



# Deep Learning In Security

An Empirical Example in User & Entity Behavior Analytics (UEBA)

Jisheng Wang

June 7, 2017

**aruba**  
a Hewlett Packard  
Enterprise company

- **Jisheng Wang, Senior Director of Data Science, CTO Office, Aruba / HPE**
  - Over 12-year experiences: Machine Learning + Big Data => Security
  - Chief Scientist, Niara, lead overall data analytics innovation and development
  - Ph.D from Penn State, Technical Lead in Cisco
- **Niara – a Hewlett Packard Enterprise company**
  - Recognized leader by Gartner in User and Entity Behavior Analytics (UEBA)
  - Re-invent enterprise security using big data and data science
  - Acquired by Aruba, a Hewlett Packard Enterprise company in Feb, 2017

# USER & ENTITY BEHAVIOR ANALYTICS

**aruba**  
a Hewlett Packard  
Enterprise company



## UEBA SECURITY

why this matters



## UEBA SOLUTION

how to detect attacks before damage is done

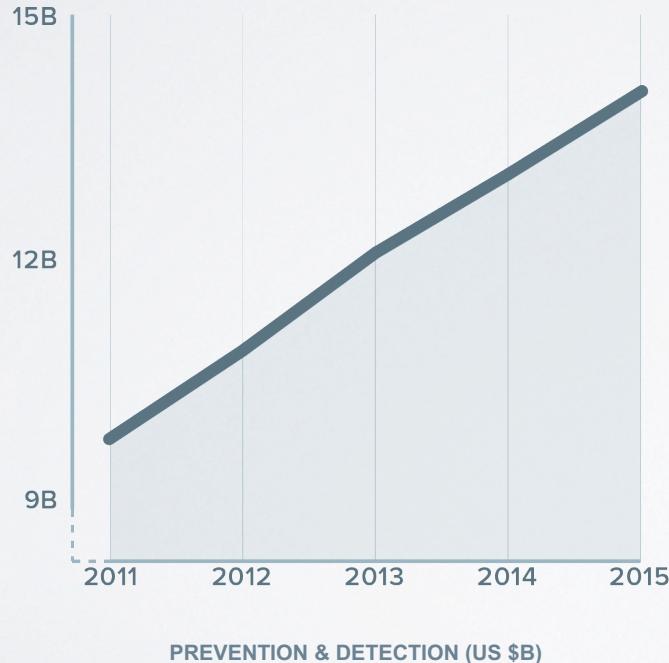


## BEYOND DEEP LEARNING

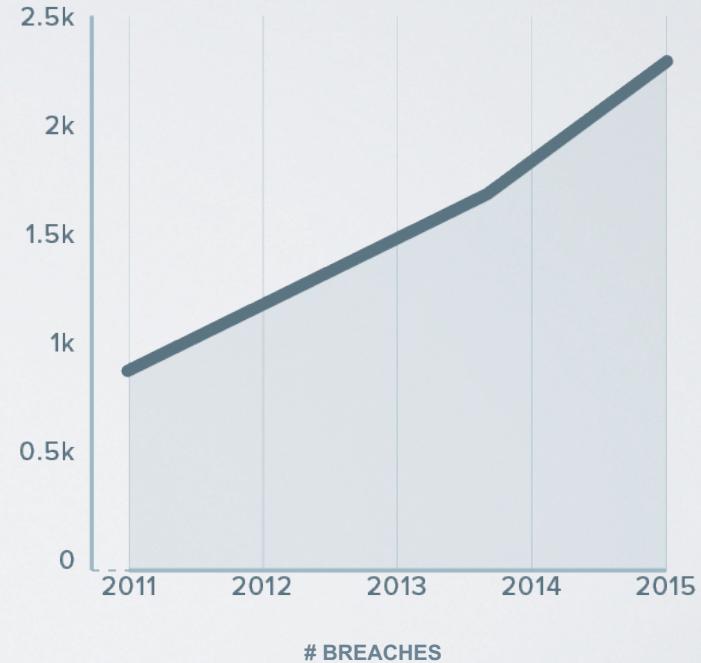
how to build a comprehensive solution

# PROBLEM THE SECURITY GAP

## SECURITY SPEND



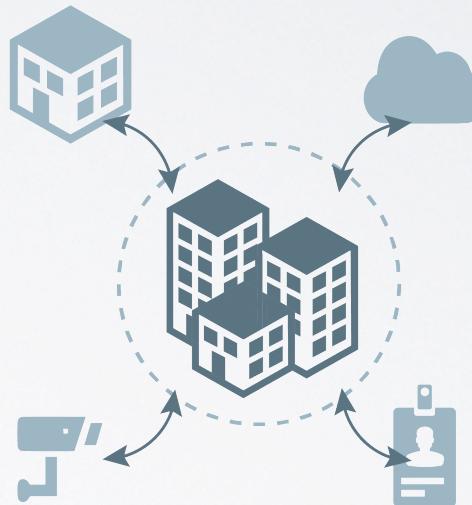
## DATA BREACHES



# PROBLEM CAUSE OF THE GAP



**ATTACKERS**  
ARE QUICKLY INNOVATING &  
ADAPTING

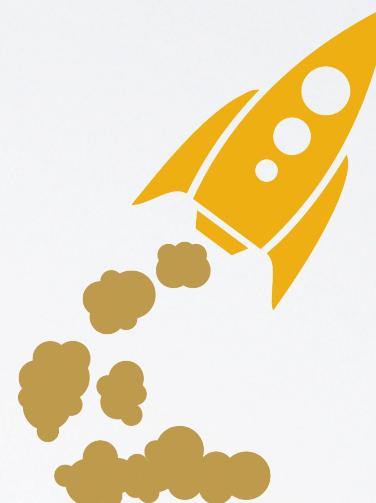


**BATTLEFIELD**  
WITH IOT AND CLOUD, SECURITY  
IS BORDERLESS

# PROBLEM ADDRESSING THE CAUSE

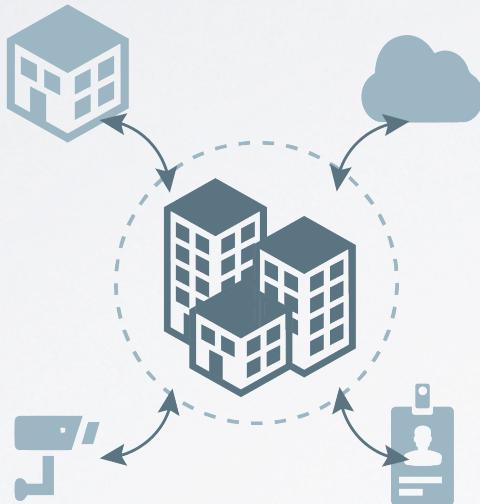


**ATTACKERS**  
ARE QUICKLY INNOVATING &  
ADAPTING



**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

## 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 servers

---

STOLEN CREDENTIALS



## MALICIOUS

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



## UEBA SECURITY

why this matters



## UEBA SOLUTION

how to detect attacks before damage is done



## BEYOND DEEP LEARNING

how to build a comprehensive solution

# REAL WORLD ATTACKS CAUGHT BY NIARA



## SCANNING ATTACK

scan servers in the data center to find out vulnerable targets

---

DETECTED WITH AD LOGS



## DATA DOWNLOAD

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

---

DETECTED WITH NETWORK TRAFFIC



## EXFILTRATION OF DATA

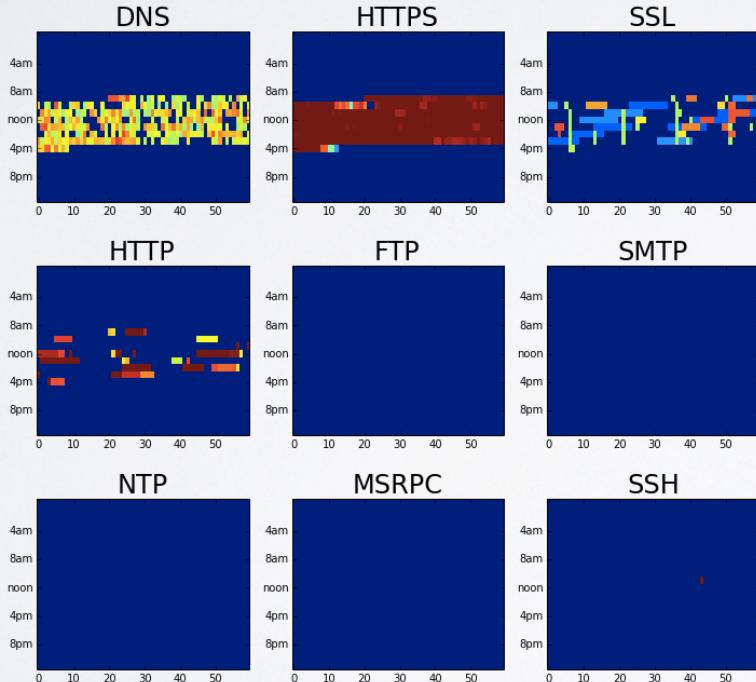
upload a large file to cloud server hosted in new country never accessed before

---

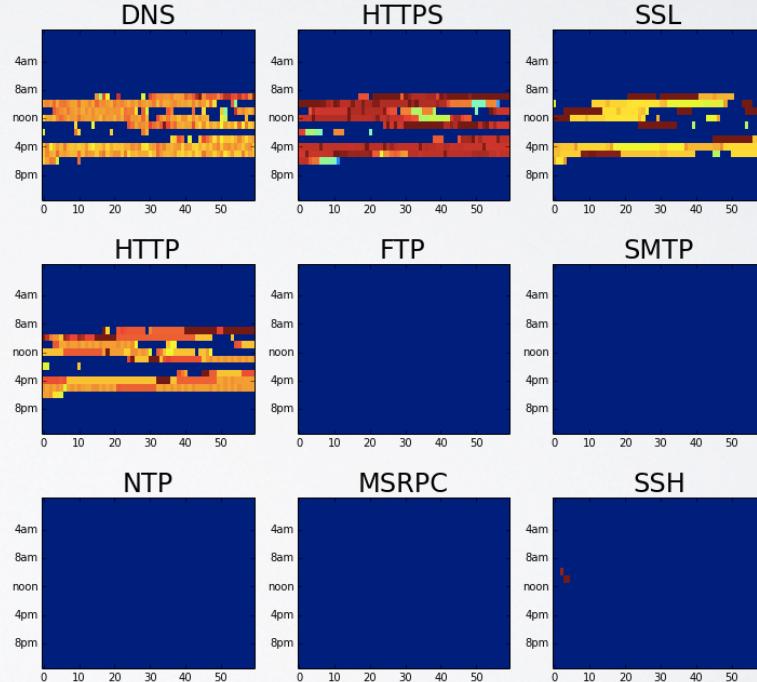
DETECTED WITH WEB PROXY LOGS

# BEHAVIOR ENCODING USERS

User 1

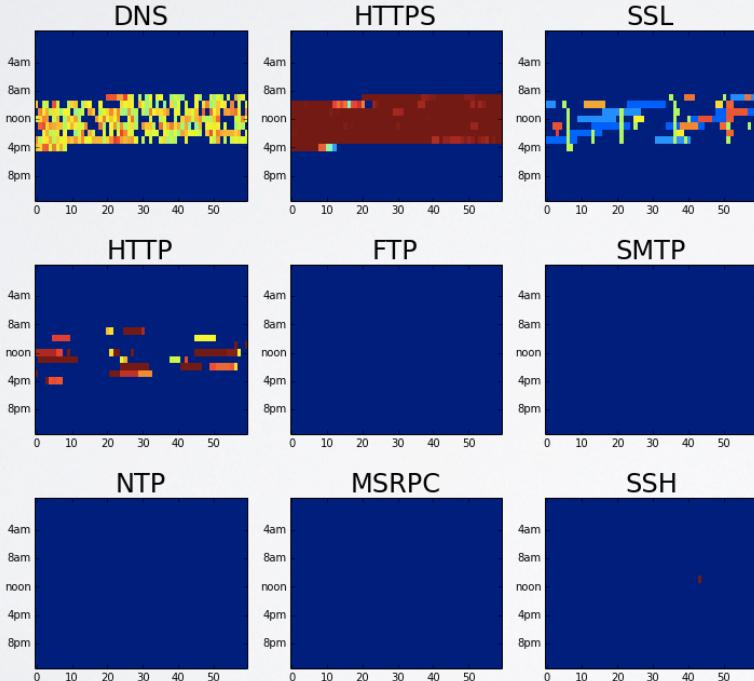


User 2

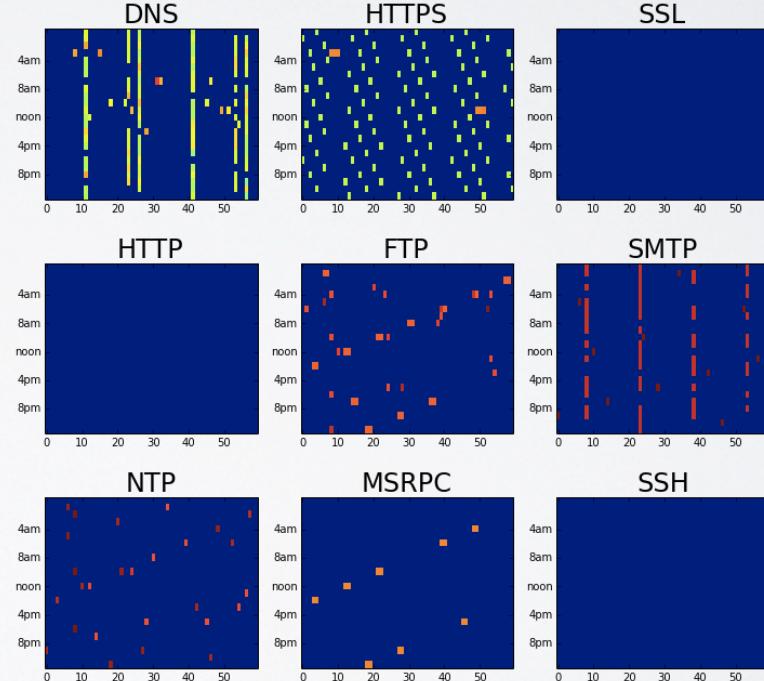


# BEHAVIOR ENCODING USER VS MACHINE

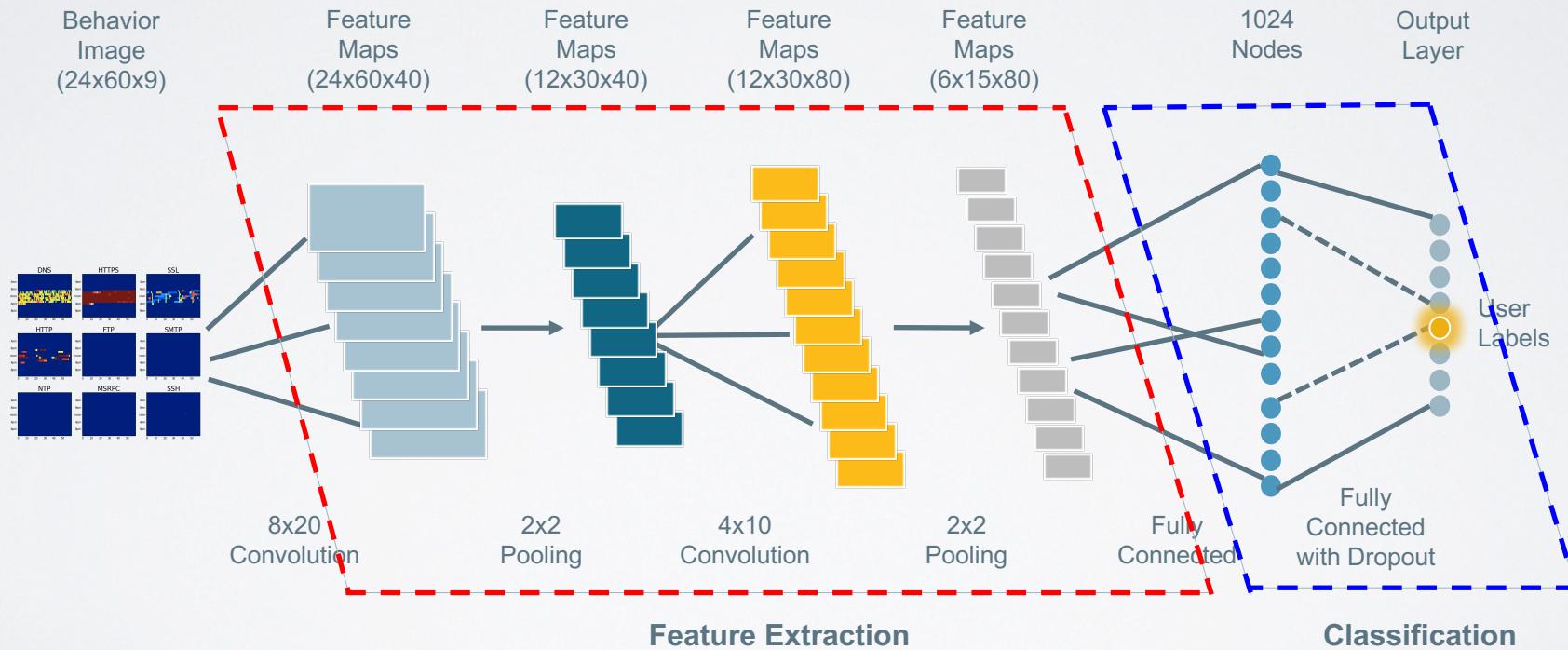
User



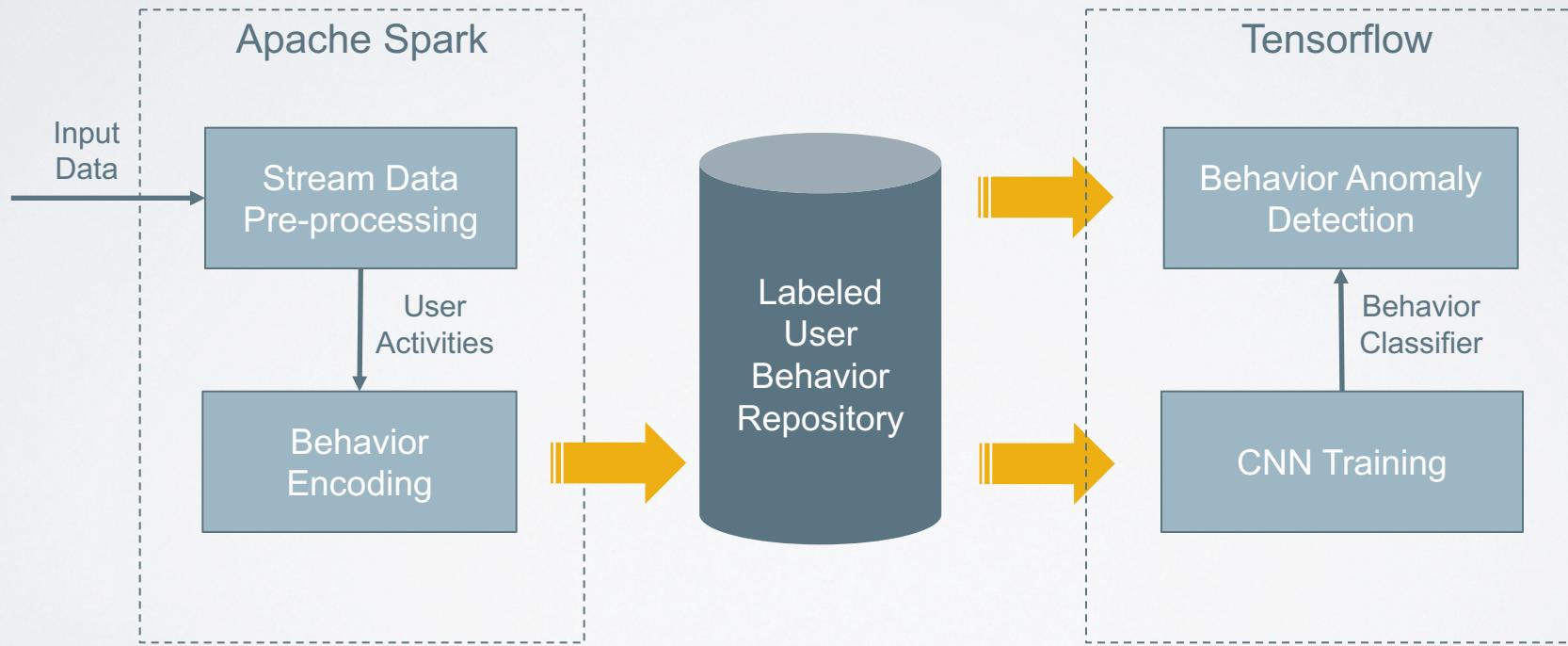
Machine



# ANOMALY DETECTION CONVOLUTIONAL NEURAL NETWORK (CNN)

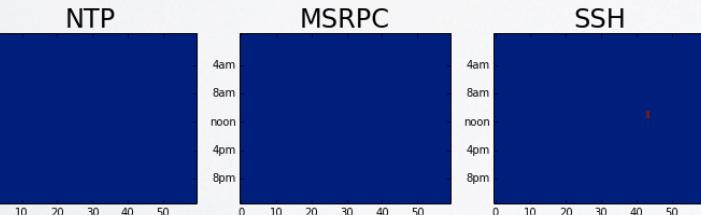
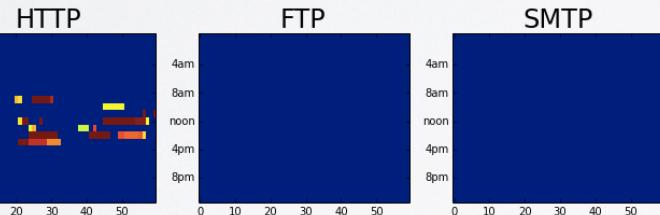
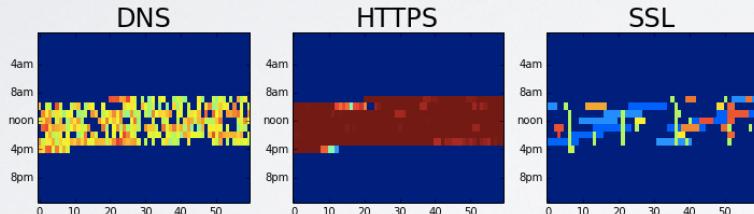


# ANOMALY DETECTION ARCHITECTURE

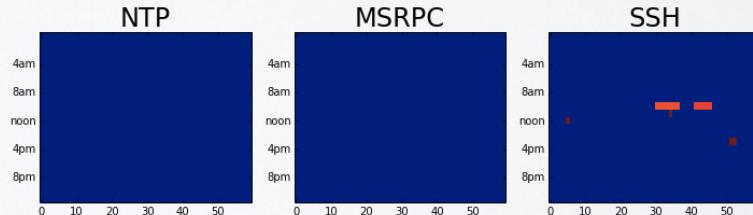
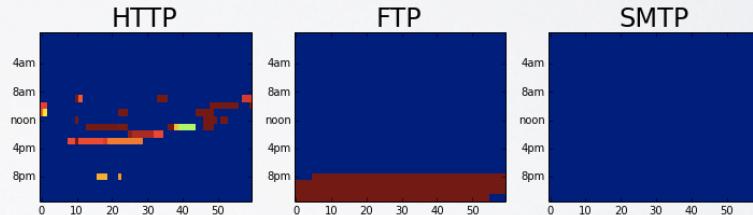
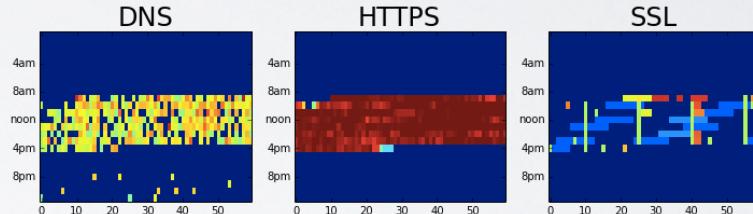


# BEHAVIOR ANOMALY USER | EXFILTRATION

User – Before Compromise

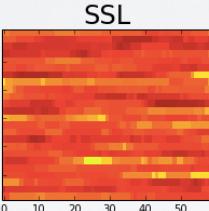
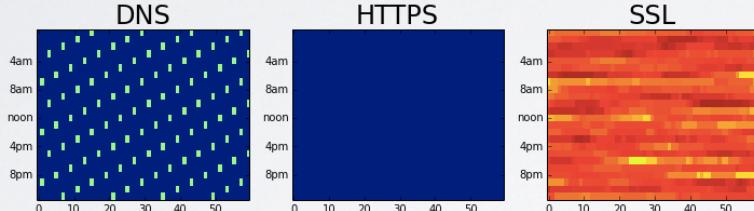


User – Post Compromise

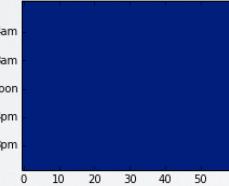


# BEHAVIOR ANOMALY IOT DEVICE | DATA DOWNLOAD

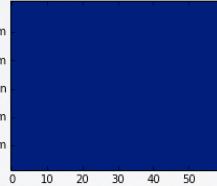
Dropcam – Before Compromise



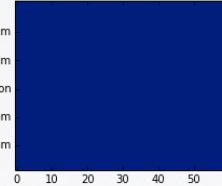
HTTP



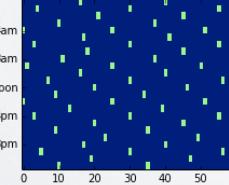
FTP



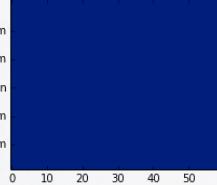
SMTP



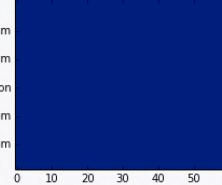
NTP



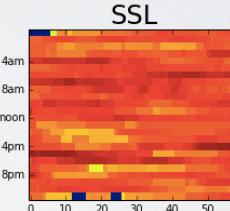
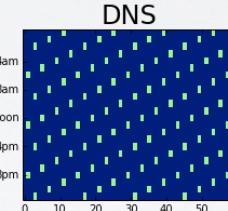
MSRPC



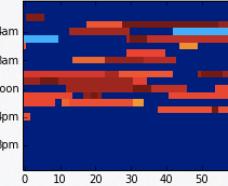
SSH



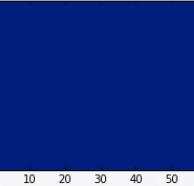
Dropcam – Post Compromise



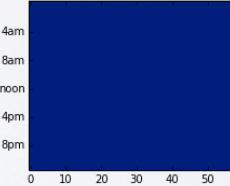
HTTP



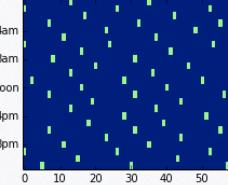
FTP



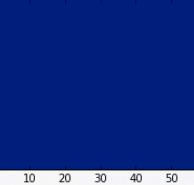
SMTP



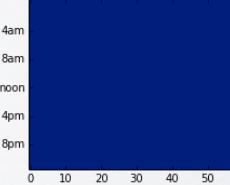
NTP



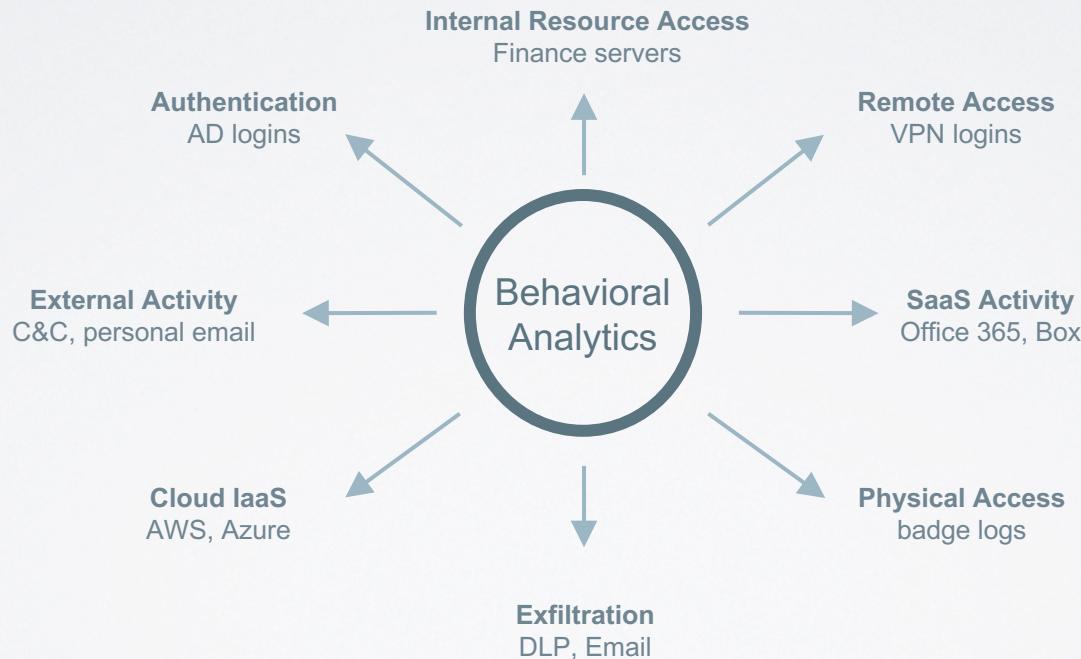
MSRPC



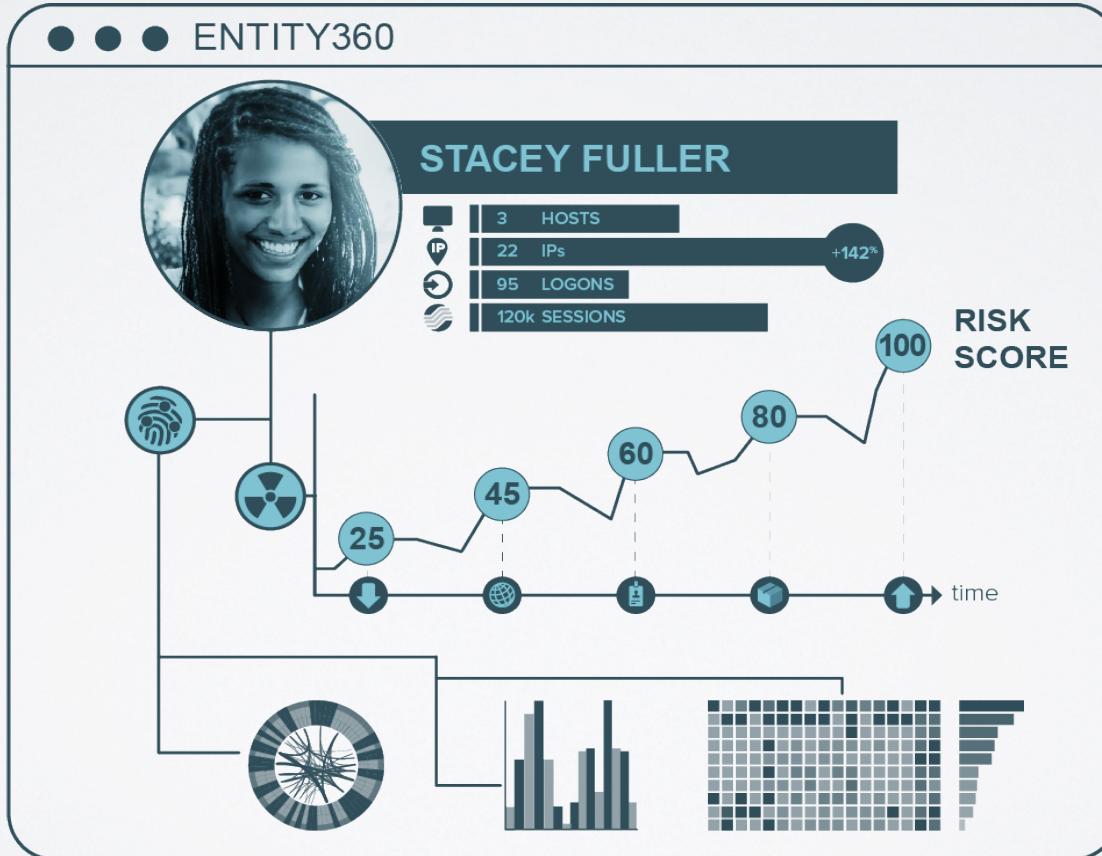
SSH



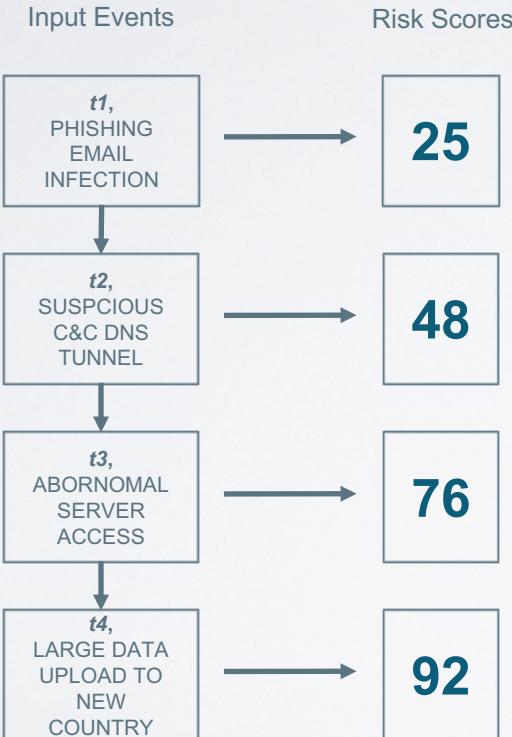
# BEHAVIOR ANALYTICS MULTI-DIMENSIONAL



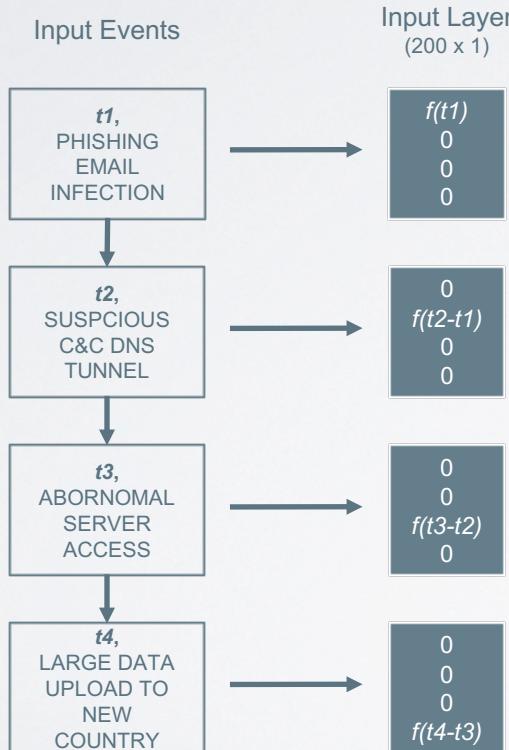
# ENTITY SCORING TEMPORAL SEQUENCE TRACKING



# ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)

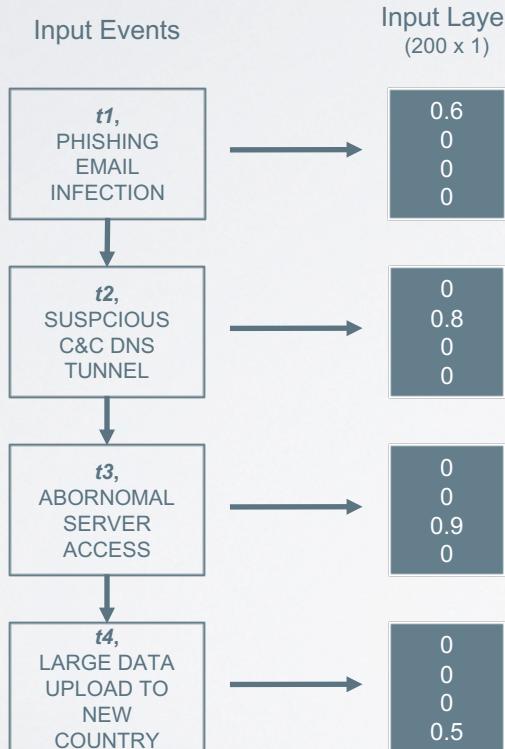


# ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



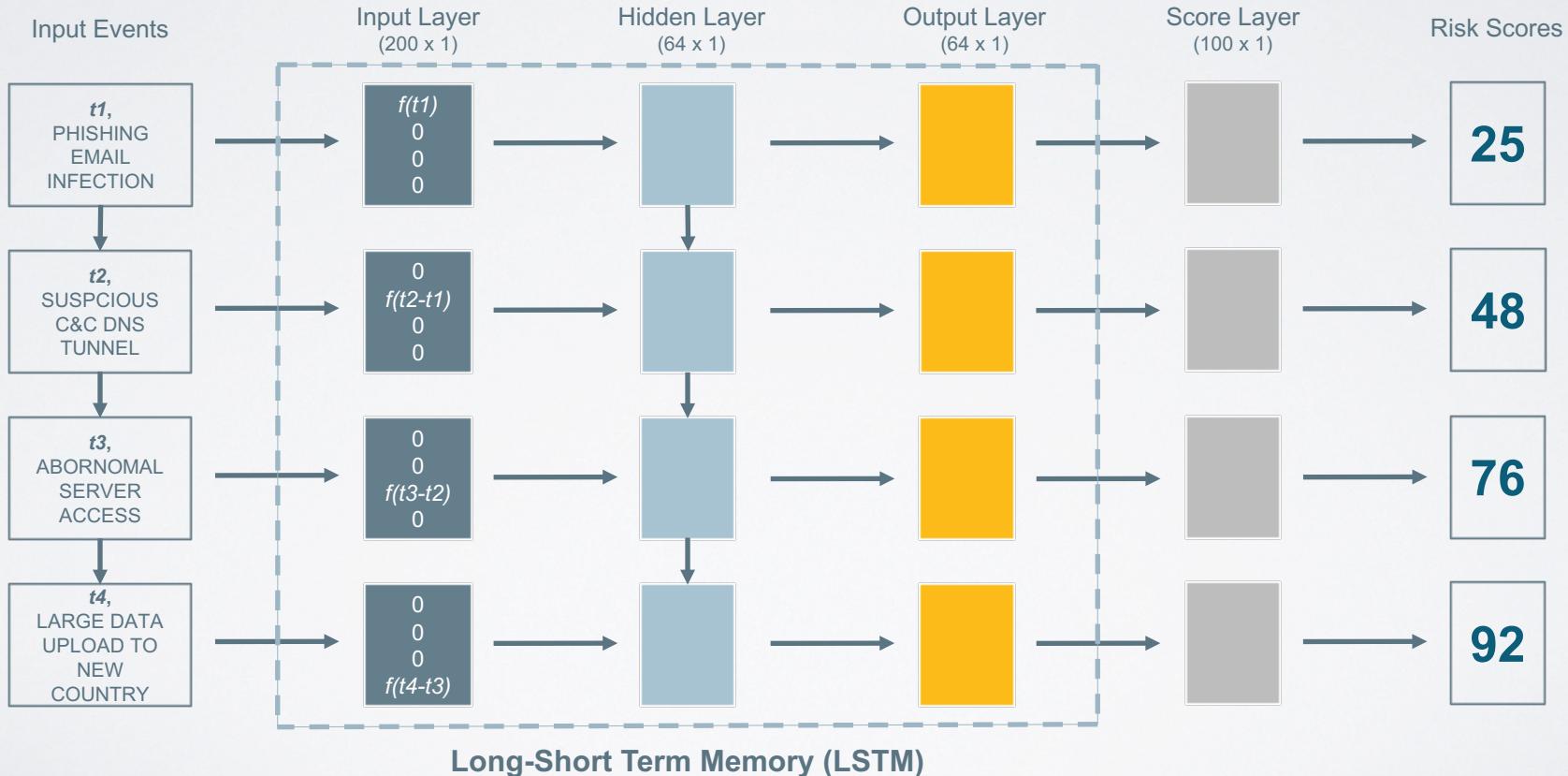
*one hot  
time-decayed  
encoding*

# ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



*one hot  
time-decayed  
encoding*

# ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



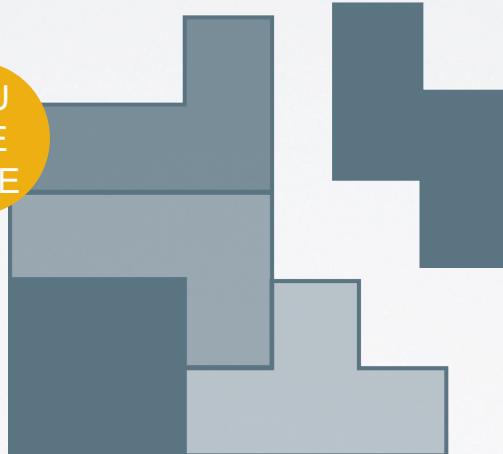
# USER & ENTITY BEHAVIOR ANALYTICS

**aruba**  
a Hewlett Packard  
Enterprise company



**UEBA SECURITY**  
what is UEBA

YOU  
ARE  
HERE

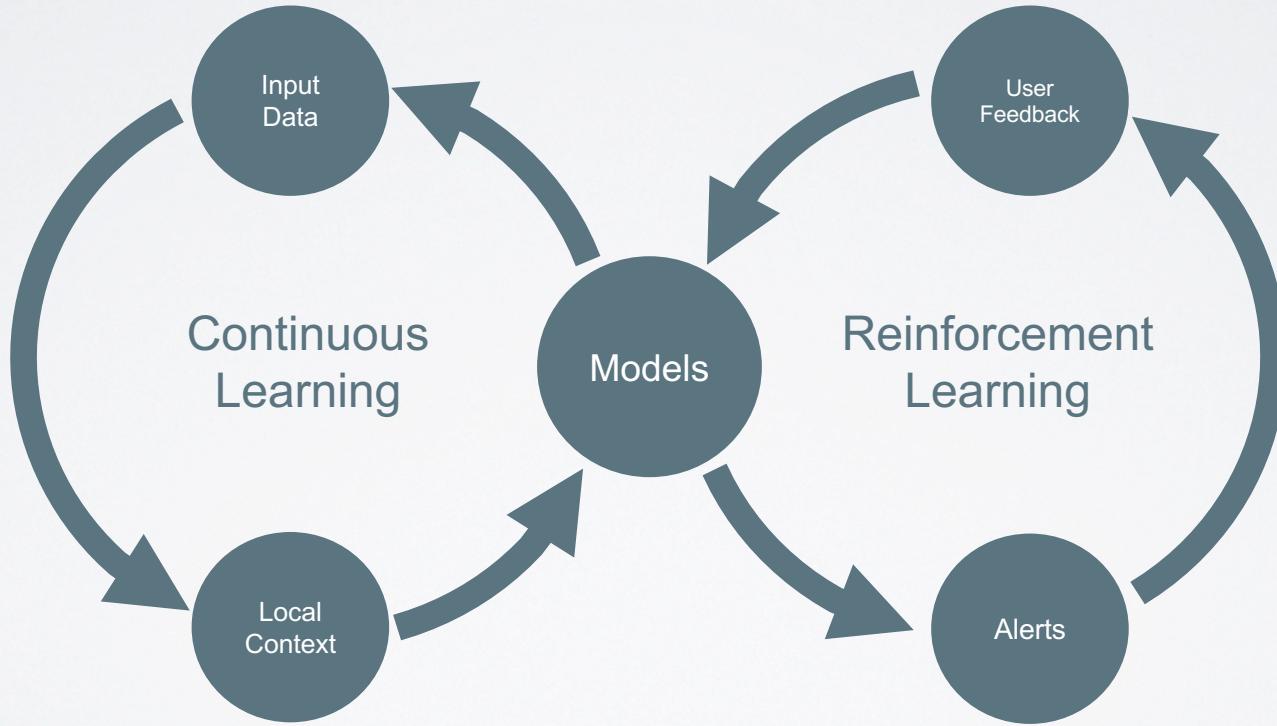


**UEBA SOLUTION**  
infrastructure needed to deep learning



**BEYOND DEEP LEARNING**  
how to build a comprehensive solution

# LOCAL CONTEXT MACHINE + HUMAN INTELLIGENCE



# TRAINING DATA GLOBAL + LOCAL INTELLIGENCE





## UEBA SECURITY

what is UEBA



## UEBA SOLUTION

infrastructure needed to deep learning



## BEYOND DEEP LEARNING

how to build a comprehensive solution



# Thank You

**aruba**  
a Hewlett Packard  
Enterprise company