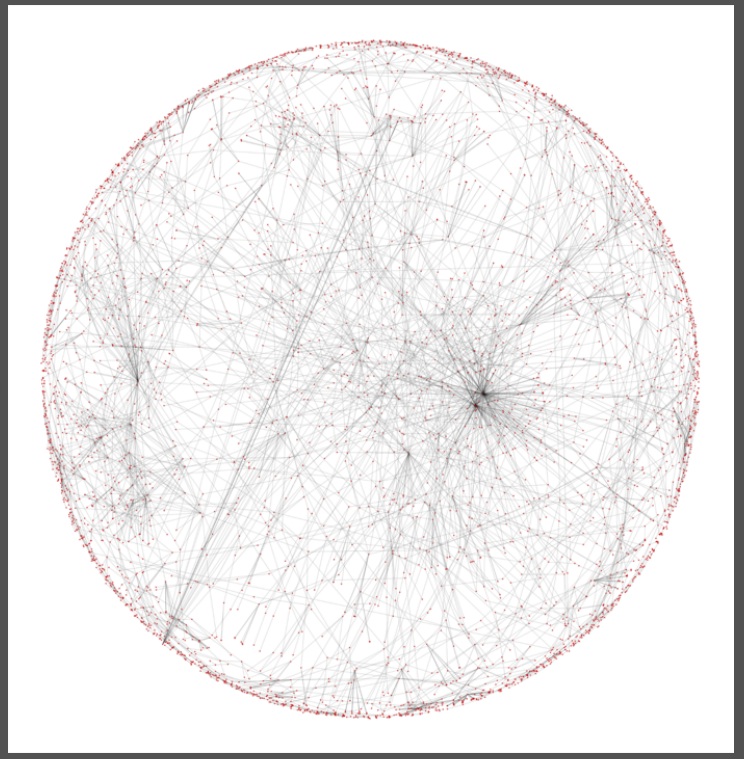
Malware Prediction Using ML & Graphs

Unknown file



Neural Net

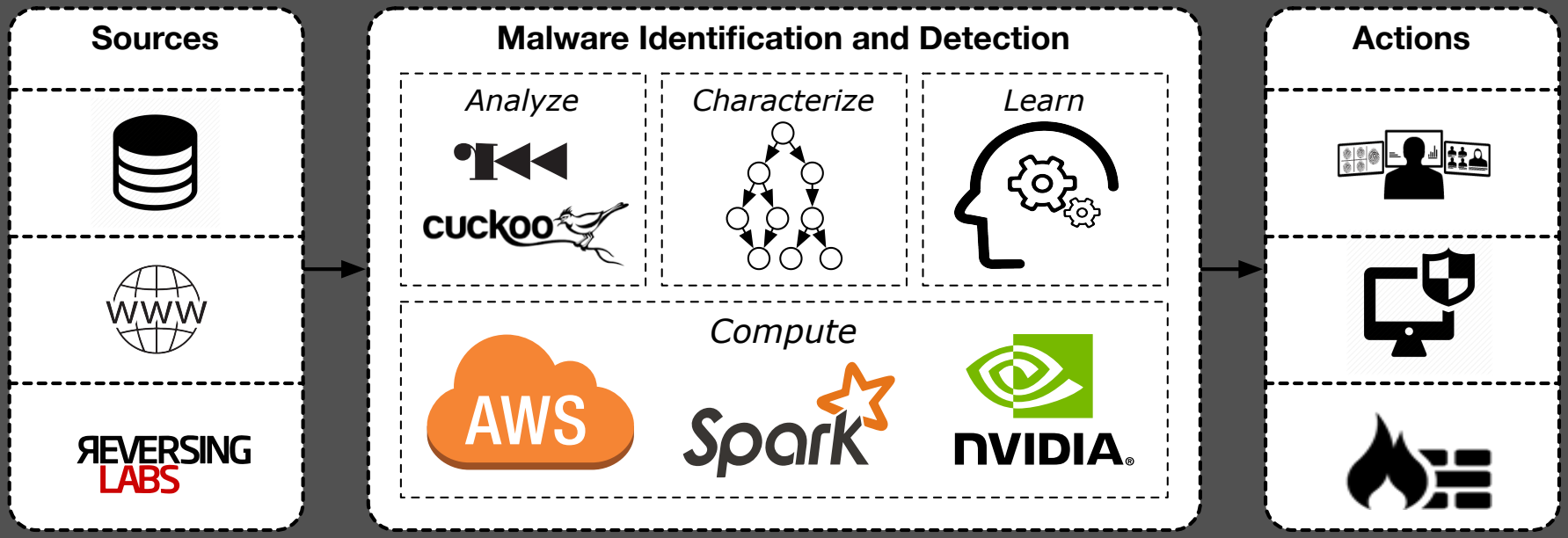
Predicted as malware



Neural network is trained to recognize malware

Machine Learning-Based Automated Malware Analysis

The Most Accurate and Fastest Platform

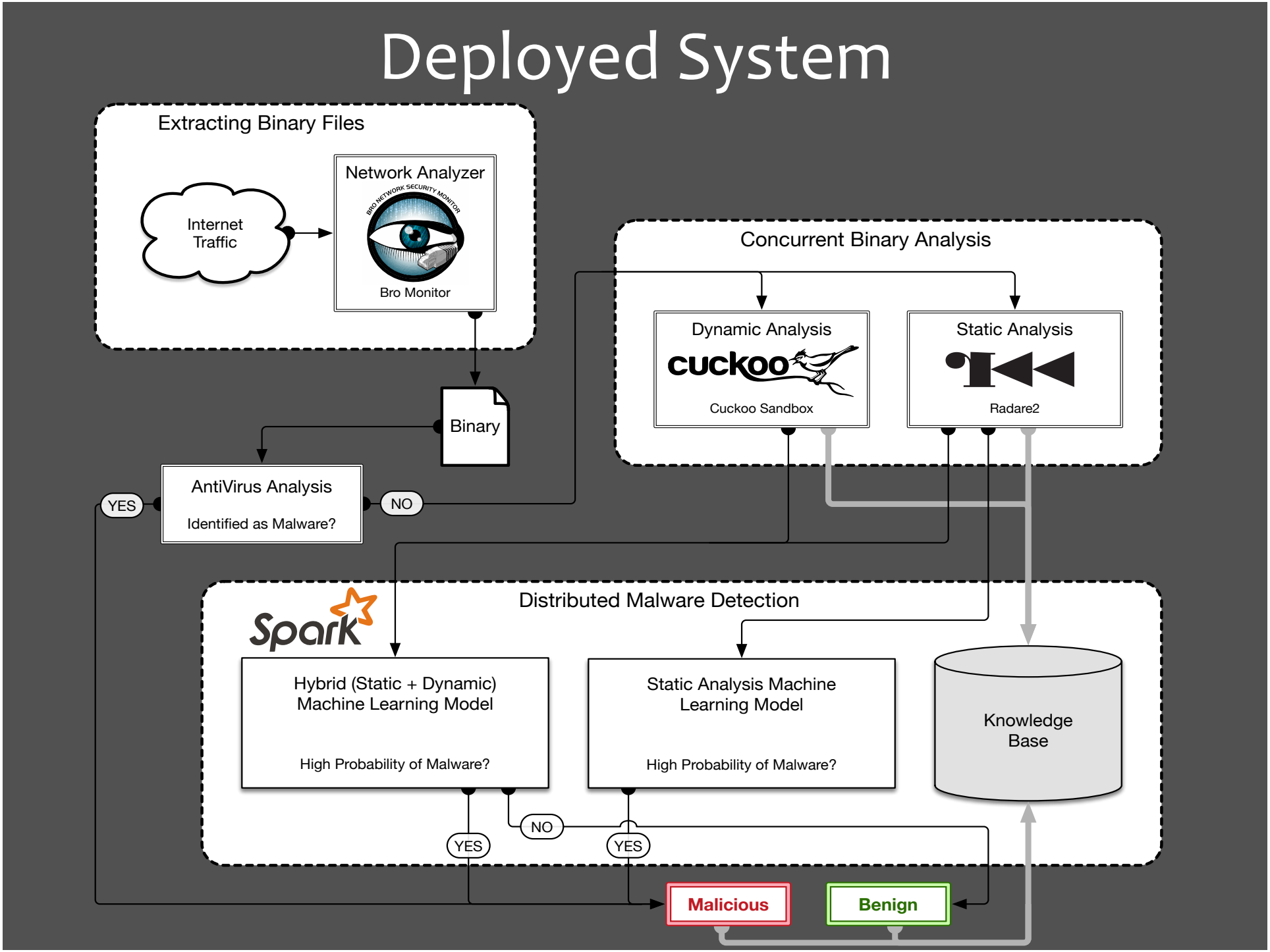


Accurately detects malware at 99.5%

Why Now?

- ***Deep Learning most accurate in AI industry***
- ***HPC platforms readily available (e.g., AWS)***
- ***Can provide comprehensive visibility***

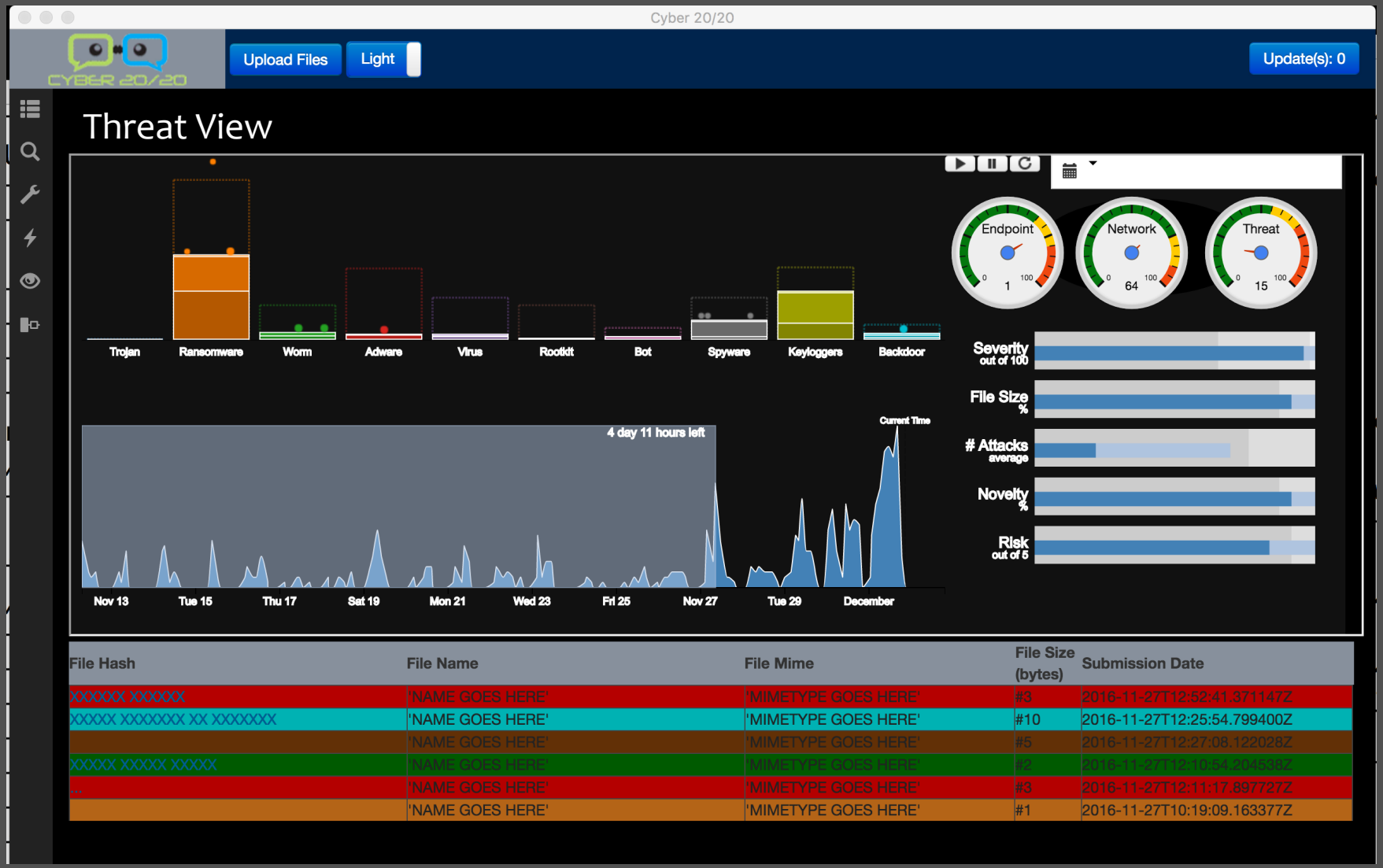
Deployed System



User Interface and Visual Analytics

CISO / Security Leaders View

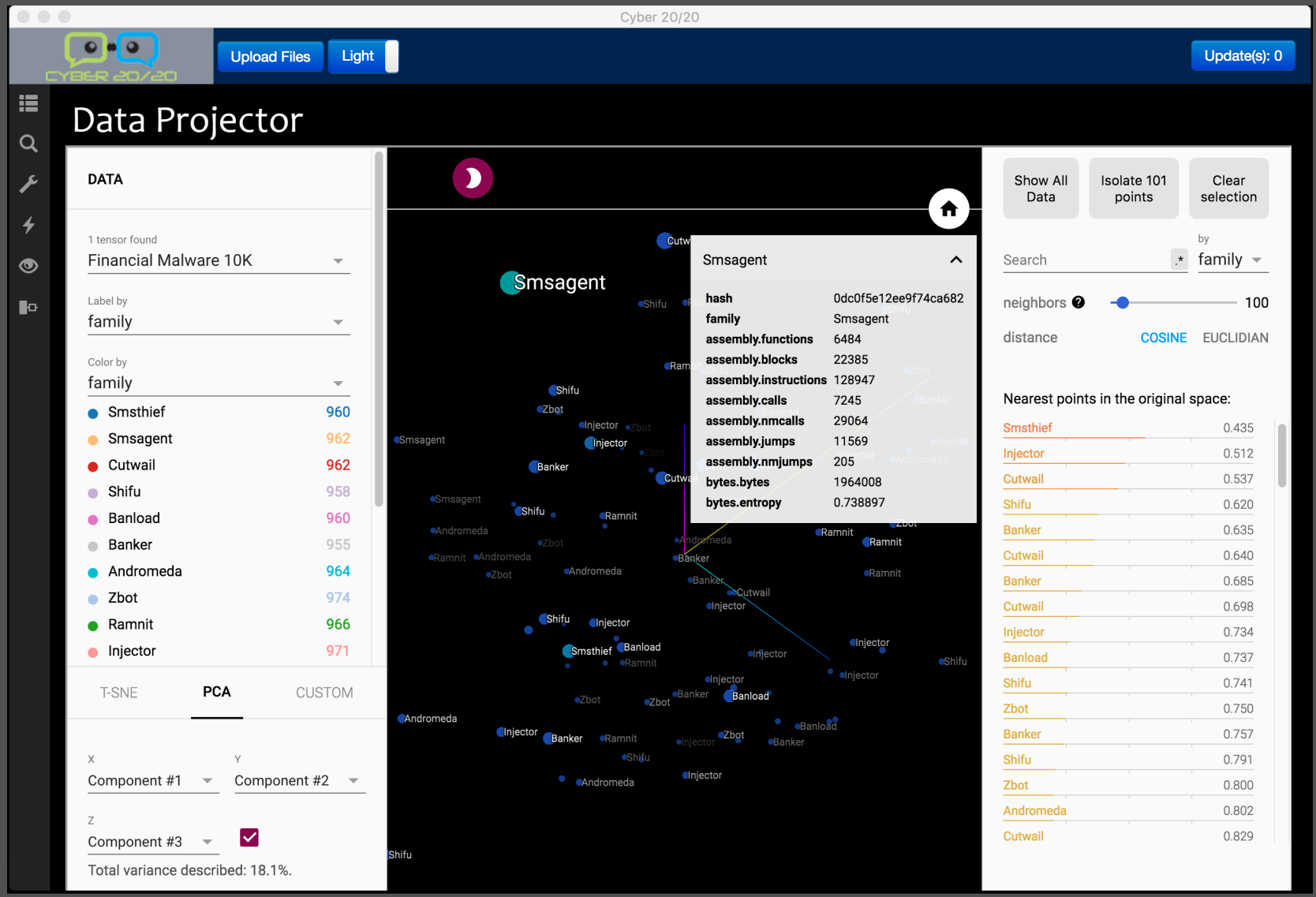
- Threat Landscape Specific to Your Enterprise



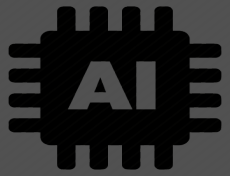
User Interface and Visual Analytics

Analysts / Incident Responders View

- Comprehensive Malware Analysis



Class Projects



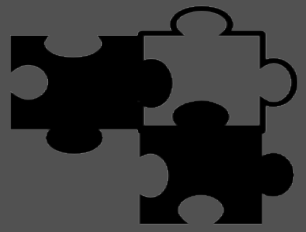
Machine Learning

Standardized Indicators of Compromise

Cyber Bot

Visual Analytics

Graphs



Analysis