

# VMware Carbon Black

Andrea Argentin – Lead Sales Engineer - Security Business Unit

# WHY CLOUD IS THE FUTURE OF SECURITY

---

## BETTER PROTECTION

BIG DATA +  
ANALYTICS

- Threat prediction & prevention
- Global threat monitoring
- Real-time intelligence

## SIMPLIFIED OPERATIONS

MANAGEMENT  
MODEL

- No infrastructure
- Easy for distributed workforce
- Automatic, real-time updates



# Cb PREDICTIVE SECURITY CLOUD

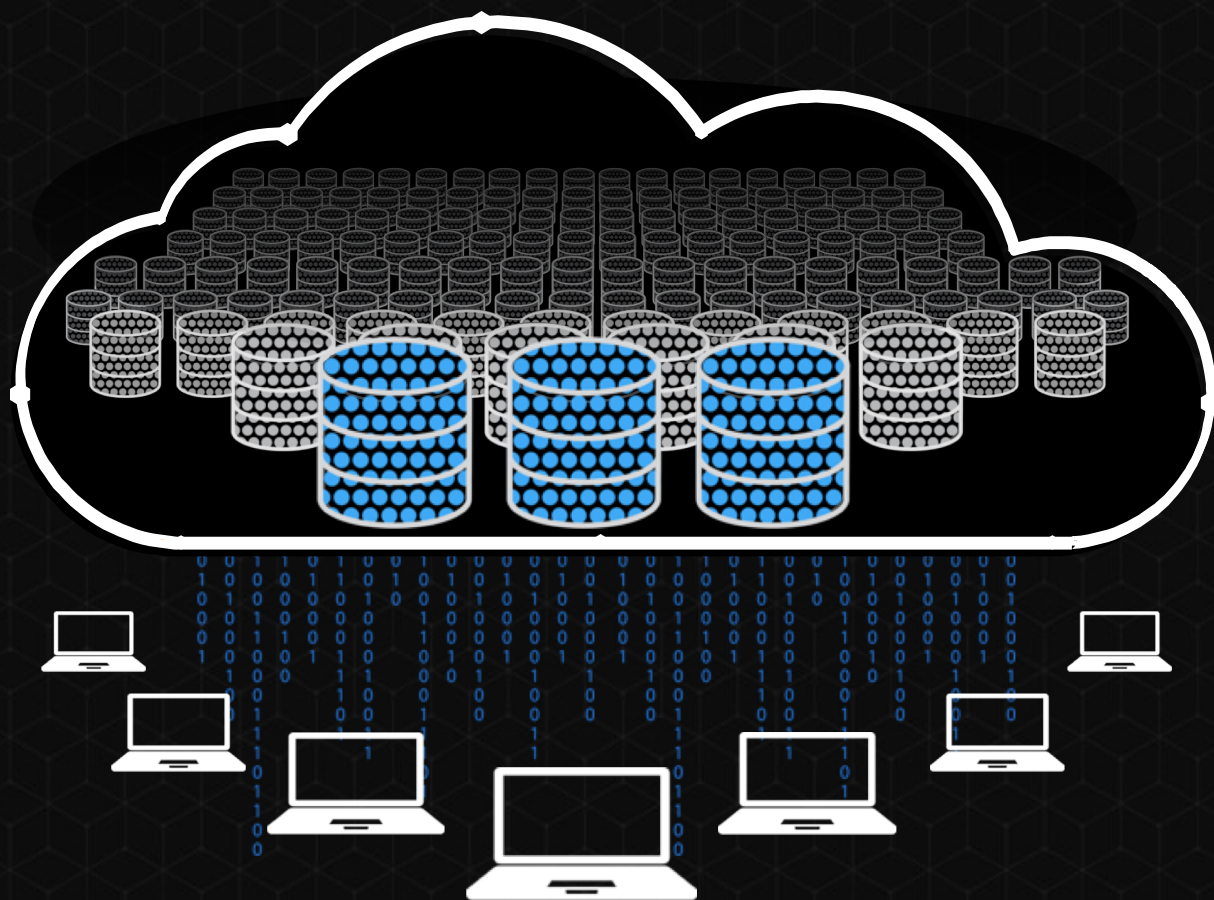




# Carbon Black's Differentiated Approach

# THE POWER OF THE PREDICTIVE SECURITY CLOUD

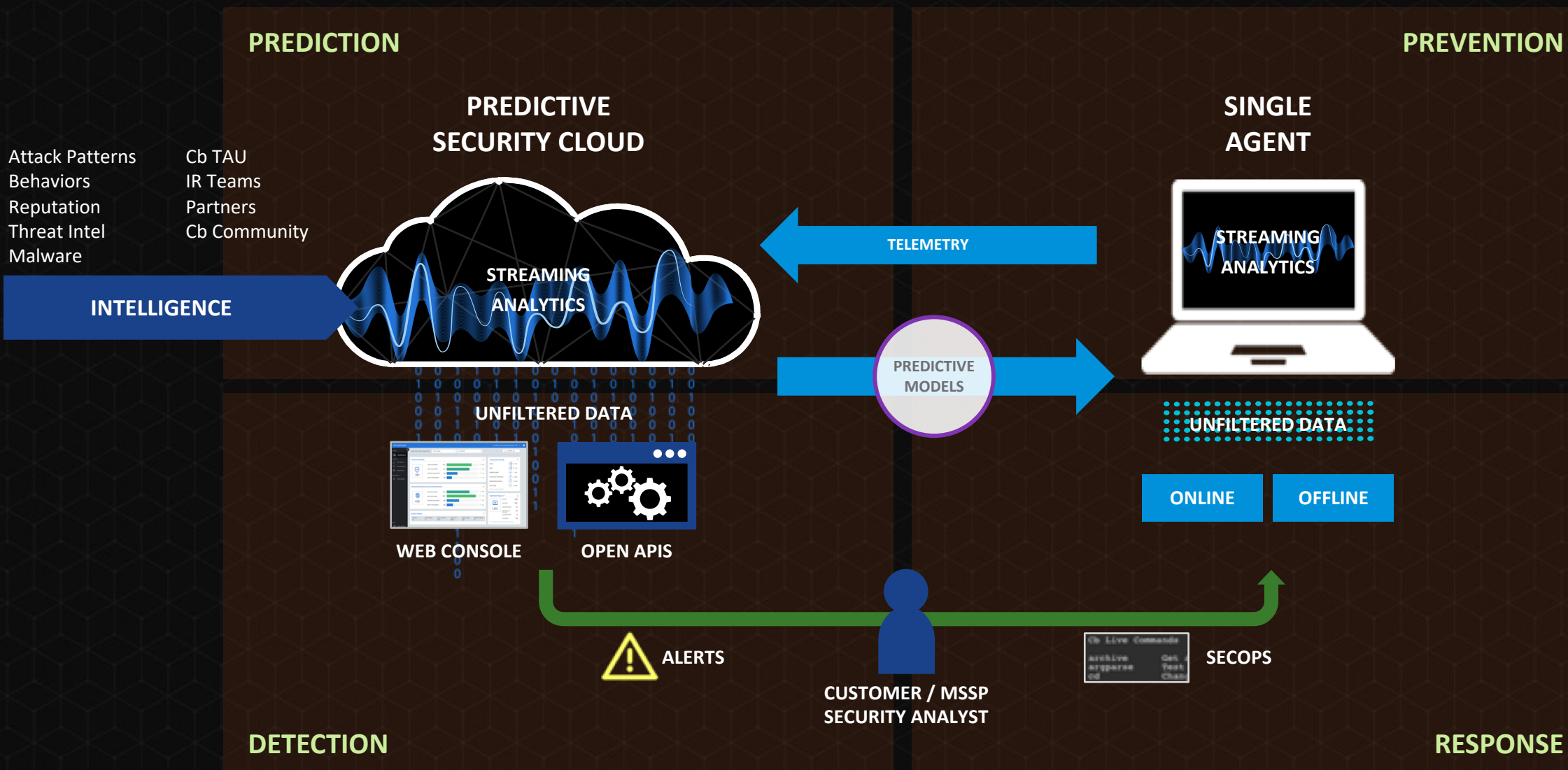
---



- **Elastic** storage and processing power
- Increased **visibility** across every environment
- Allows us to **learn, develop** and **deploy** new solutions much faster



# PSC ARCHITECTURE





# Agenda

**1 How the PSC Detects**

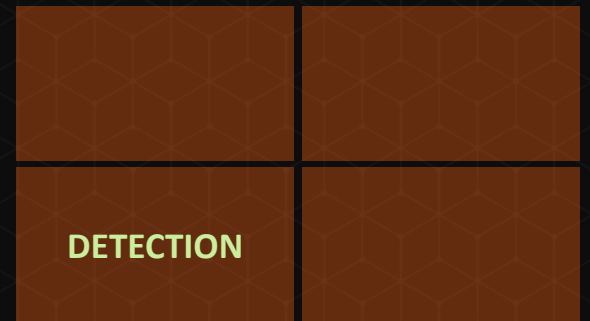
**2 How the PSC Learns**

**3 How the PSC Prevents**

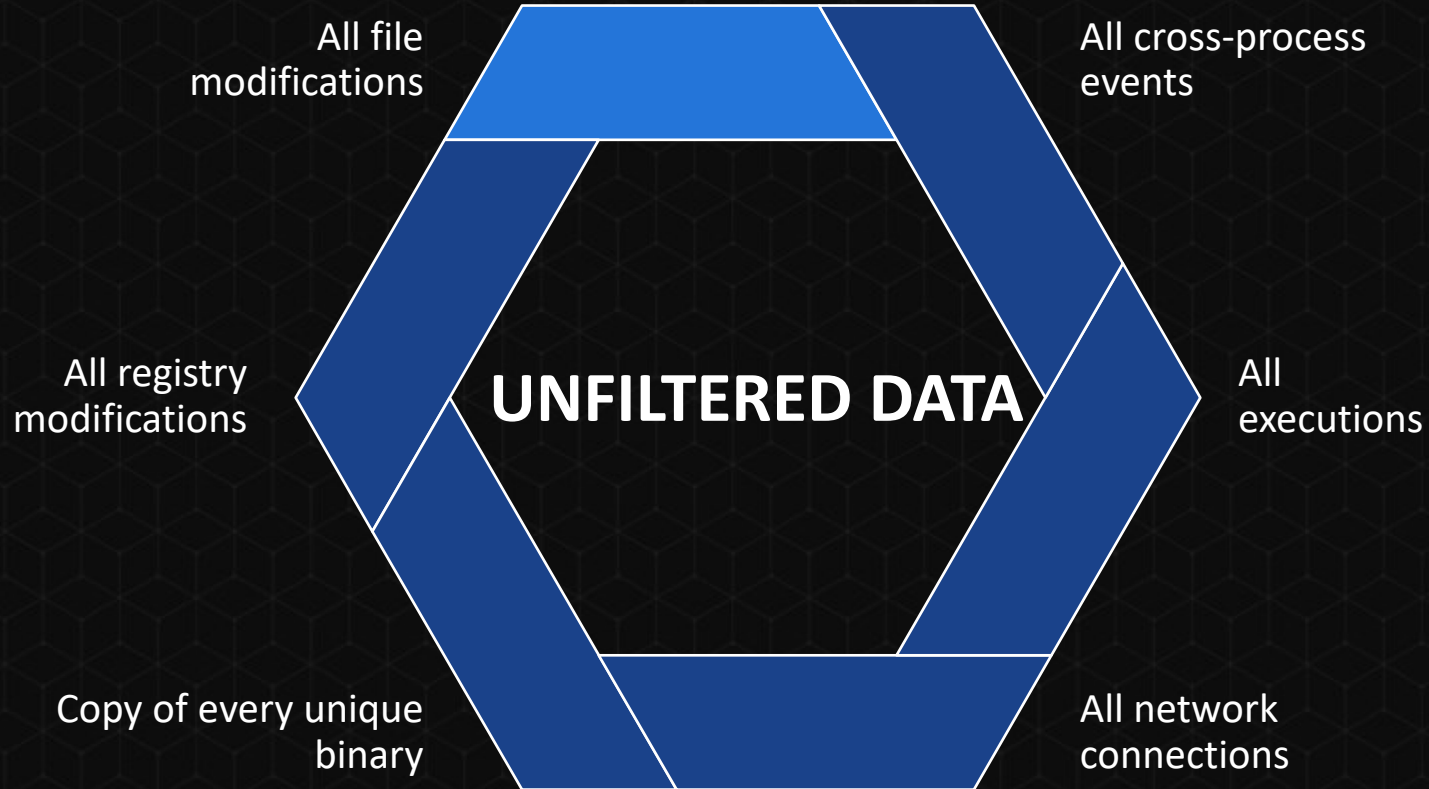
UNFILTERED DATA

---

# How the PSC Detects



# Step 1: Unfiltered Data Collection



**No blind spots**

**Continuous recording**

**Proprietary data shaping**

## Step 2: Tagging TTPs

### TACTICS TECHNIQUES, AND PROCEDURES (TTPs)

Individual patterns of  
behavior often found with  
malicious activity

Merchant ID  
& reputation

Purchase in a strange  
place

Luxury items

Small purchase  
followed by large  
purchase

**Monthly Mortgage Statement**

Customer Service: (800) 282-5284  
Loan Number: 5174292  
Regular mail: P.O. Box 14542, Des Moines, IA 50326  
Overnight mail: 1 Hour Campus, 82501-018, Des Moines, IA 50326

**For Informational Purposes**

Statement date: 05/21/01  
Home loan facts: Principal balance as of 05/21/01: \$146,127.97  
Interest rate: 7.500%  
Interest paid - year to date: \$1,605.51  
Future balance - year to date: \$146,127.97

**Next Payment 06/01/01**

Payment	\$1,405.51
Other payment(s)	\$10,806.12
Late charges	\$544.07
Other charges	\$25.00
<b>Total</b>	<b>\$18,840.70</b>

**ACCOUNT STATEMENT**

Payment	\$1,405.51
Other payment(s)	\$10,806.12
Late charges	\$544.07
Other charges	\$25.00
<b>Total payment</b>	<b>\$18,840.70</b>
Adjusted Principal	\$
Adjusted Interest	\$
Other	\$
<b>Total Enclosed</b>	<b>\$</b>

685 Loan Number: 5174292  
Customer Service: (800) 282-5284  
WELLS FARGO HOME MORTGAGE, INC.  
PO BOX 14542  
DES MOINES IA 50326-2842

751742920140551014617397



# Step 8: Detection Through Data Science

PERSISTENCE

Confidence: Low

PERSISTENCE

UNKNOWN\_APP

Confidence: Medium

READ\_USER\_DATA

PERSISTENCE

UNKNOWN\_APP

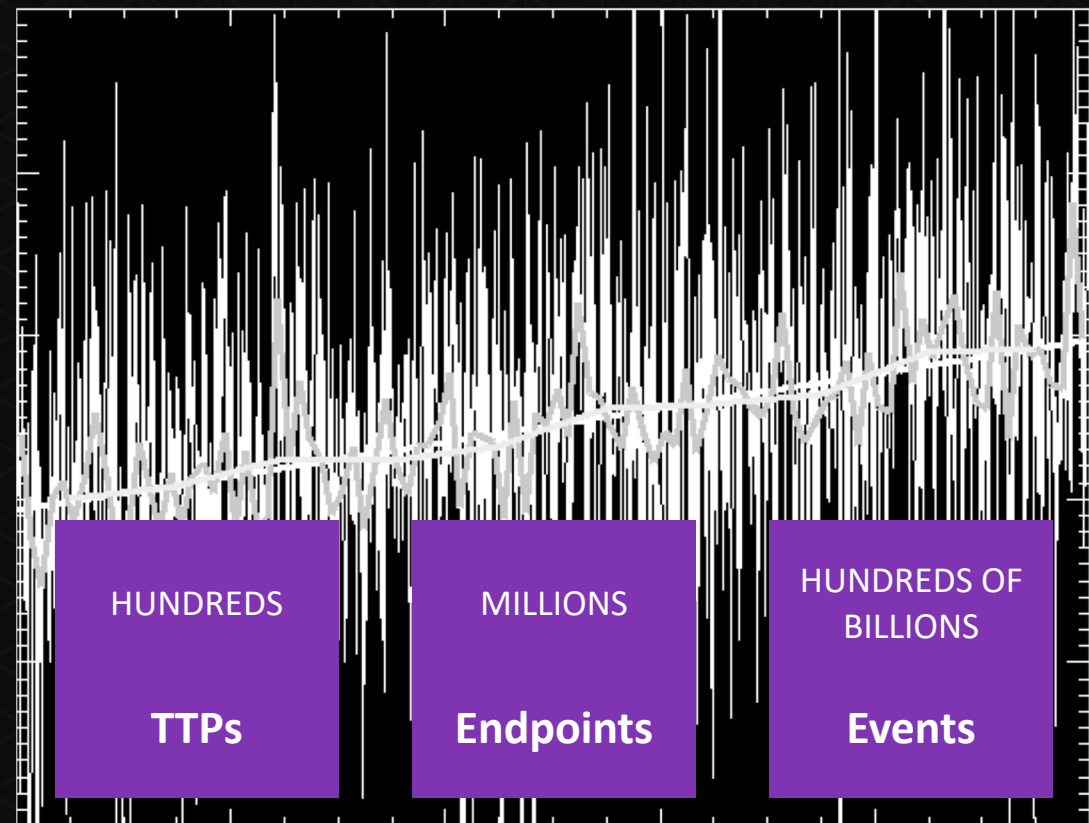
READ\_USER\_DATA

Confidence: High

CODE\_INJECTION

HARVEST\_PASSWORDS

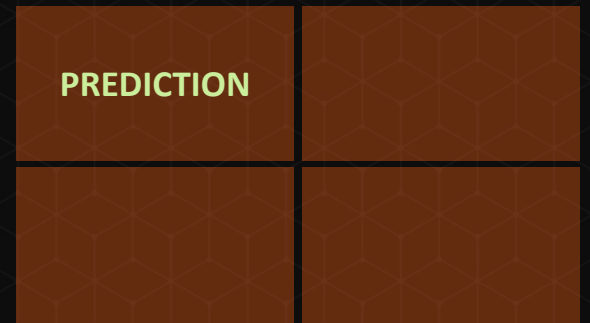
## Probabilistic Modeling + Temporal Analysis



DATA SCIENCE

---

# How the PSC Learns

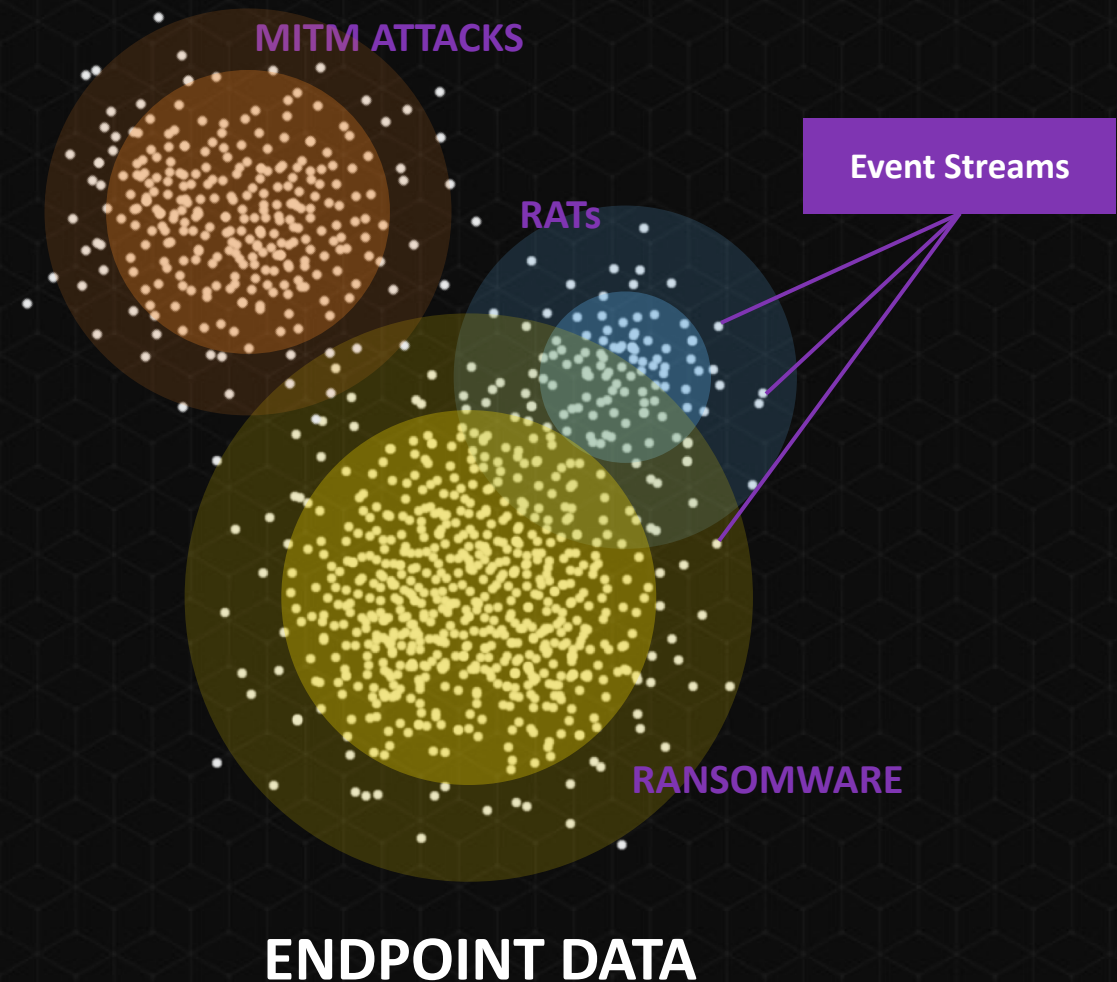


# TTP PATTERNS LET US VISUALIZE ATTACK FAMILIES

Event streams (sequences) get associated with TTPs.

Similar attacks have similar groupings of TTPs.

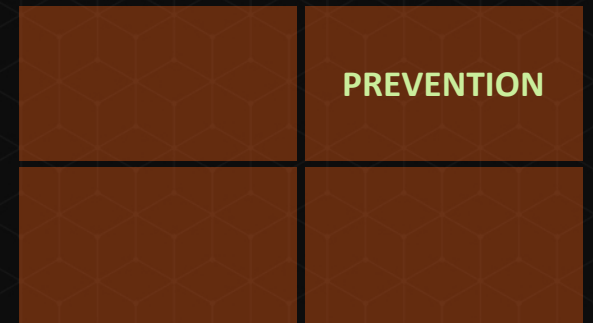
These patterns allow us to identify families of attacks.



## PREDICTIVE MODELS

---

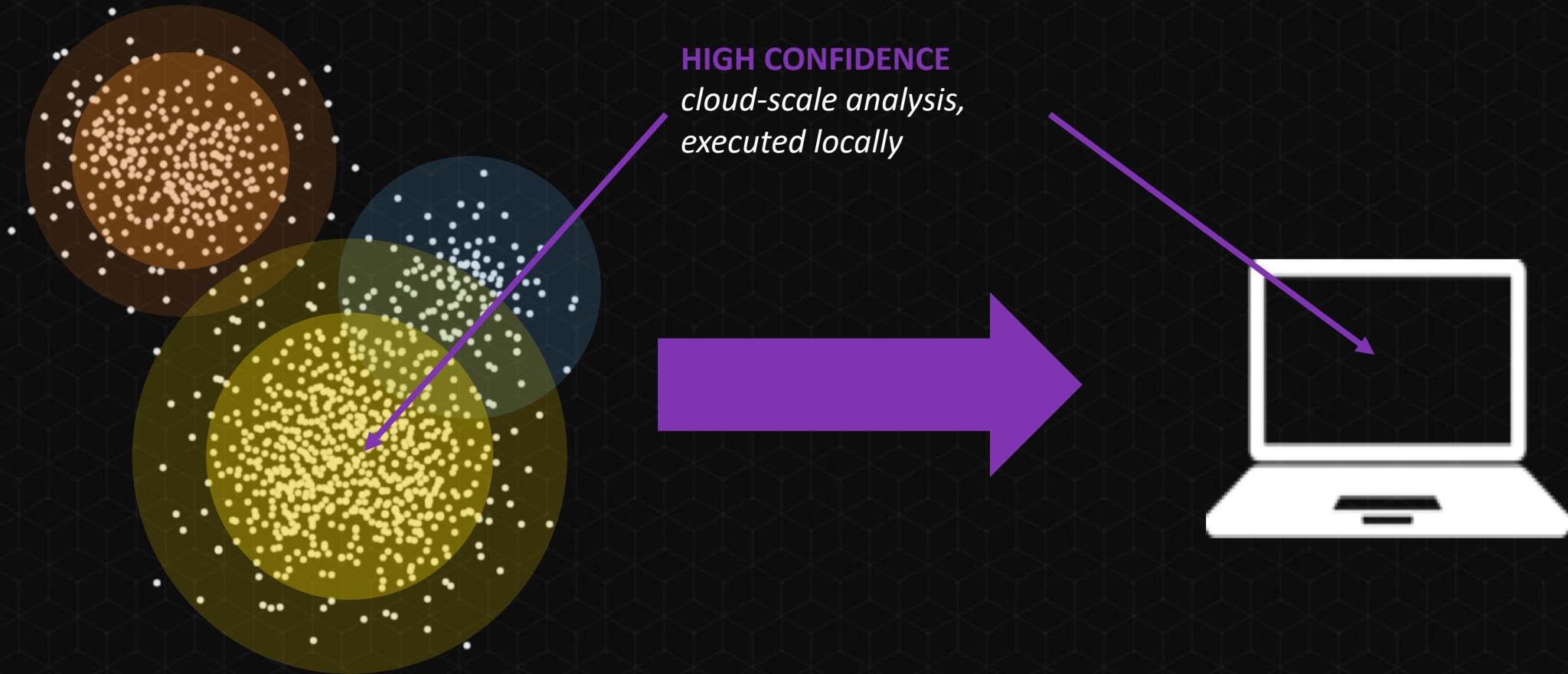
# How the PSC Prevents



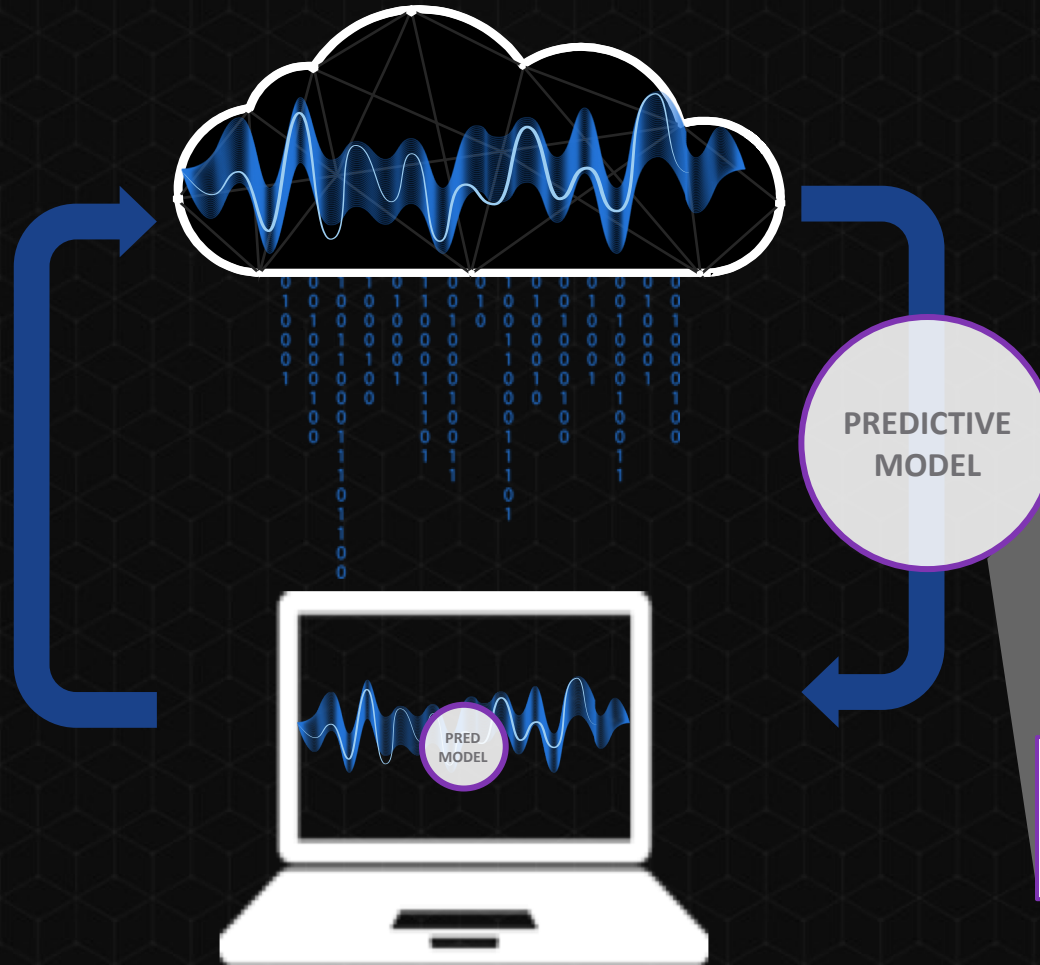


# PREVENTING HIGH-CONFIDENCE BEHAVIORS

---



# LOCAL PREDICTIVE MODEL



## PREDICTIVE MODEL

- High-confidence detection model
- Generated from cloud analysis
- Matches behaviors (TTPs) locally
- Customizable

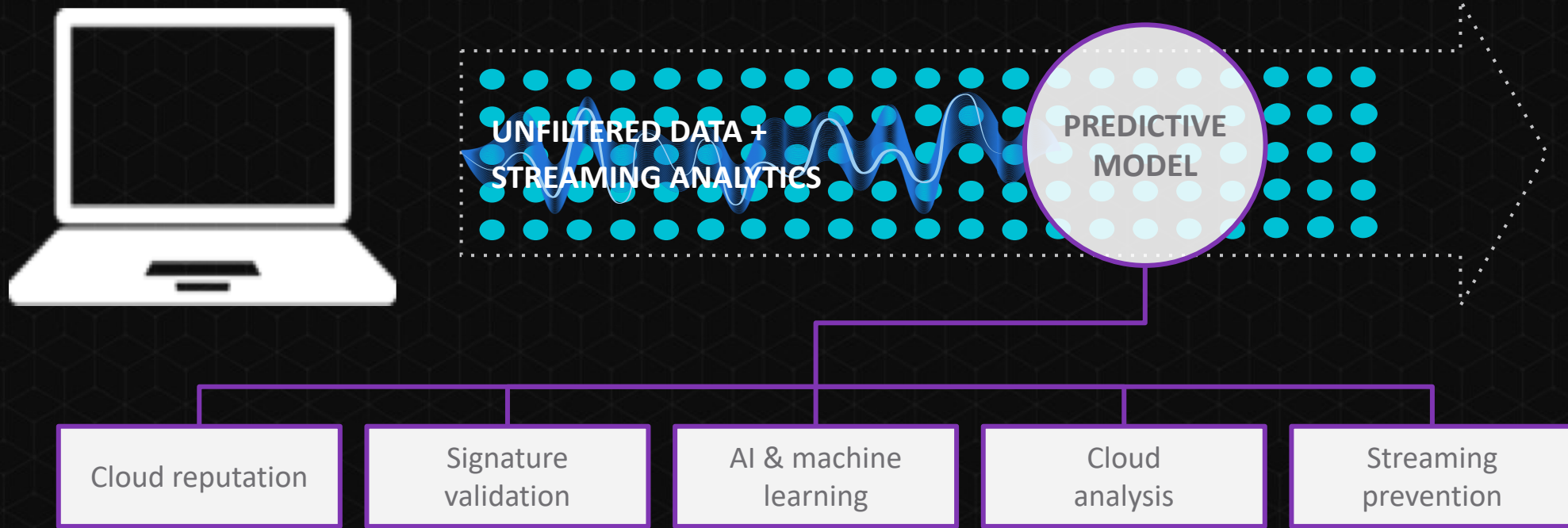
Unknown application or process



Scrapes memory of another process

Performs ransomware-like behavior

# HIGHER-CONFIDENCE PREVENTION, EARLIER



Additional protective layers plug into the streaming analytics engine to identify and block known and unknown malware.



Thank You!