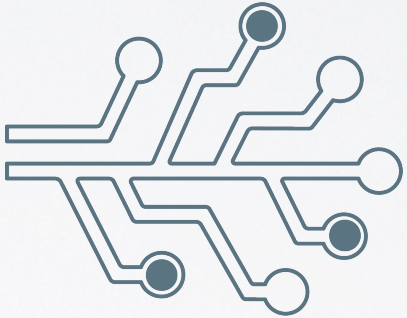
Deep Learning in Security:

Examples, Infrastructure, Challenges and Suggestion

USER & ENTITY BEHAVIOR ANALYTICS (UEBA)

UEBA SECURITY
why this matters

USE CASES
how to detect malicious insiders

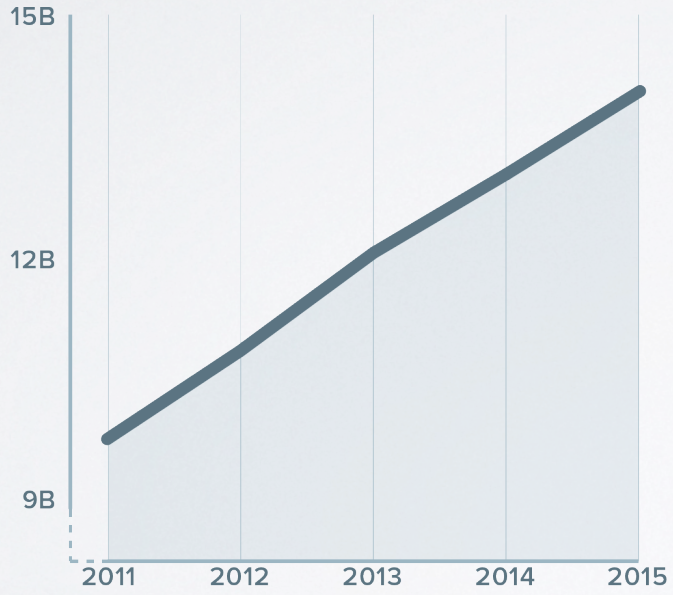


INFRASTRUCTURE
how to build big data infrastructure

CHALLENGES
how to build an enterprise solution

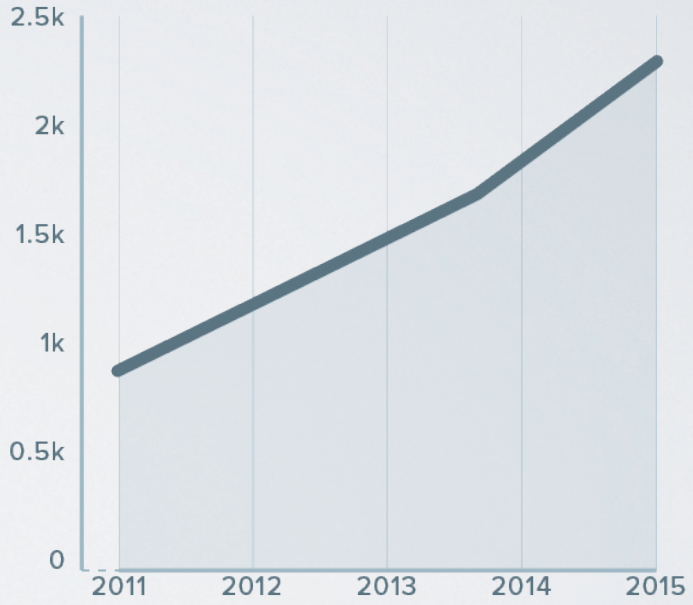
PROBLEM THE SECURITY GAP

SECURITY SPEND



PREVENTION & DETECTION (US $B)

DATA BREACHES

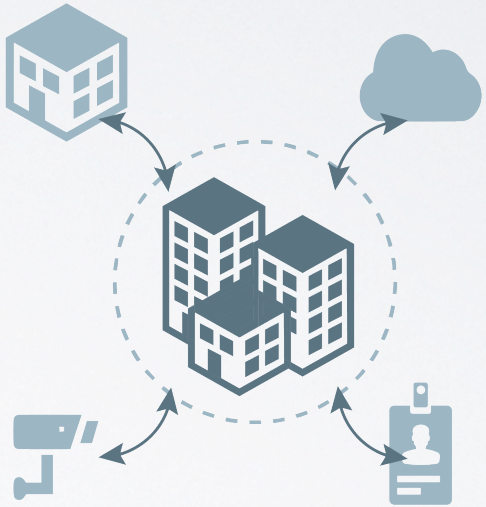


BREACHES

PROBLEM CAUSE OF THE GAP

ATTACKERS

ARE QUICKLY INNOVATING & ADAPTING



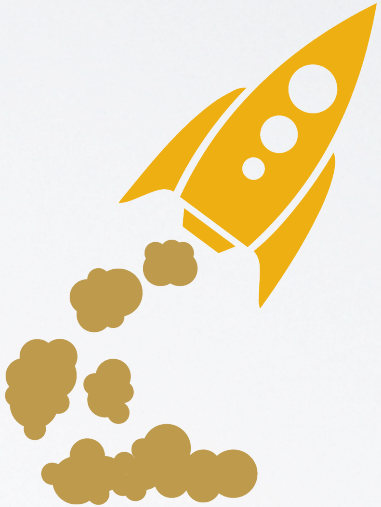
BATTLEFIELD

WITH IOT AND CLOUD, SECURITY IS BORDERLESS

PROBLEM ADDRESSING THE CAUSE

ATTACKERS

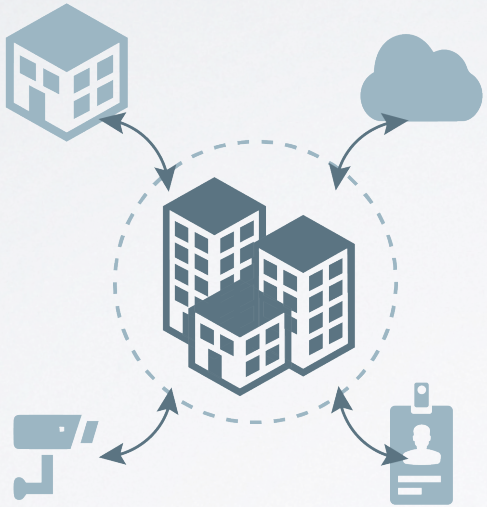
ARE QUICKLY INNOVATING & ADAPTING



DEEP LEARNING

SOLUTIONS MUST BE RESPONSIVE TO CHANGES

PROBLEM ADDRESSING THE CAUSE



BATTLEFIELD

WITH IOT AND CLOUD, SECURITY
IS BORDERLESS

INSIDER BEHAVIOR

LOOK AT BEHAVIOR CHANGE OF
INSIDE USERS AND MACHINES

USER & ENTITY BEHAVIOR ANALYTICS (UEBA)

MACHINE LEARNING DRIVEN
BEHAVIOR ANALYTICS IS
A NEW WAY TO **COMBAT ATTACKERS**

1. **Machine driven, not only human driven**
2. **Detect compromised users, not only attackers**
3. **Post-infection detection, not only prevention**

REAL WORLD NEWS WORTHY EXAMPLES

COMPROMISED

40 million credit cards were stolen from Target's severs

STOLEN CREDENTIALS

Edward Snowden stole more than 1.7 million classified documents

INTENDED TO LEAK INFORMATION

NEGLIGENT

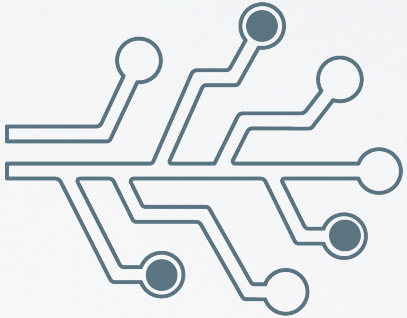
DDoS attack from 10M+ hacked home devices took down major websites

ALL USED THE SAME PASSWORD

USER & ENTITY BEHAVIOR ANALYTICS

UEBA SECURITY
why this matters

USE CASES
how to detect malicious insiders



INFRASTRUCTURE
how to build big data infrastructure

CHALLENGES
how to build an enterprise solution

REAL WORLD ATTACKS CAUGHT

SCANNING ATTACK

scan servers in the data center to find out vulnerable targets

DETECTED WITH
Active Directory (AD) LOGS

DATA DOWNLOAD

download data from internal document repository which is not typical for the host

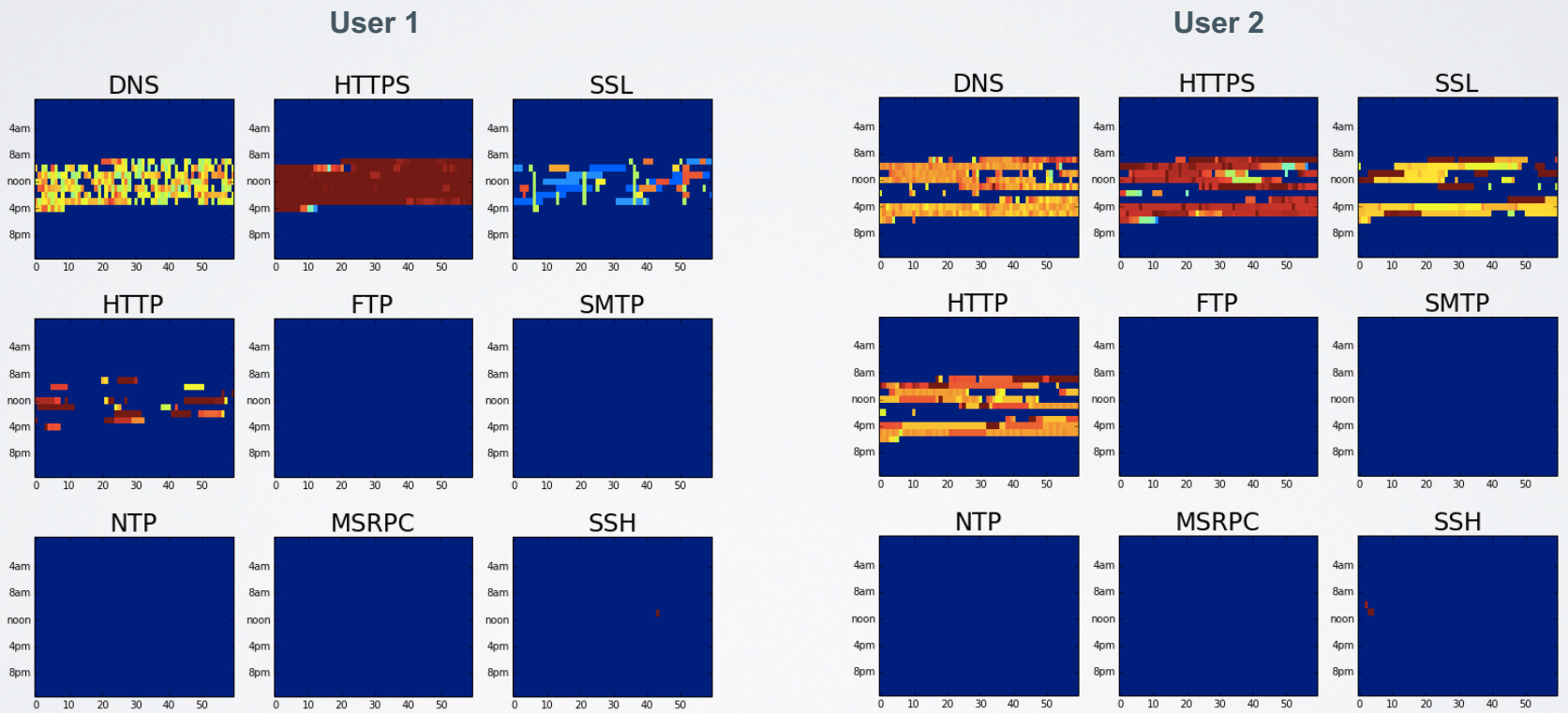
DETECTED WITH **NETWORK TRAFFIC**

EXFILTRATION OF DATA

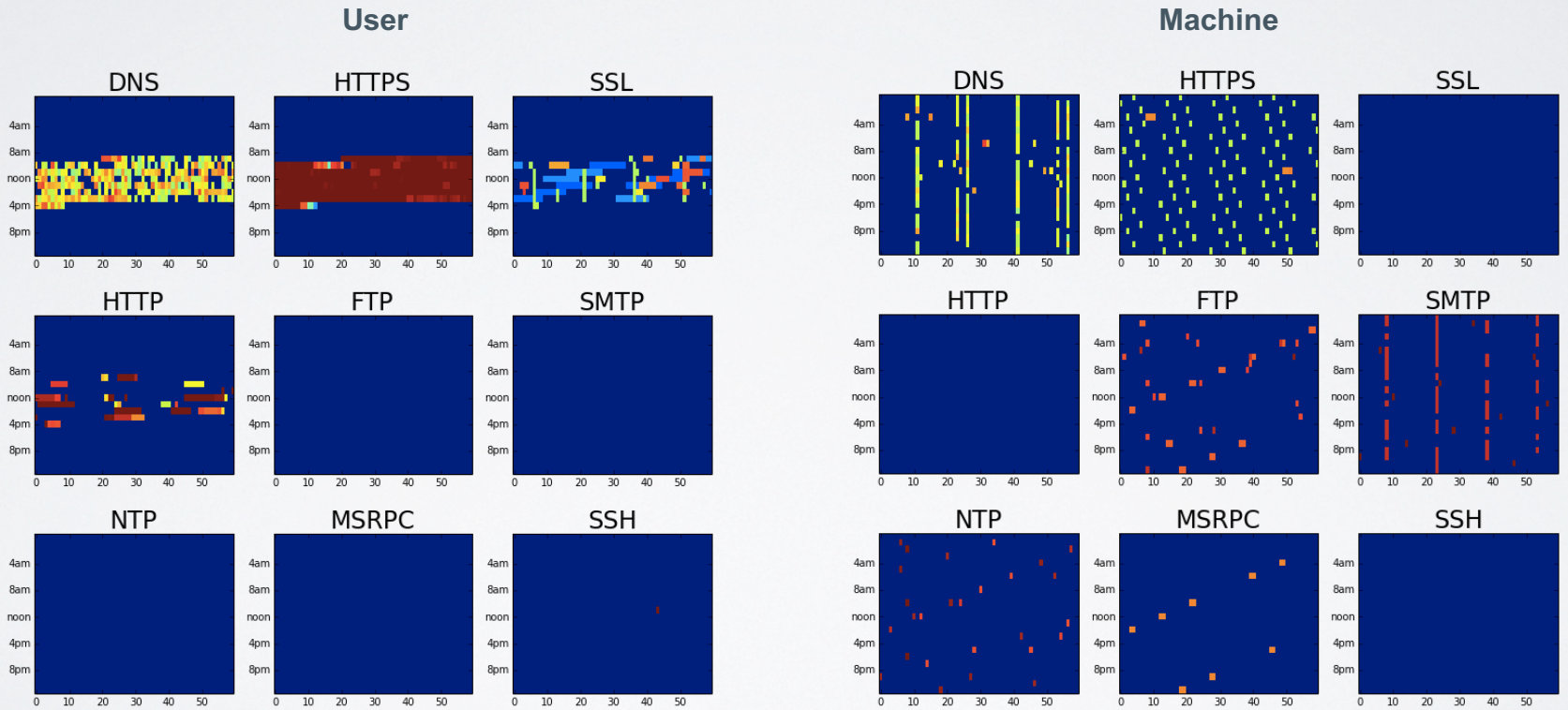
upload a large file to cloud server hosted in new country never accessed before

DETECTED WITH **WEB PROXY LOGS**

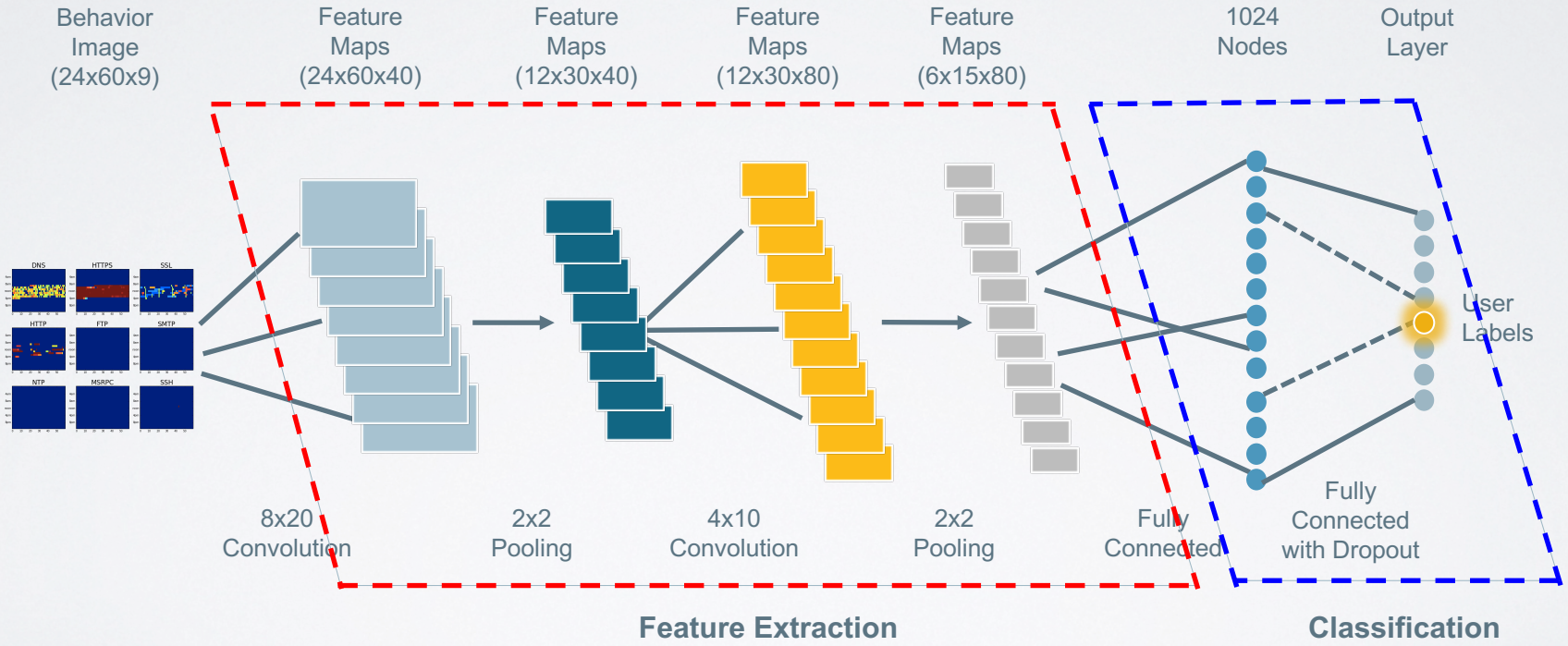
BEHAVIOR ENCODING USERS



BEHAVIOR ENCODING USER VS MACHINE

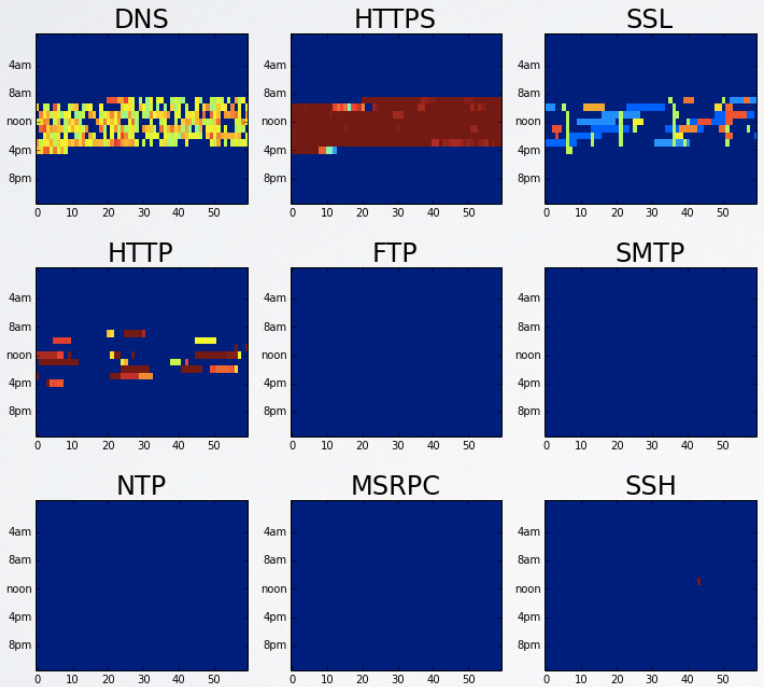


ANOMALY DETECTION CONVOLUTIONAL NEURAL NETWORK (CNN)

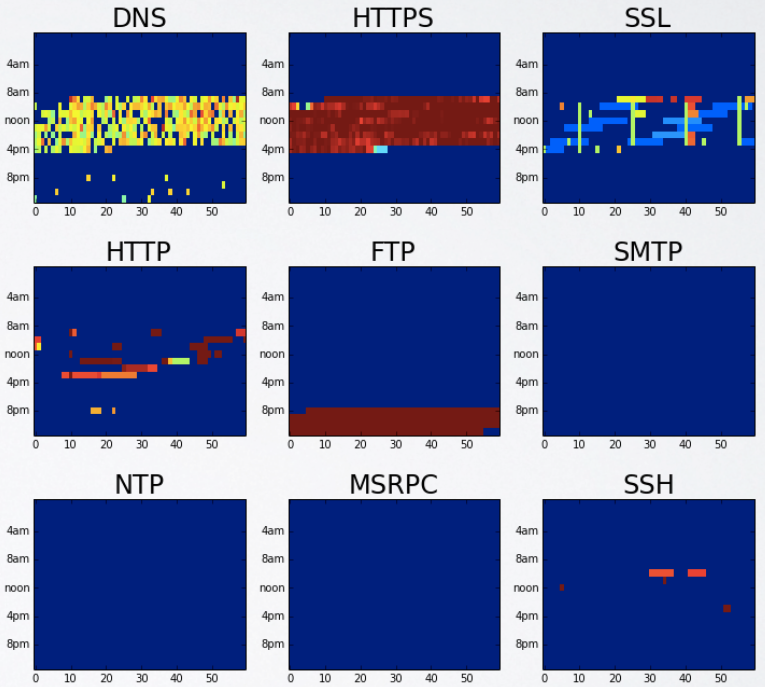


BEHAVIOR ANOMALY USER | EXFILTRATION

User – Before Compromise

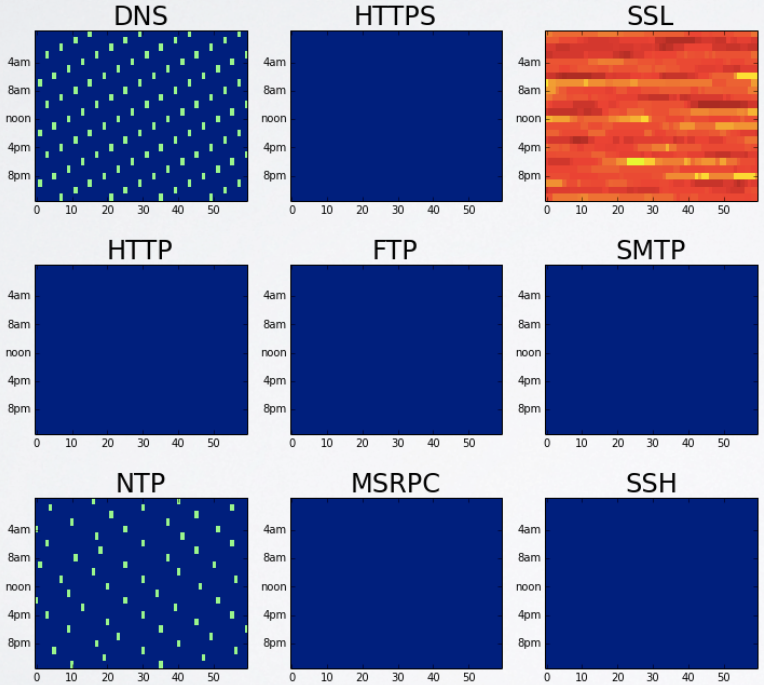


User – Post Compromise

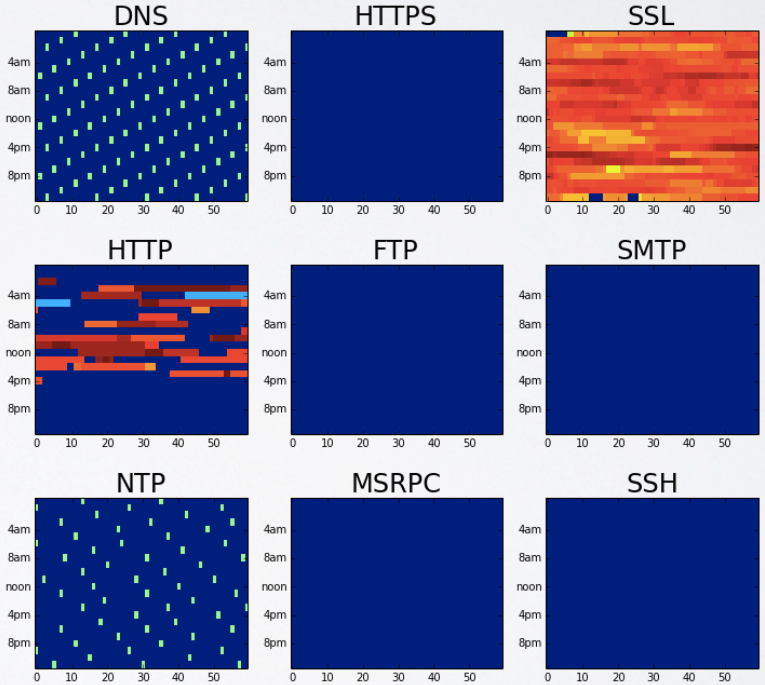


BEHAVIOR ANOMALY IOT DEVICE | DATA DOWNLOAD

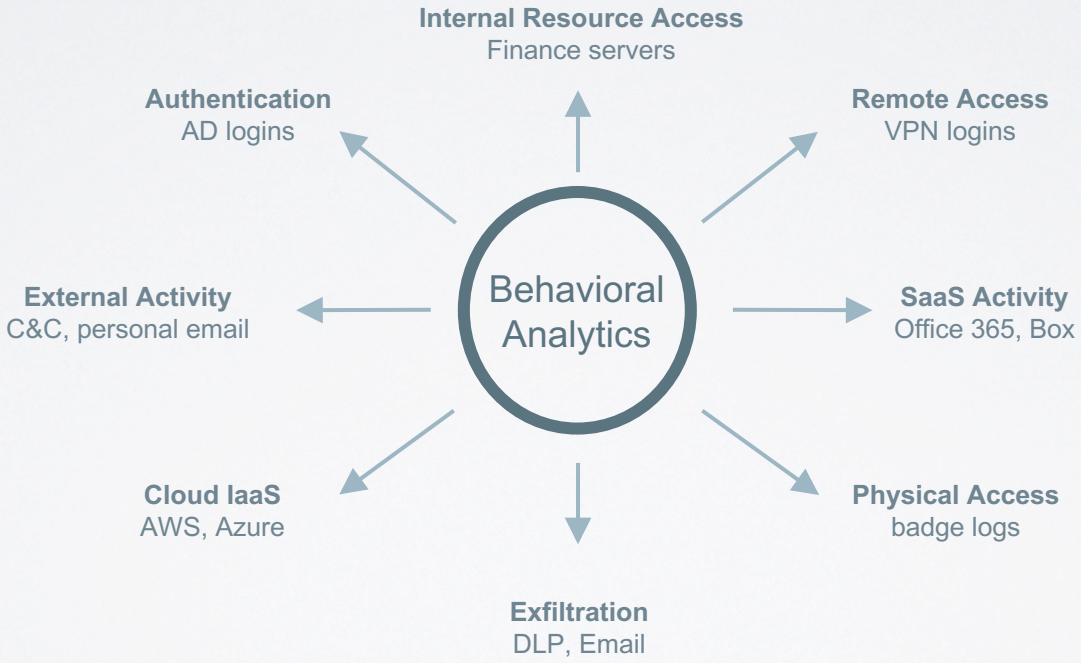
Dropcam – Before Compromise



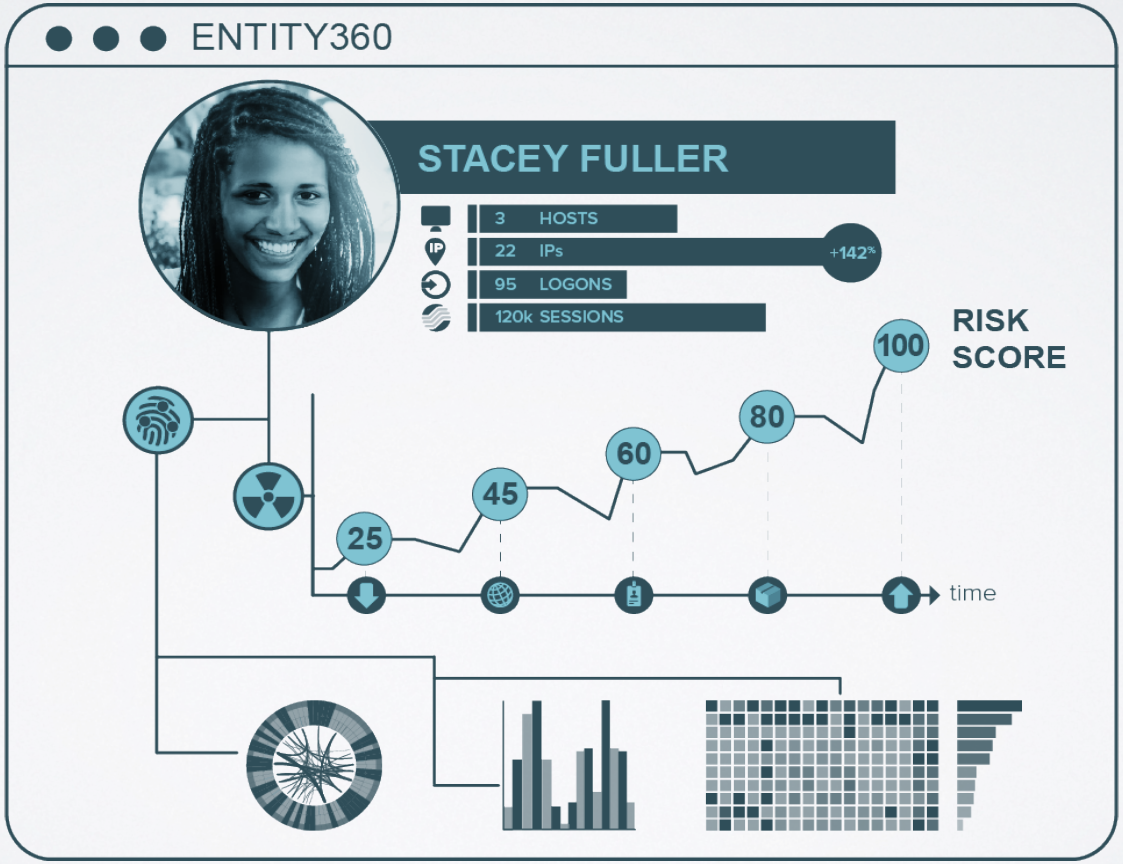
Dropcam – Post Compromise



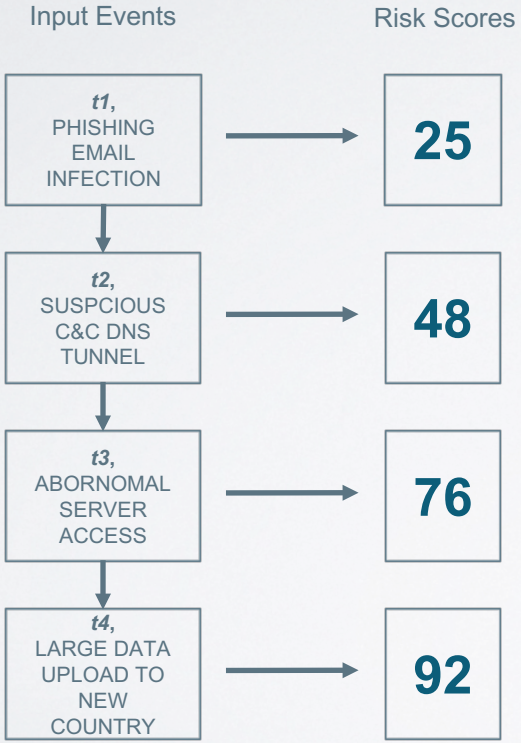
BEHAVIOR ANALYTICS MULTI-DIMENSIONAL



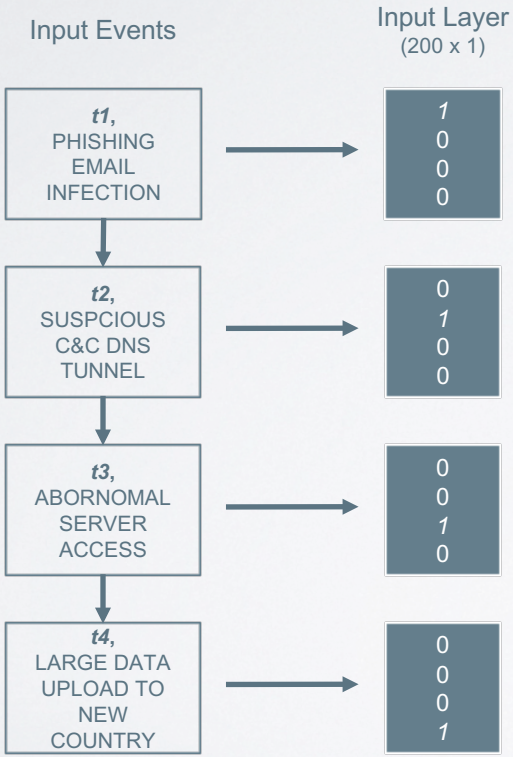
ENTITY SCORING TEMPORAL SEQUENCE TRACKING



ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)

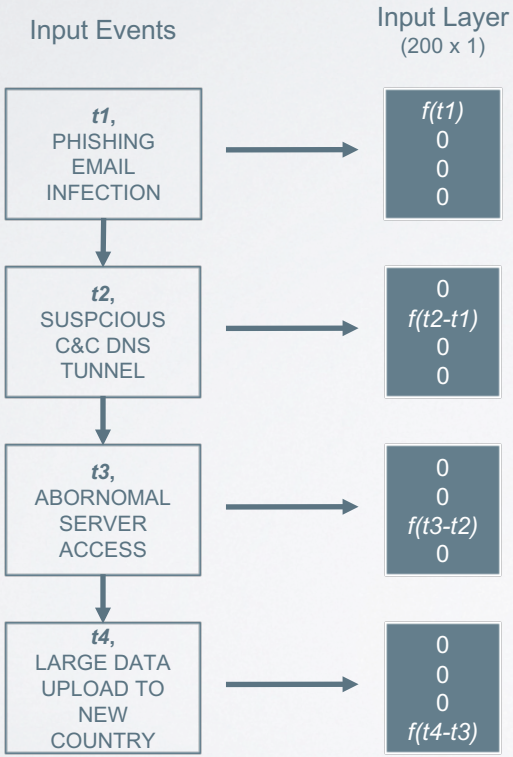


ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



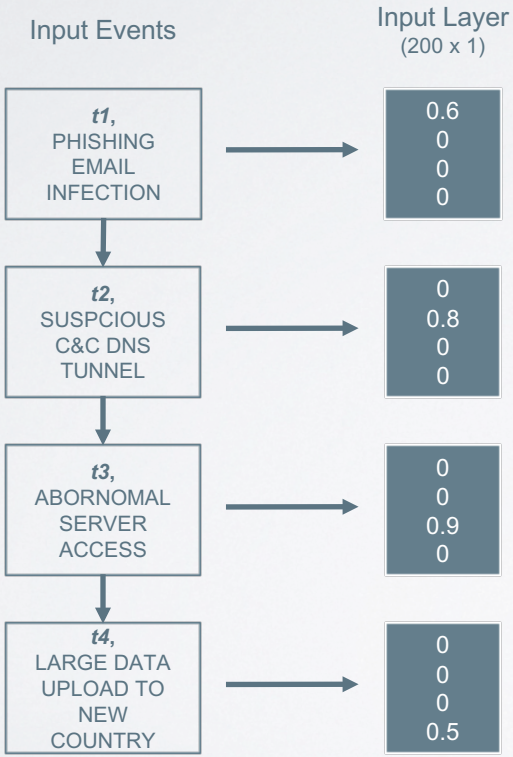
one hot encoding

ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



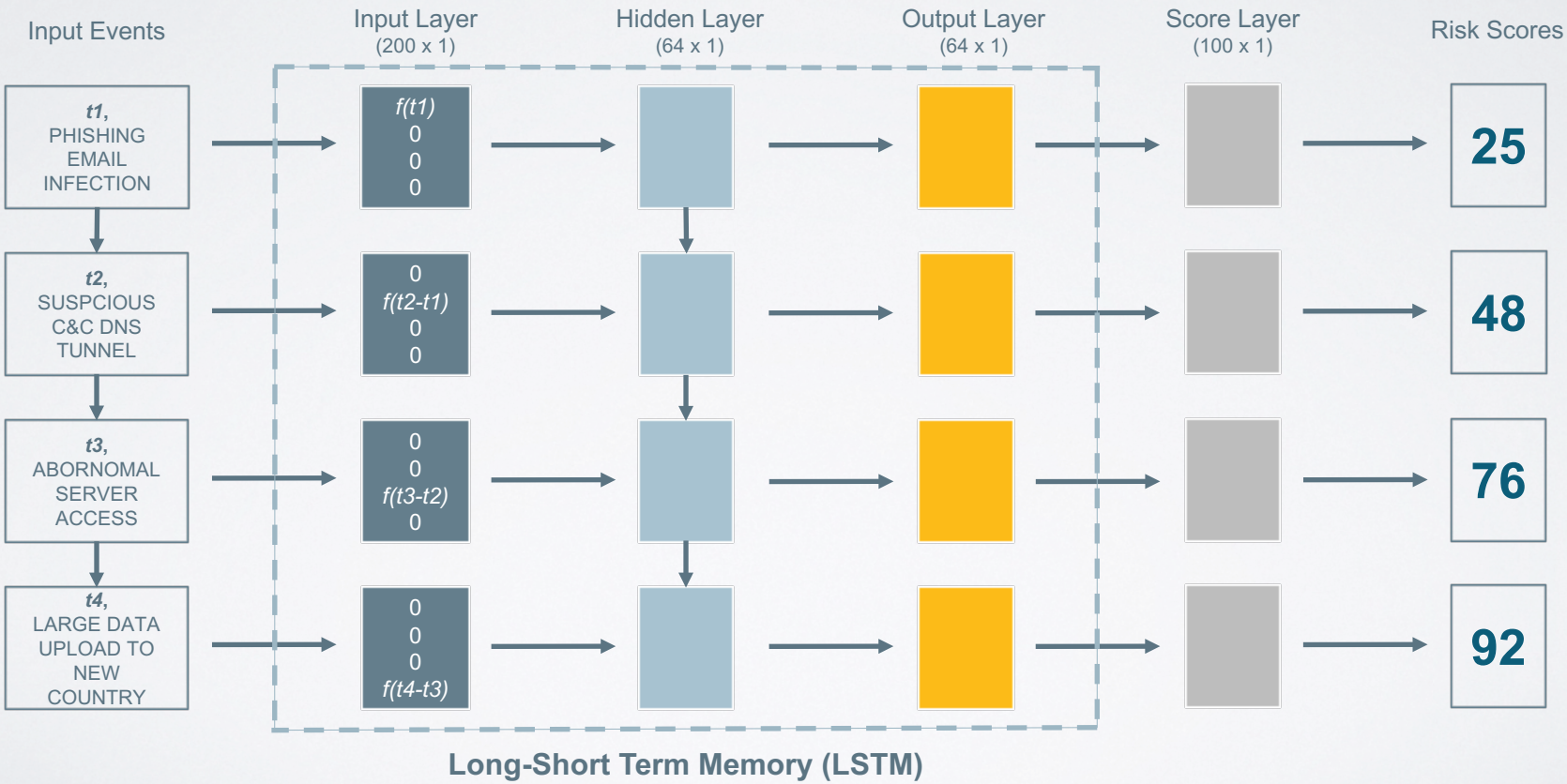
one hot
time-decayed
encoding

ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



one hot
time-decayed
encoding

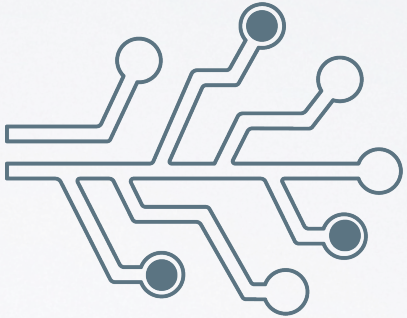
ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



USER & ENTITY BEHAVIOR ANALYTICS

UEBA SECURITY
why this matters

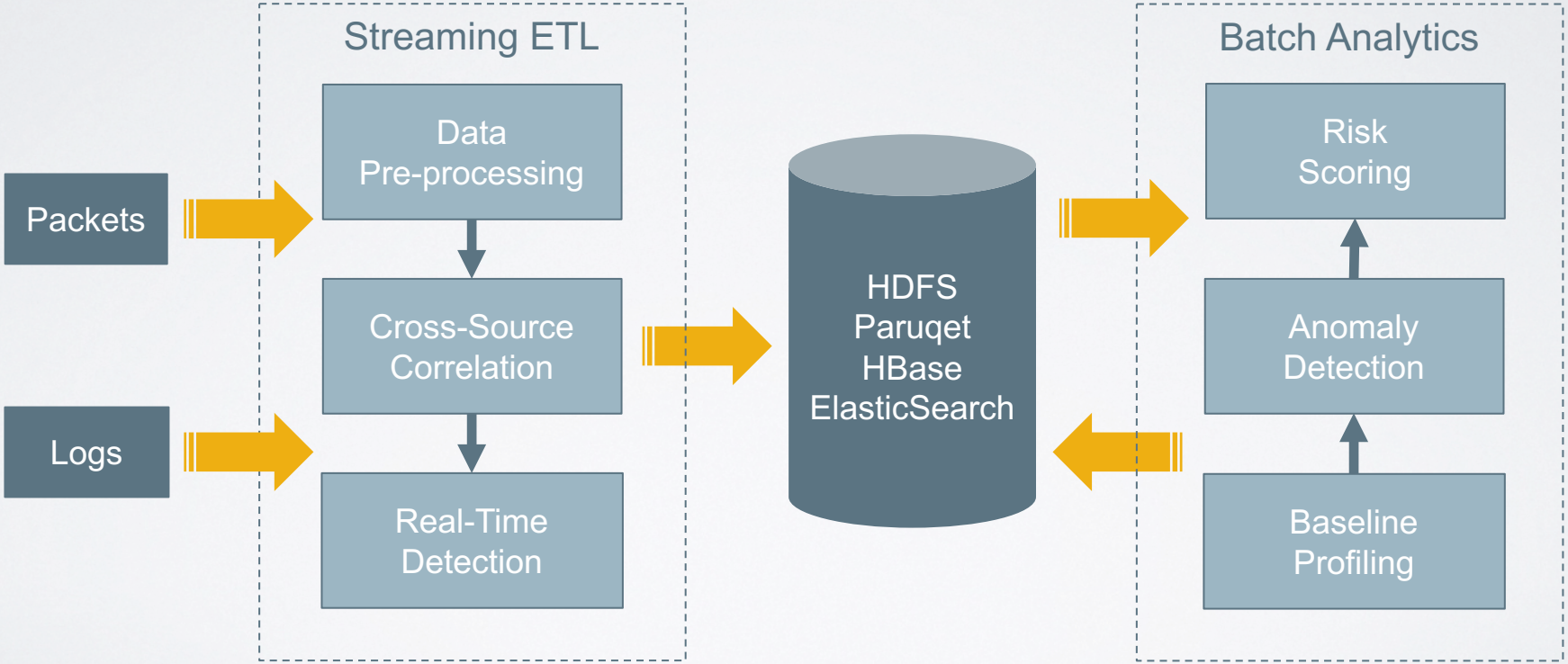
USE CASES
how to detect malicious insiders



INFRASTRUCTURE
how to build big data infrastructure

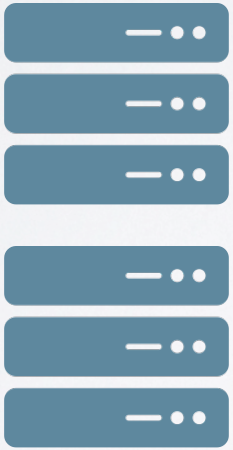
CHALLENGES
how to build an enterprise solution

DATA PIPELINE ARCHITECTURE

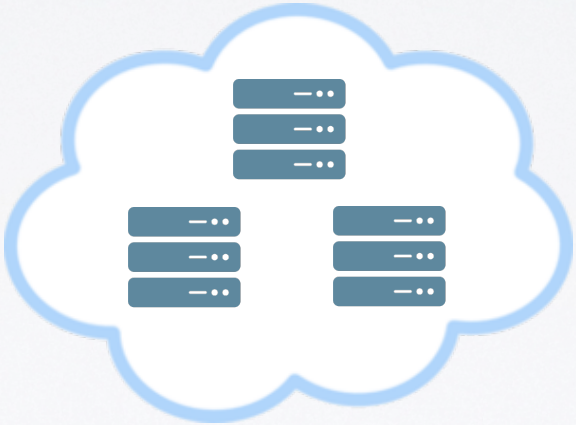


DEPLOYMENT OPTIONS ON-PREMISES & CLOUD

On Premises



Private Cloud

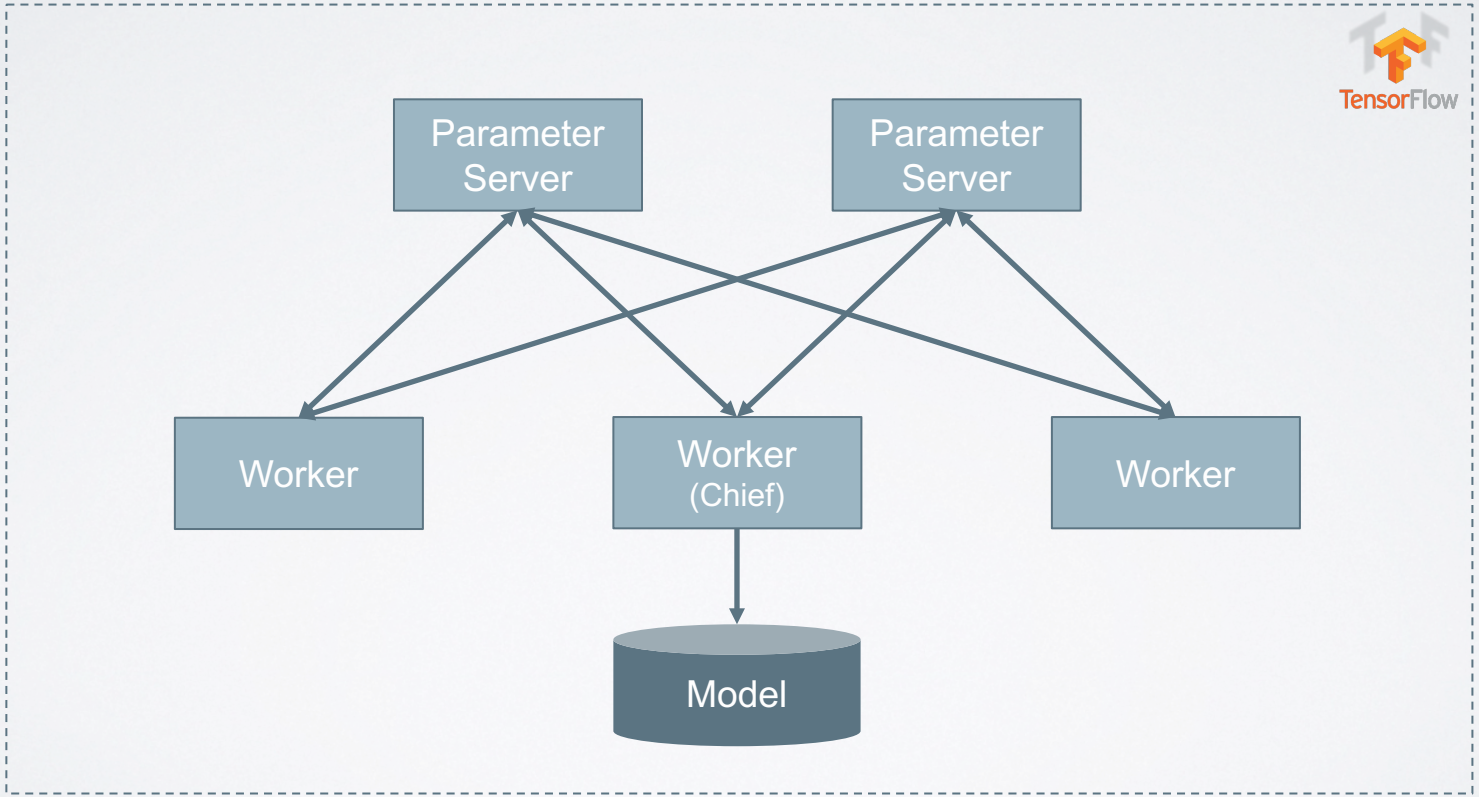


Public Cloud

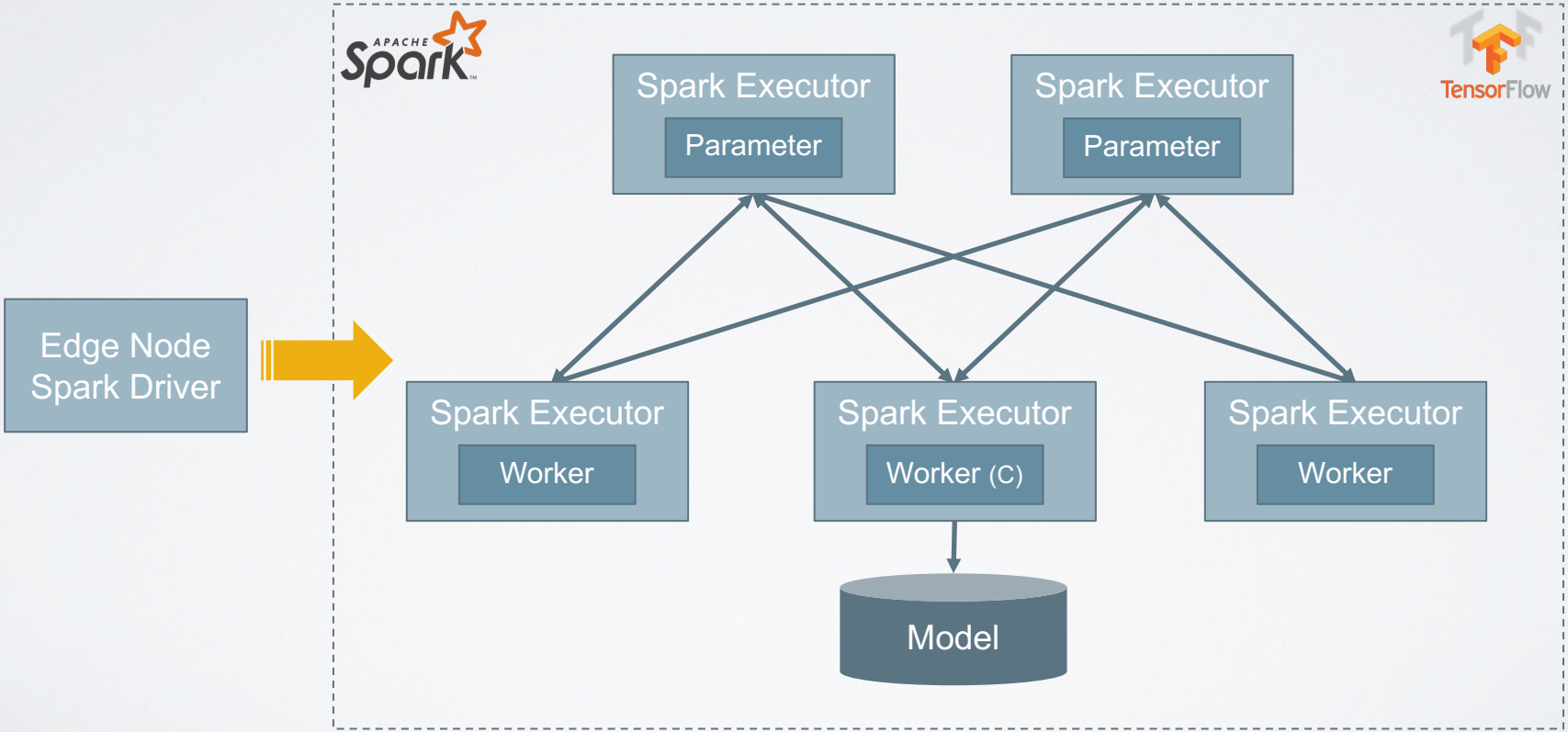
amazon web services™

Microsoft Azure

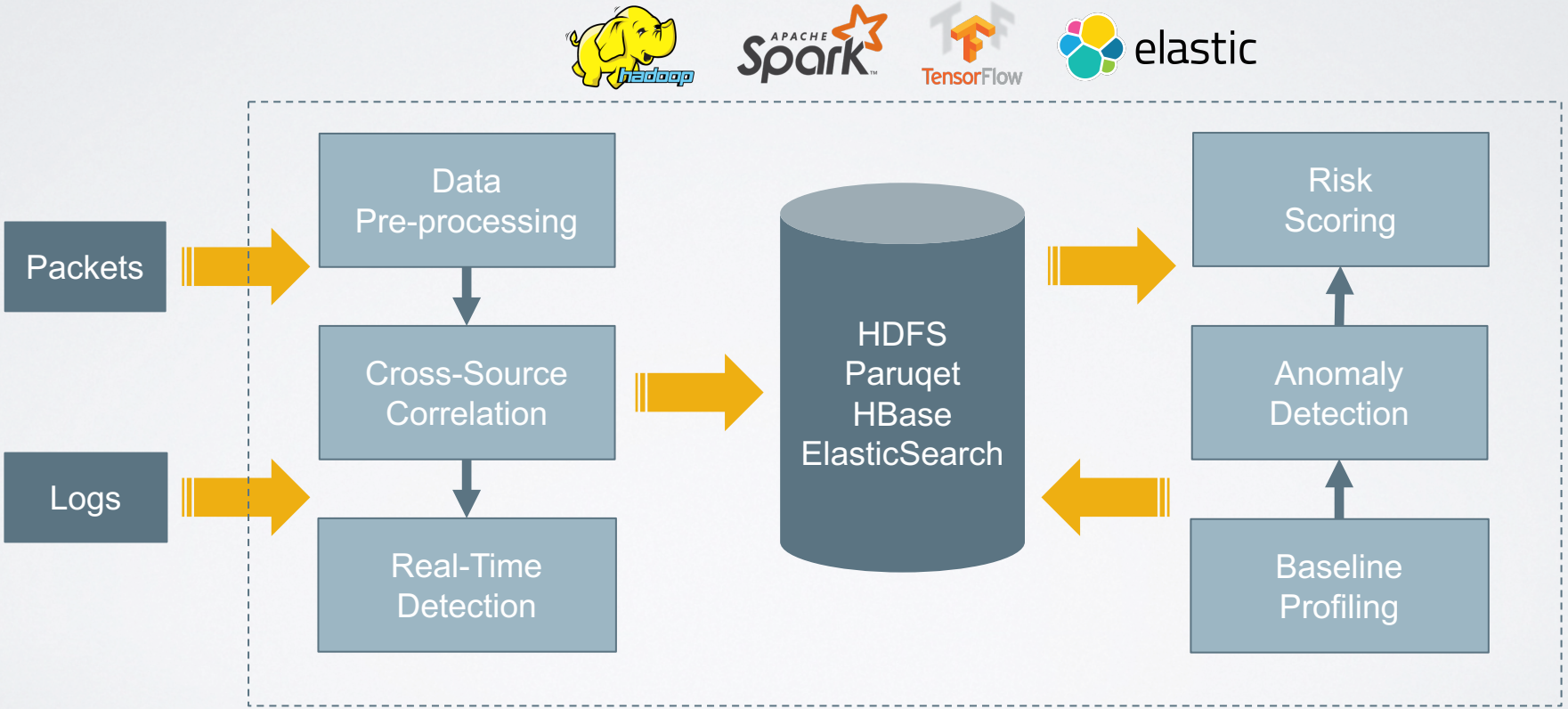
DEPLOYMENT STRATEGIES DISTRIBUTED TENSORFLOW



DEPLOYMENT STRATEGIES TENSORFLOW ON SPARK



DATA PIPELINE BIG DATA ECOSYSTEM



USER & ENTITY BEHAVIOR ANALYTICS

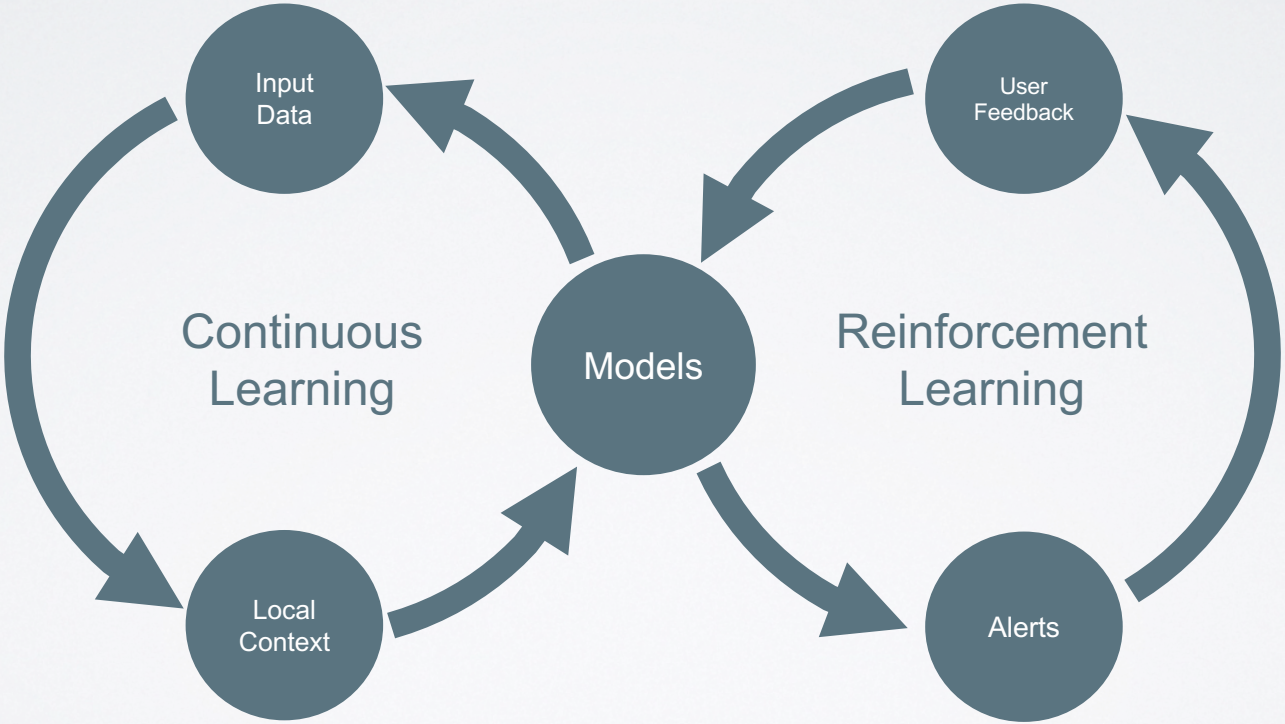
UEBA SECURITY
why this matters

USE CASES
how to detect malicious insiders

INFRASTRUCTURE
how to build big data infrastructure

CHALLENGES
how to build an enterprise solution

LOCAL CONTEXT HUMAN + MACHINE INTELLIGENCE

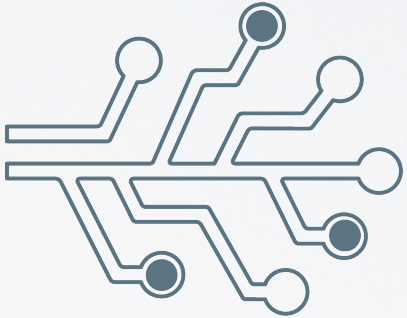


TRAINING DATA GLOBAL + LOCAL INTELLIGENCE

USER & ENTITY BEHAVIOR ANALYTICS

UEBA SECURITY
why this matters

USE CASES
how to detect malicious insiders



INFRASTRUCTURE
how to build big data infrastructure

CHALLENGES
how to build an enterprise solution

Thank You