PREDICTIVE SECURITY

Patent Pending

TECH MILEAGE
SOFTWARE SOLUTIONS

CONTENTS

PREDICTIVE SECURITY – A NEED

Explosion of Data Security Breaches

- Recent global security breaches have triggered awareness of the need to proactively protect sensitive customer data
- CISO/CSO organizations are looking into **predictive** security models as compared to current **reactive** security models

10.7MM

Records Exposed

**Identity Theft Resource Center, 2014 Data Breach Category Summary, June 2014*

BY THE TIME A BREACH IS DETECTED, IT'S TOO LATE

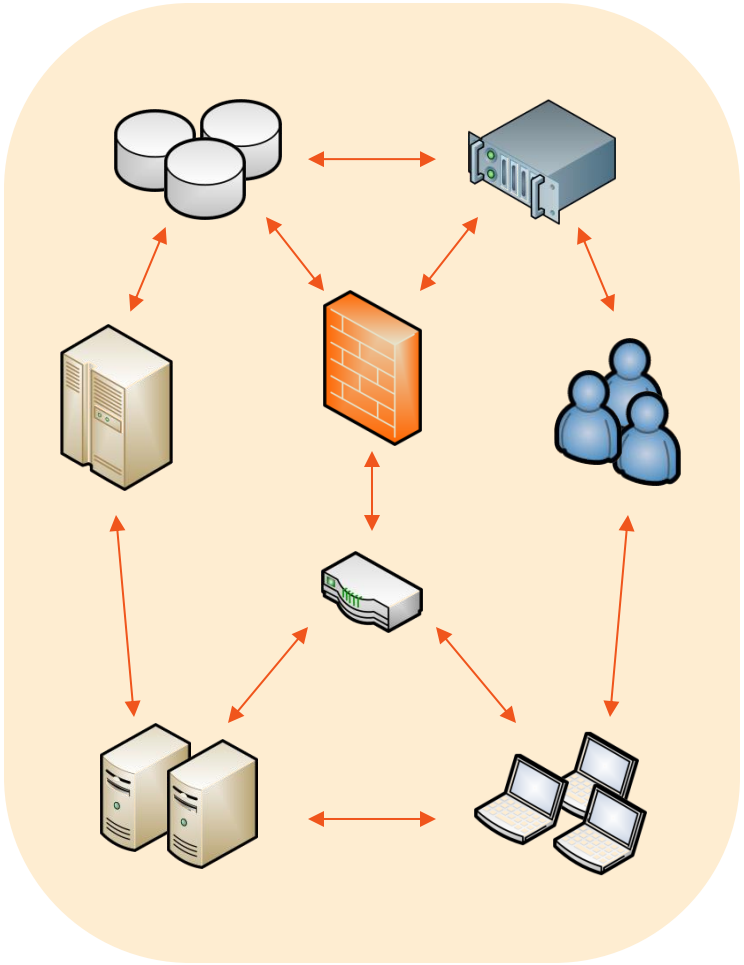
Reactive Approaches are No Longer Sufficient

- Security increasingly viewed as liability and not just cost of doing business
- Current reactive privacy assurance and personal data security practices are being questioned
- Security failures can cause significant direct or indirect financial impact
  - *e.g. stock market reaction to recent breaches*
- Reactive approach is costly and ineffective
  - *e.g. loss of brand reputation*
- Consumer insecurity decreases loyalty
- Security breaches due to "Authorized Malicious Access" can be as costly as a cyber attack

Emerging paradigm dictates a need for a continuously verifiable predictive security model

PROPOSED SOLUTION

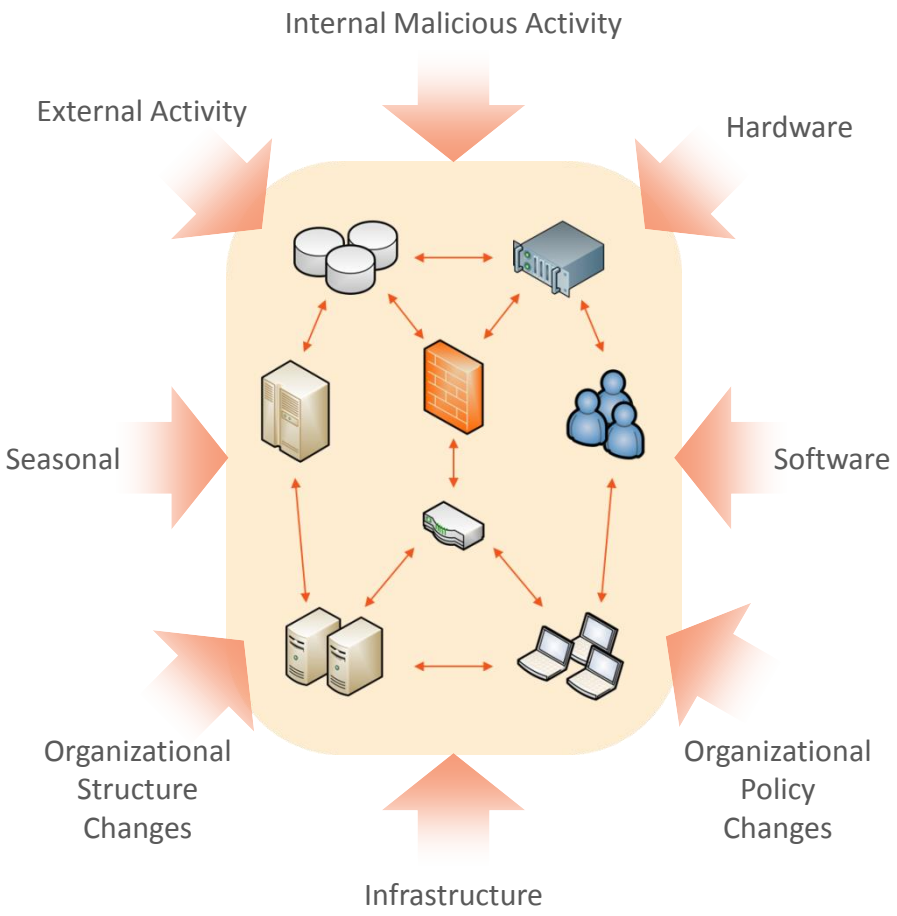
Every Organization is a Finely Balanced Ecosystem



- Organizational ecosystems consist of *entities*
  - Databases, Servers, Human Resources, Networks, etc.
- Every entity has rules and policies which determine its behavior
- To exist, the ecosystem needs to be in balance
- Every entity has a predictable pattern of behavior; a combination of these behaviors brings the ecosystem into a balanced state
- Due to the dynamic nature of entities, ecosystem balance needs to be adaptive
- Every entity has its own internal balance – entities can go out of balance for legitimate or illegitimate reasons

ADAPTIVE BALANCE OF ECOSYSTEM

Causes of Imbalances in the Ecosystem

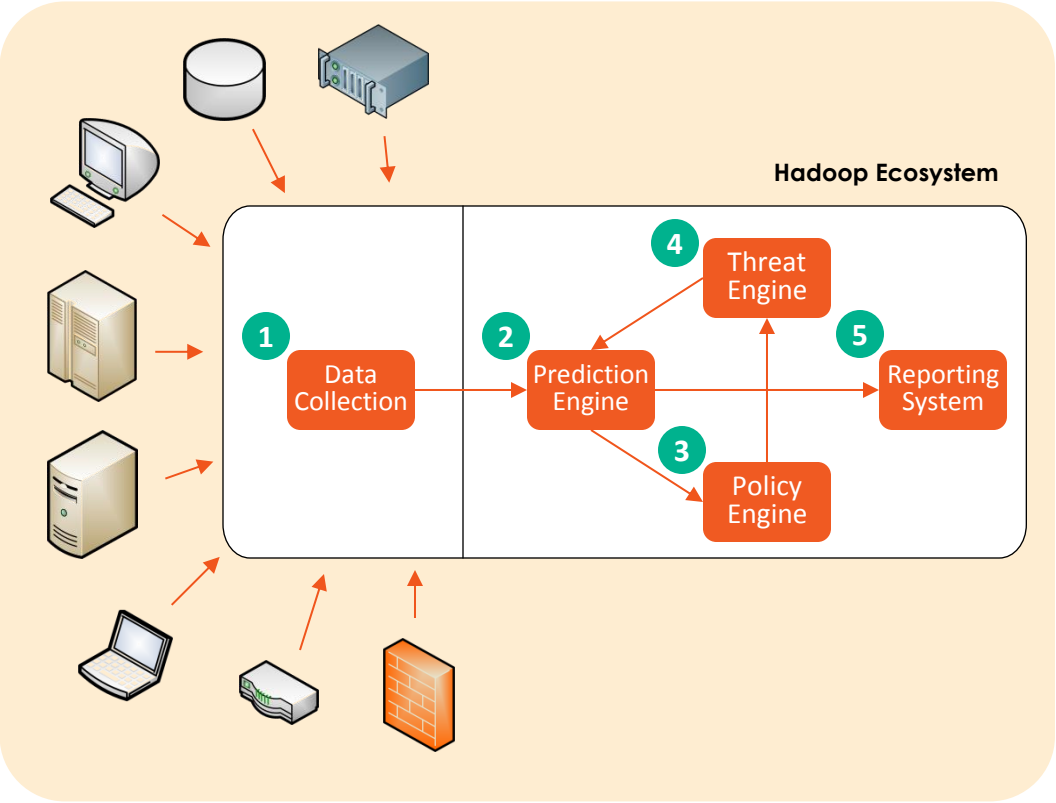


- When an entity is out of balance, it creates an imbalance in the whole ecosystem
- The ecosystem will try to **adaptively** balance itself by examining recent changes in the behavior (rules and policies) of the entity creating the imbalance
- If the cause of the imbalance is legitimate, the ecosystem adaptively comes to a **new balance** – which becomes the baseline for the ecosystem
- If the cause of the imbalance is not determined, the ecosystem raises alerts
- Alerts can be used to calculate threat level
- Threat levels determine the action required within the ecosystem to create a balance

CONCEPT OVERVIEW

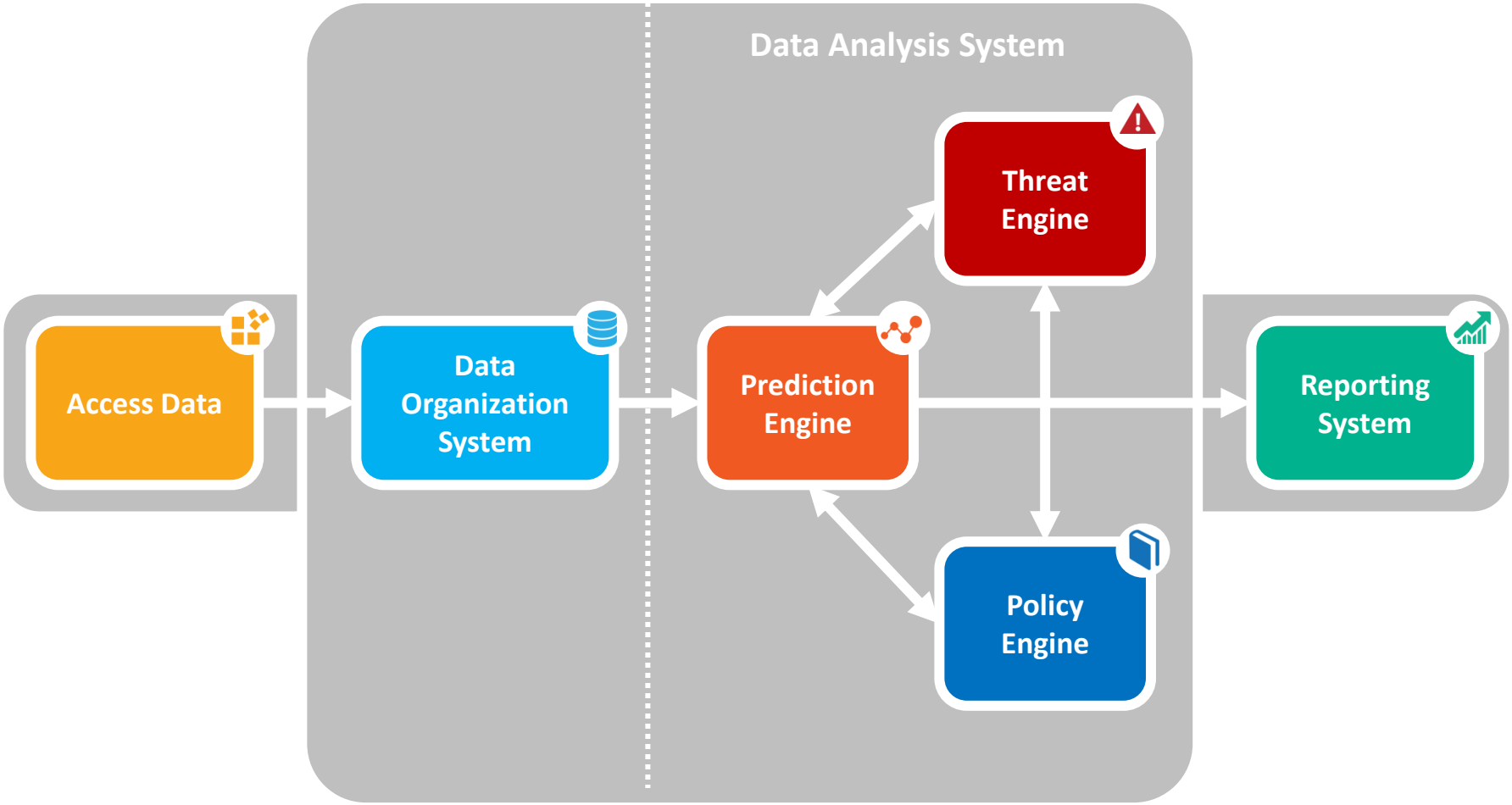
PREDICTIVE MODELING FOR BALANCING THE ECOSYSTEM

5 Steps to a Balanced Ecosystem

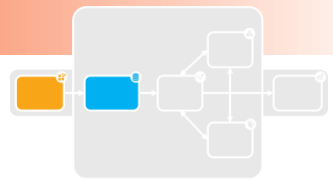


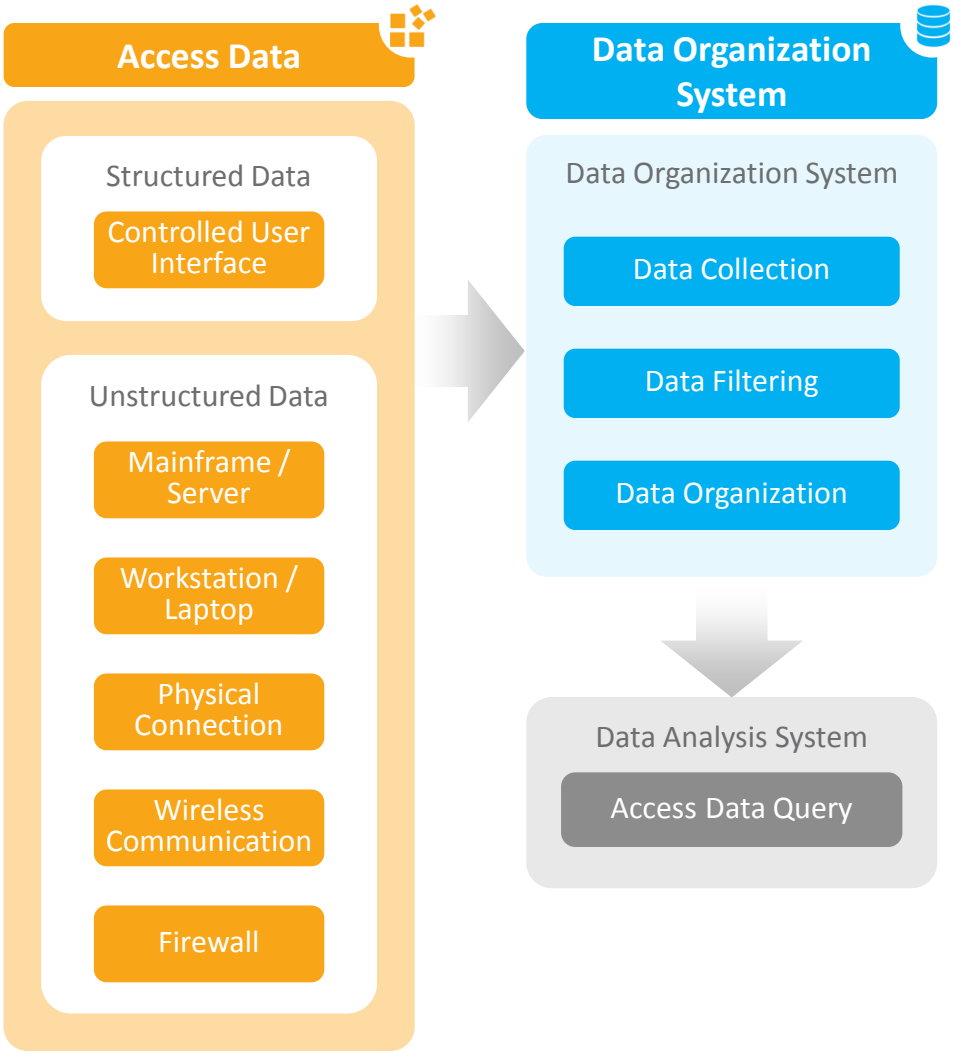
1. Collect structured and unstructured data from every entity in the organization's ecosystem
2. Process the information to identify patterns and correlations for every entity with as much granularity as possible
3. Match the patterns and correlations against rules and policies
4. Identify anomalous behaviors and calculate the level of threat
5. Generate heat maps and identify possible areas of impact
   - Identify individuals/vendors/actors posing a threat
   - Take appropriate action, either manually or automatically

SYSTEM OVERVIEW



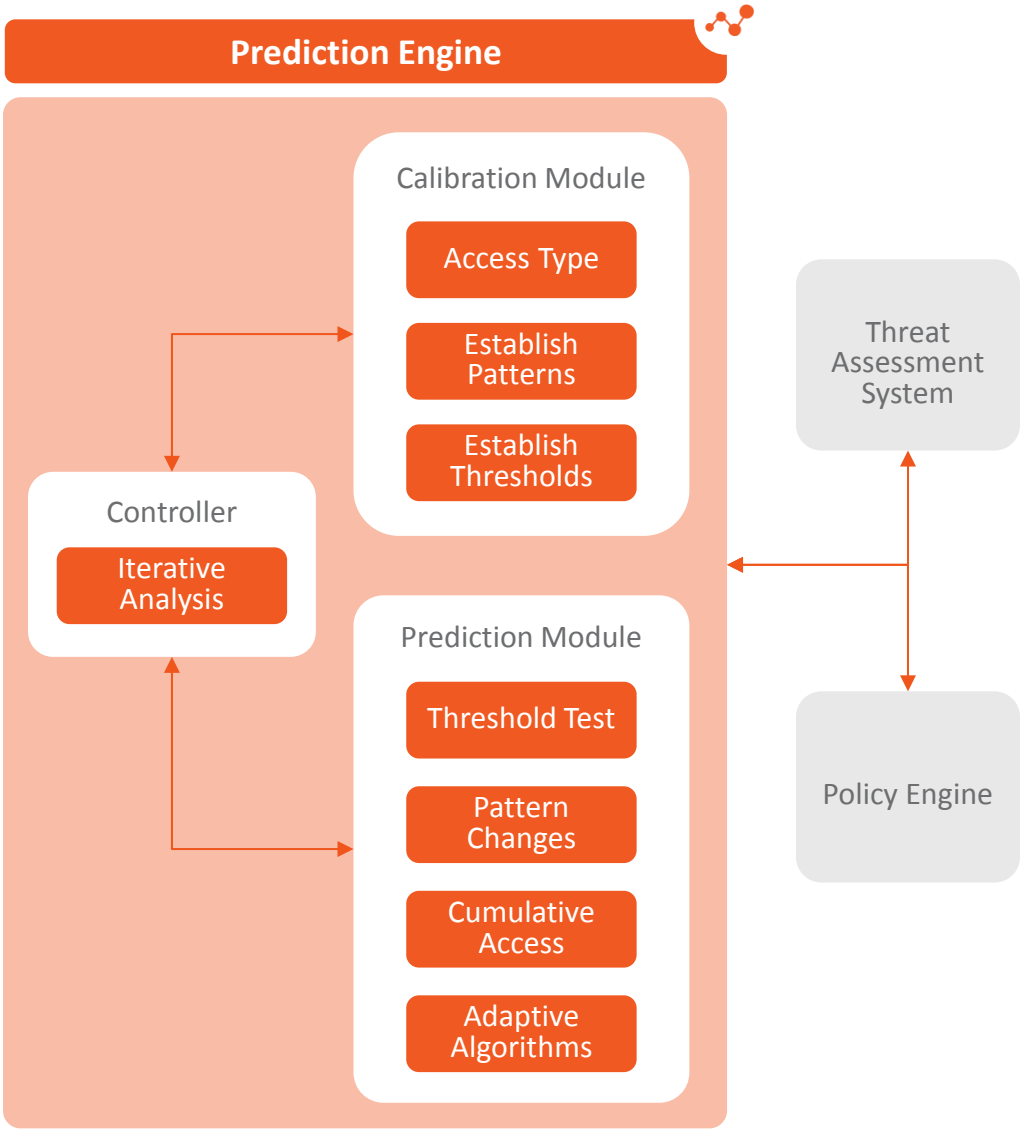
DATA COLLECTION & PROCESSING





- Collect structured or unstructured data from every relevant entity in the organization's ecosystem
- Extract relevant info from the data received and organize for analysis

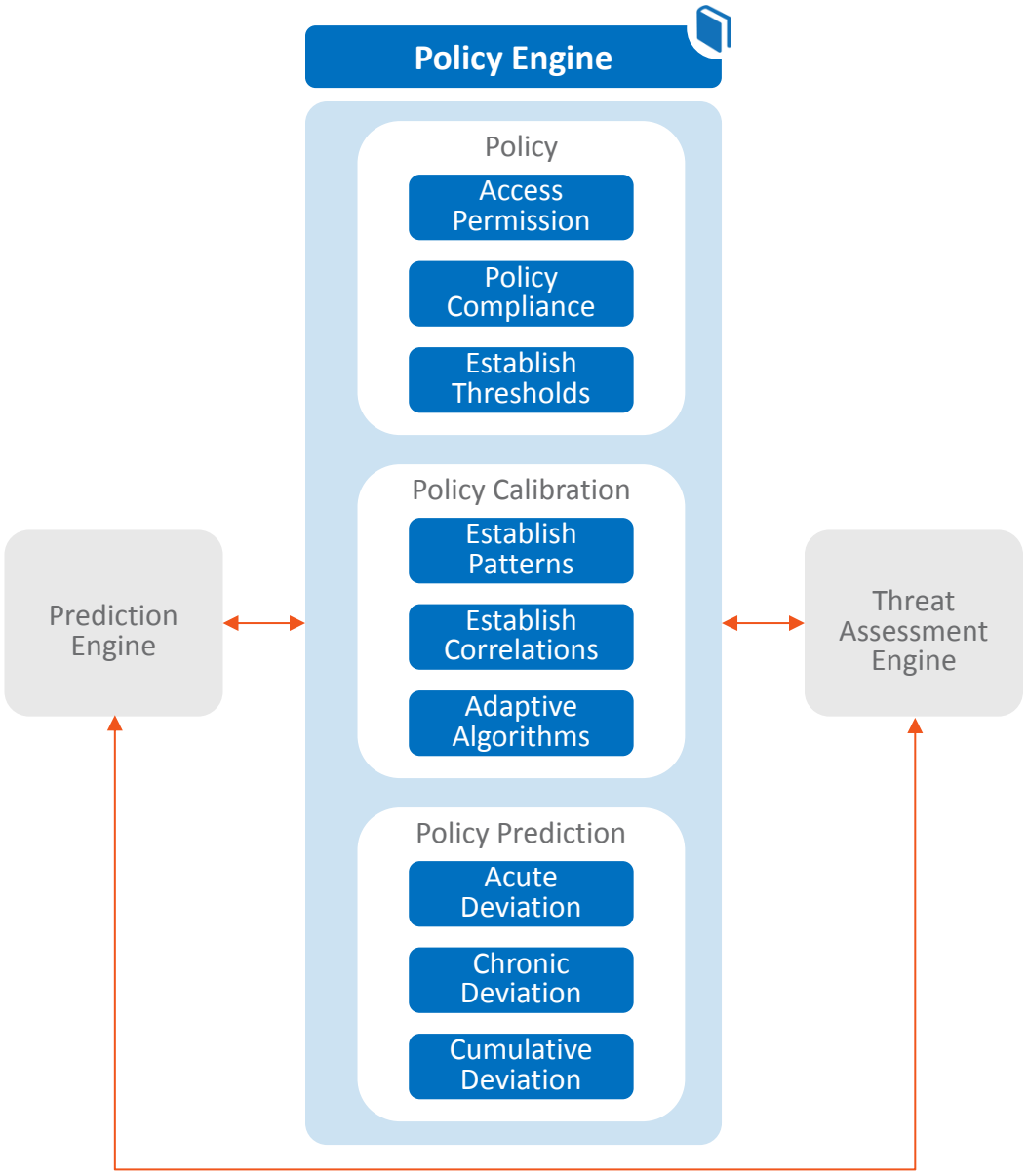
PREDICTION ENGINE



Agent-based Predictive Meta-Model Solution

- Process the collected information to identify patterns and correlations for every entity with as much granularity as possible
- Identify anomalous behaviors based on the deviation from existing patterns

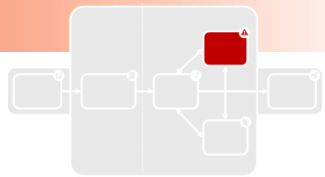
POLICY ENGINE

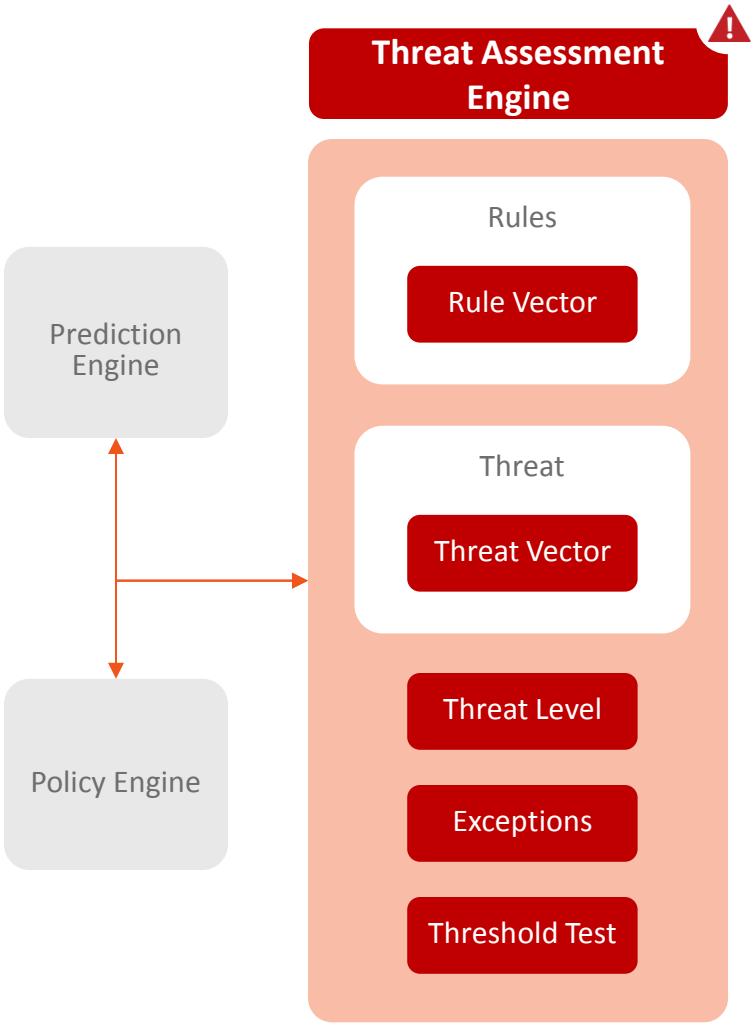


Engine to Maintain Organization-level Policies for Different Entities

- Once anomalous behaviors are identified, determine the severity of the deviation

THREAT ASSESSMENT / RULES ENGINE

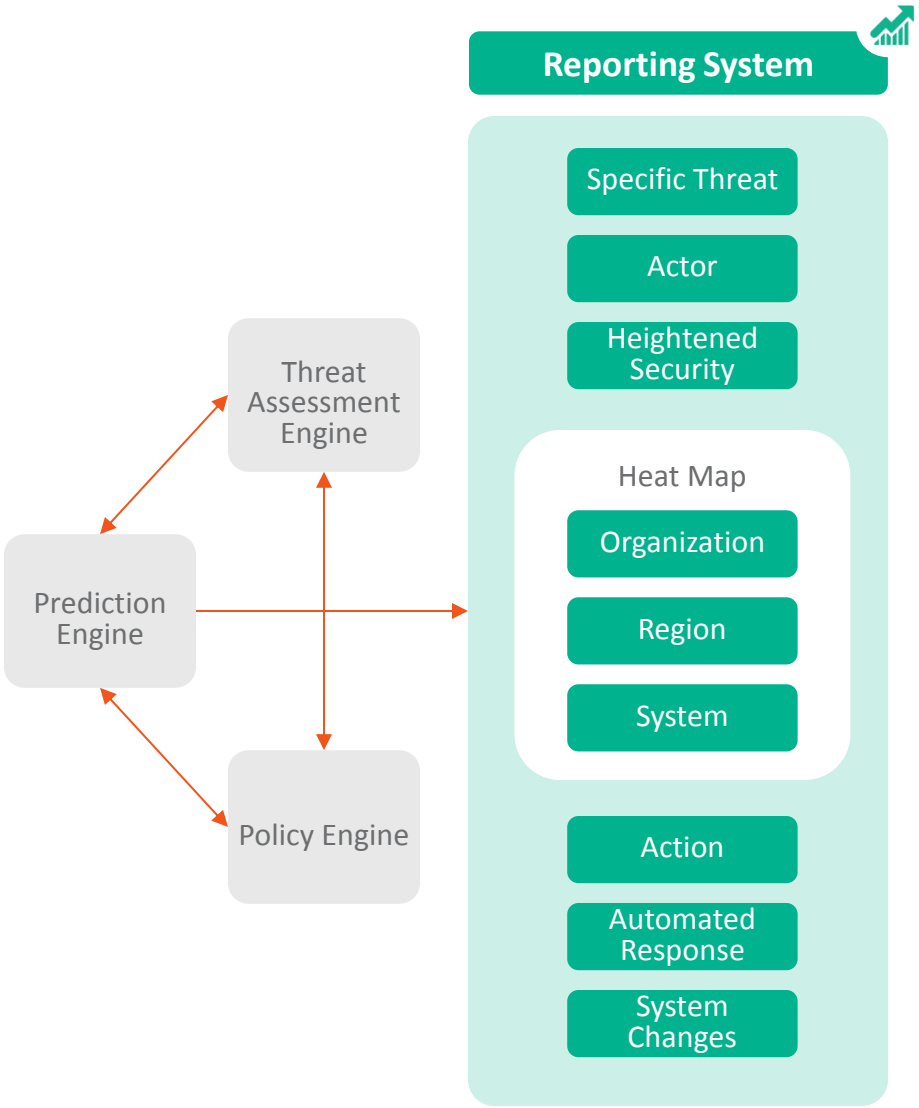




Engine to Maintain Organization-level Rules for Different Entities and Systems

- Calculate the level of threat posed by the policy deviation

REPORTING & ALERTS



Reporting System

- Generate reports and alerts to trigger manual or automated actions and responses

VIRTUAL CASE STUDY – TARGET SECURITY BREACH

Anatomy of a Security Breach

- Among various theories for the breach, one points to an "Authorized Malicious Access"
  - Credentials of a specific Target vendor were compromised
  - Credentials were used to access Target's internal systems & place malware on POS systems
  - Malware infected POS terminals for up to 2-3 months
  - Malware infection did not impact day-to-day operations; hence the breach was not noticed by internal IT
  - Breach was detected after a few days, however people failure extended it to 2-3 months; by the time the breach was detected, data losses had already occurred
  - Data for 70+ million customers was compromised
  - Strong reaction from stock market and customers

Analysts are estimating the cost of the Target breach to be in the range of **$1+ BILLION**

eBay breach was similar:
http://www.troyhunt.com/2014/05/the-ebay-breach-answers-to-questions.html

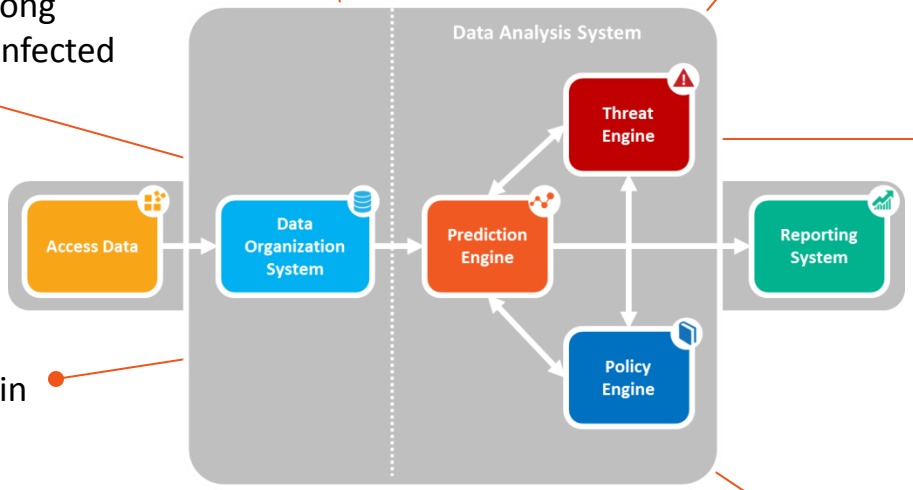
APPLYING PREDICTIVE SECURITY TO TARGET

How Predictive Security Would Have Detected the Breach

Predictive models would have identified vendors not following security policies

An imbalance in the ecosystem would have been detected based on transactions, network traffic, domains, etc.

Proactive monitoring of account access patterns could have identified **malicious intent** long before POS terminals were infected



An imbalance in the terminals could have identified the changes in activity and processing in the initial stages

Sudden changes in account **access patterns and footprints** could have been detected within the first 1-2 days, long before any data was lost

Correlations of network logs and data transactions would have identified changes in the behavior of traffic

Early identification of the imbalance in the organization's ecosystem could have saved millions and customer loyalty

TEAM

Dr. Chris Stephens

Full Professor and founding member (since 2000), C3-Centro de Ciencias de la Complejidad, Universidad Nacional Autonoma de Mexico, Mexico D.F. 04510

100+ publications in top international journals and proceedings, in data mining, quantitive analysis, complex adaptive systems, and artificial intelligence, with 1600+ global citations.

Dr. Eric Golla

Highly skilled and experienced leader of business intelligence, modeling, advanced analytics, model governance and data mining. Proven track record connecting resources, developing solutions, enhancing relationships, and providing effective executive communication.

Mike Tobin

Experienced analytical executive, leading groups responsible for customer insight, marketing research, database marketing, analytics and business intelligence, data warehousing and house file hygiene. 12 years each on the agency and client side of marketing analytics. Frequent conference presenter and published author on database marketing and business analytics topics.

ANALYTICS PATENTS

Patent Pending

- “Preventing malicious authorized access using predictive modeling”
  - Assigned inventor: Rajesh Kumar