VMware Carbon Black

Andrea Argentin – Lead Sales Engineer - Security Business Unit

vmware®

WHY CLOUD IS THE FUTURE OF SECURITY

BETTER PROTECTION

BIG DATA + ANALYTICS

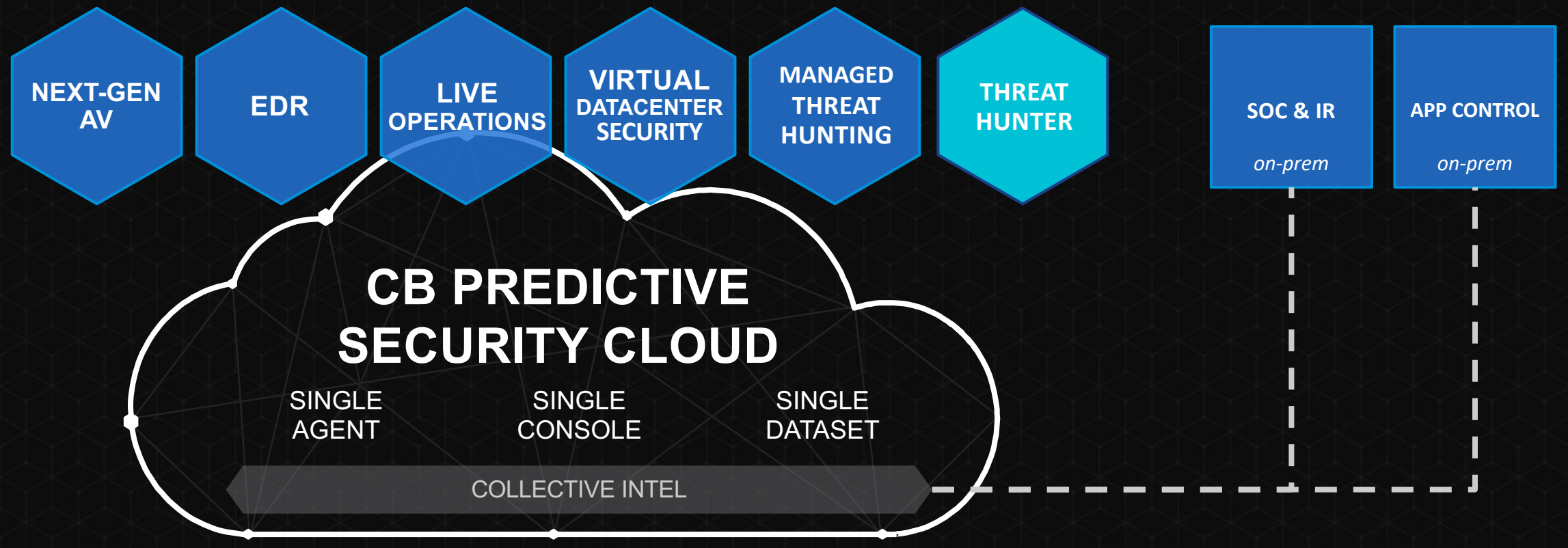
- Threat prediction & prevention
- Global threat monitoring
- Real-time intelligence

SIMPLIFIED OPERATIONS

MANAGEMENT MODEL

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

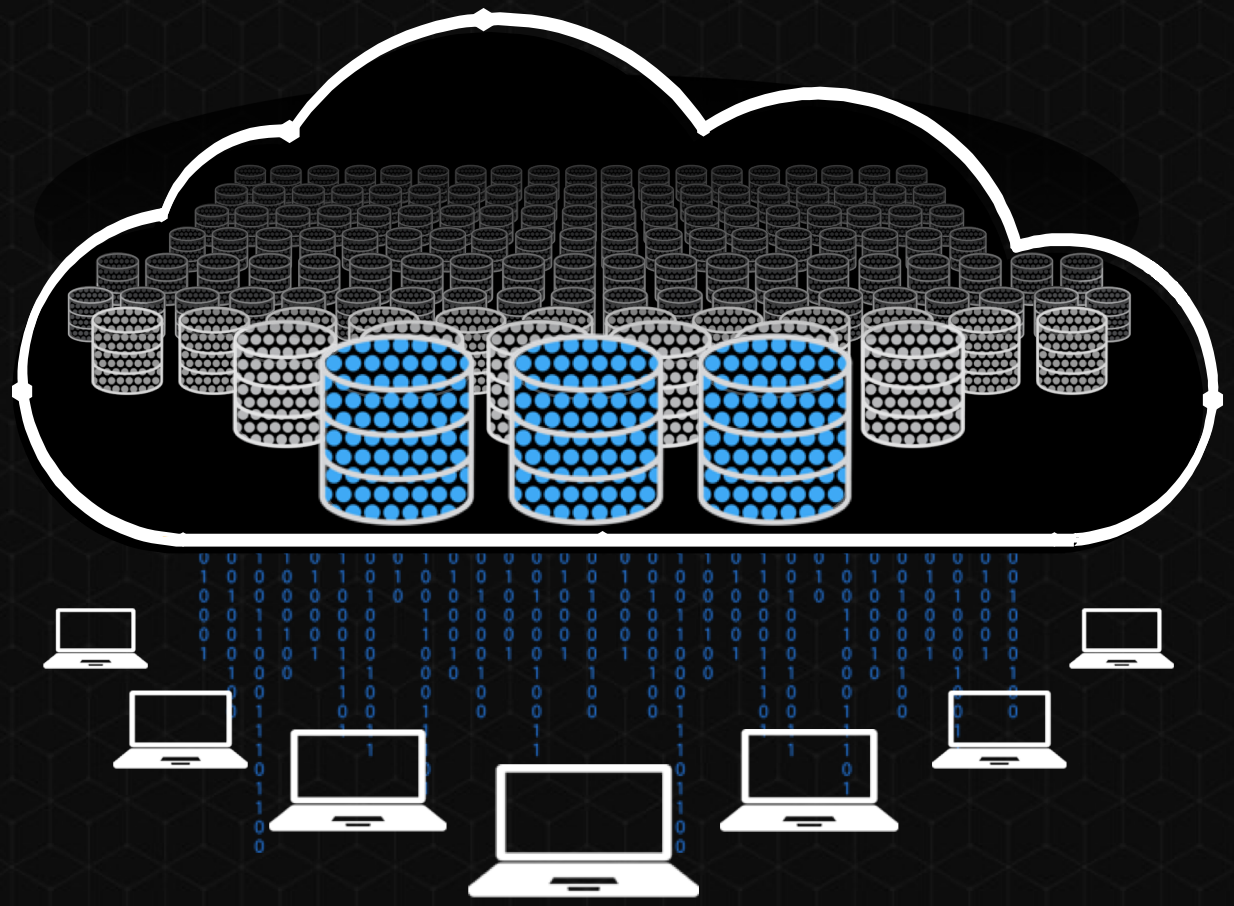
Cb PREDICTIVE SECURITY CLOUD



Carbon Black's Differentiated Approach

Carbon Black.

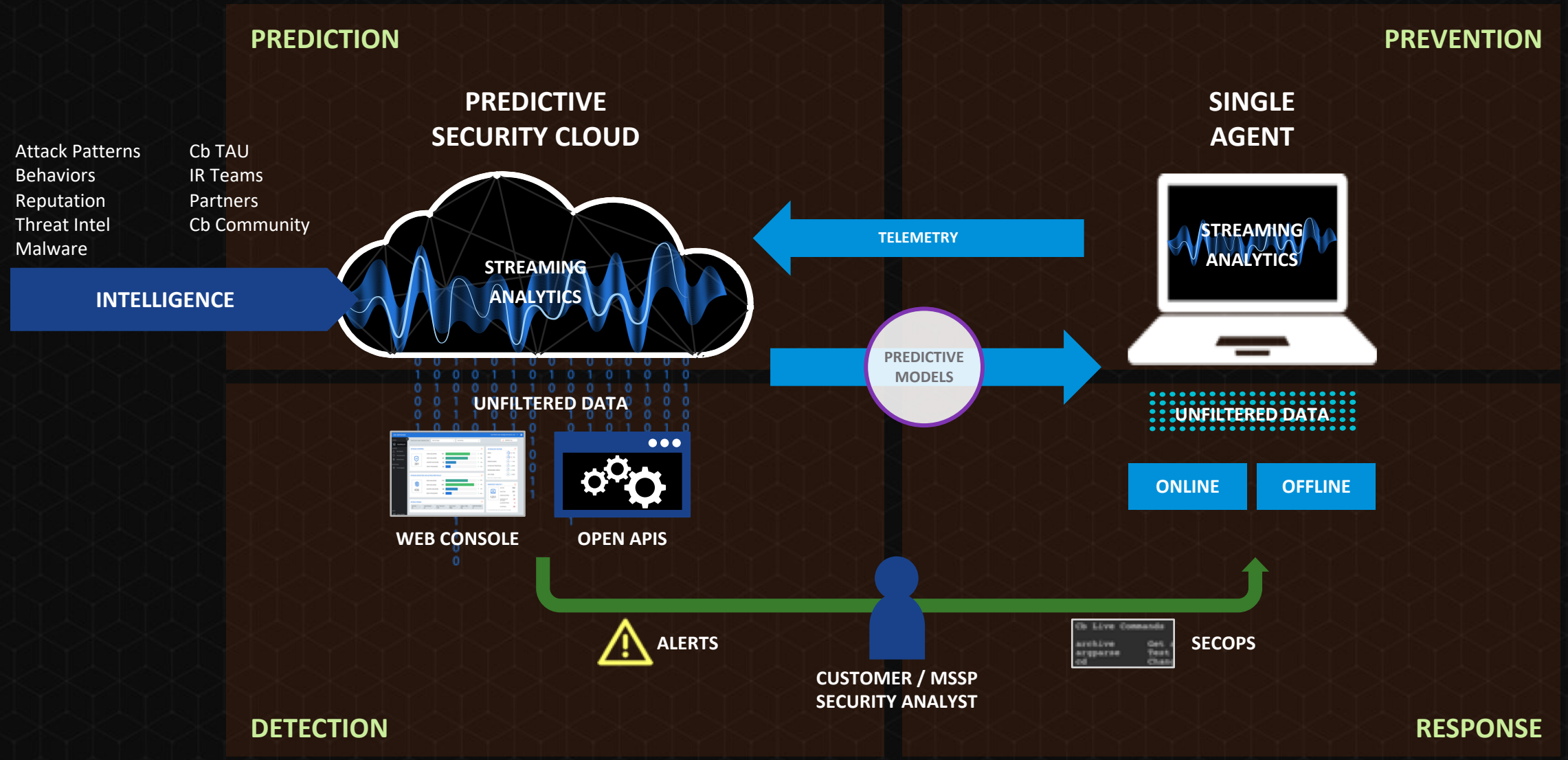
THE POWER OF THE PREDICTIVE SECURITY CLOUD



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

vmware

PSC ARCHITECTURE



vmware

Agenda

1 How the PSC Detects

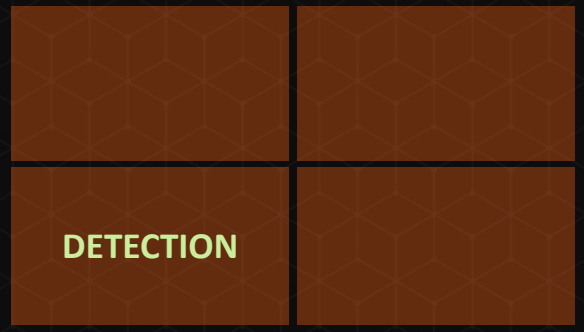
2 How the PSC Learns

3 How the PSC Prevents

Carbon Black.

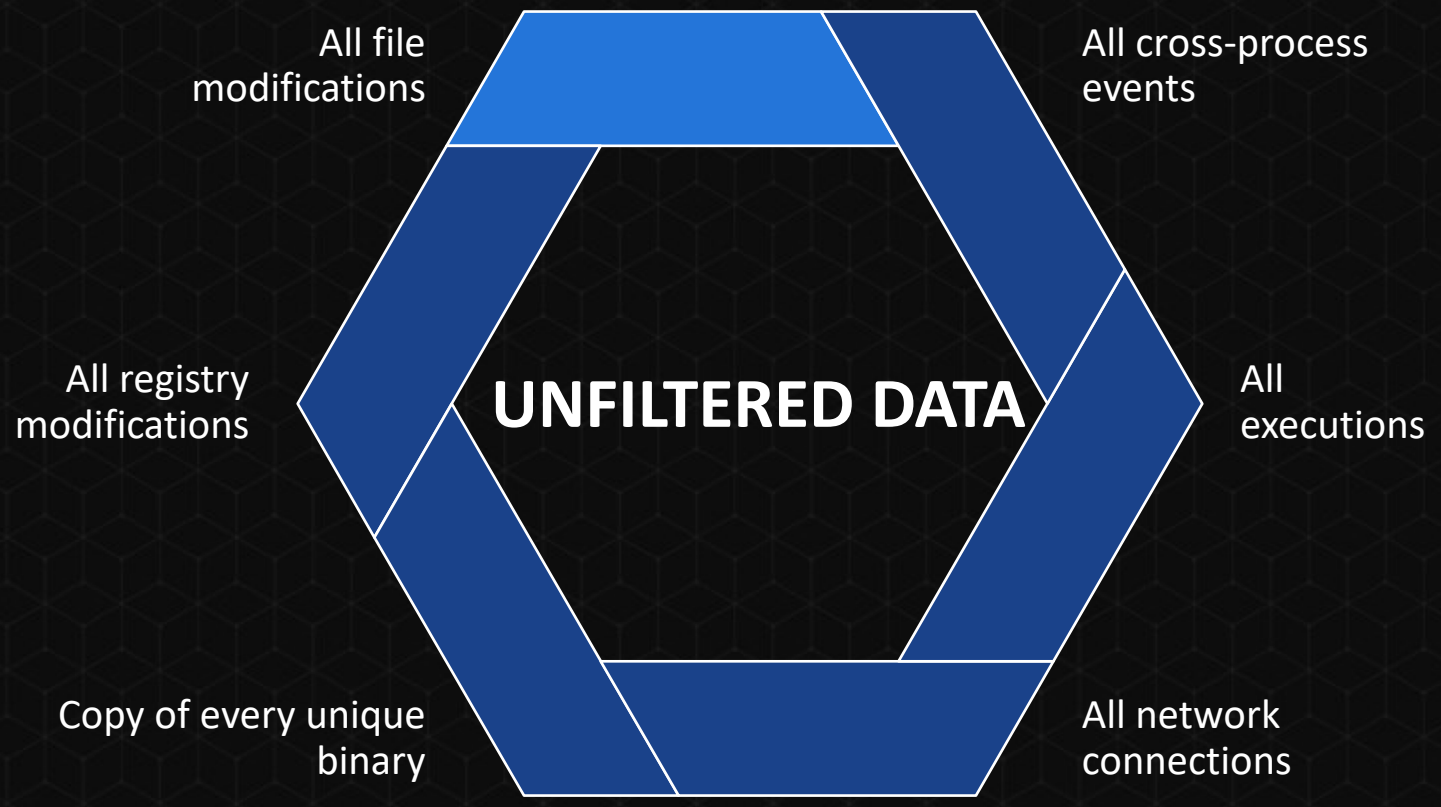
UNFILTERED DATA

How the PSC Detects



Carbon Black.

Step 1: Unfiltered Data Collection



No blind spots

Continuous recording

Proprietary data shaping

Step 2: Tagging TTPs

TACTICS TECHNIQUES, AND PROCEDURES (TTPs)

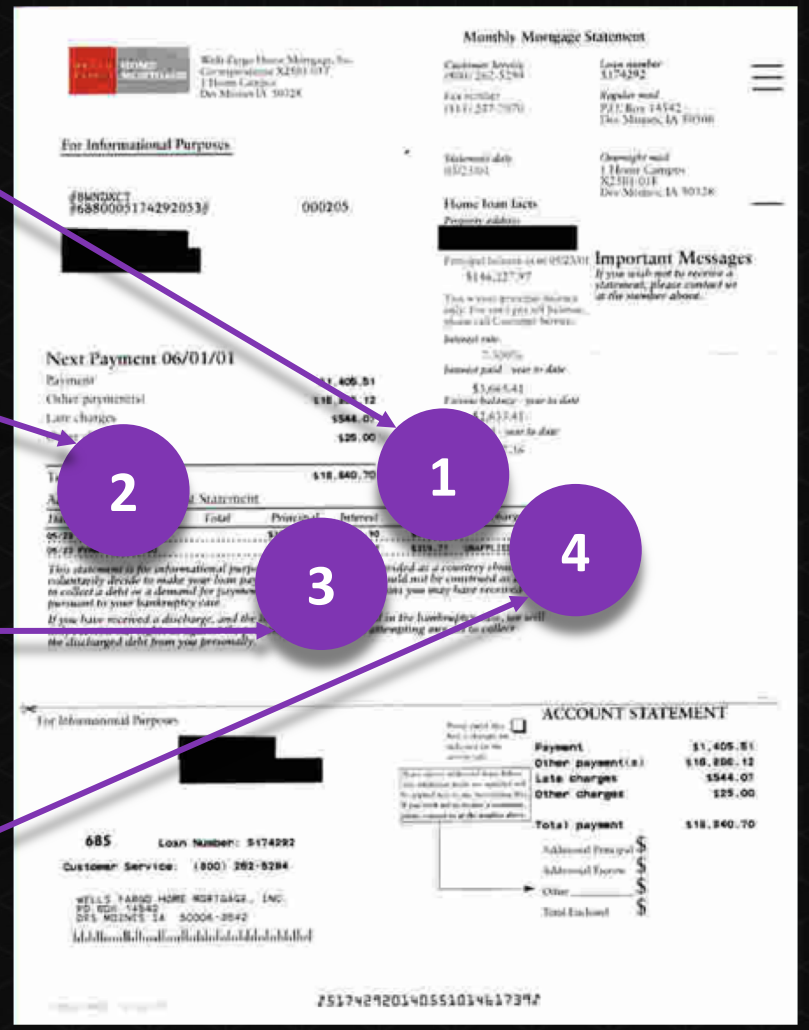
Individual patterns of behavior often found with malicious activity

Merchant ID & reputation

Purchase in a strange place

Luxury items

Small purchase followed by large purchase



Step 3: Detection Through Data Science

PERSISTENCE

Confidence: Low

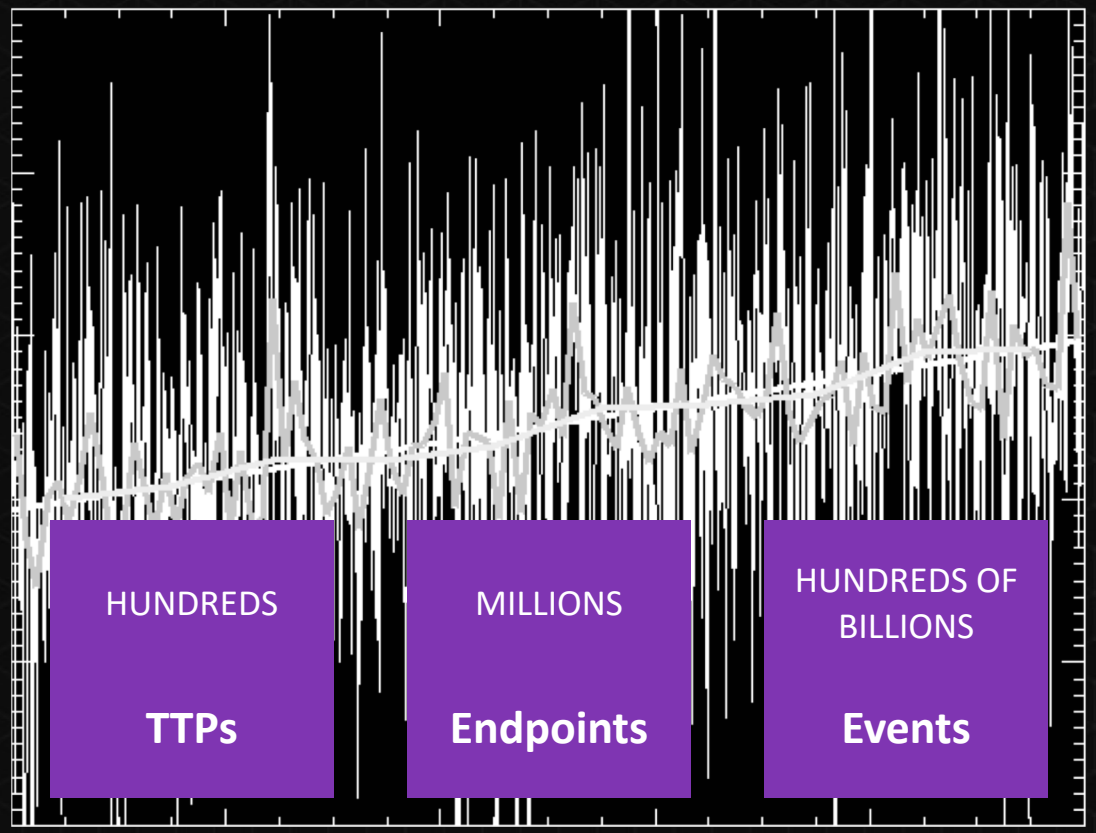
PERSISTENCE
UNKNOWN_APP
READ_USER_DATA

Confidence: Medium

PERSISTENCE
UNKNOWN_APP
READ_USER_DATA
CODE_INJECTION
HARVEST_PASSWORDS

Confidence: High

Probabilistic Modeling + Temporal Analysis



DATA SCIENCE

How the PSC Learns

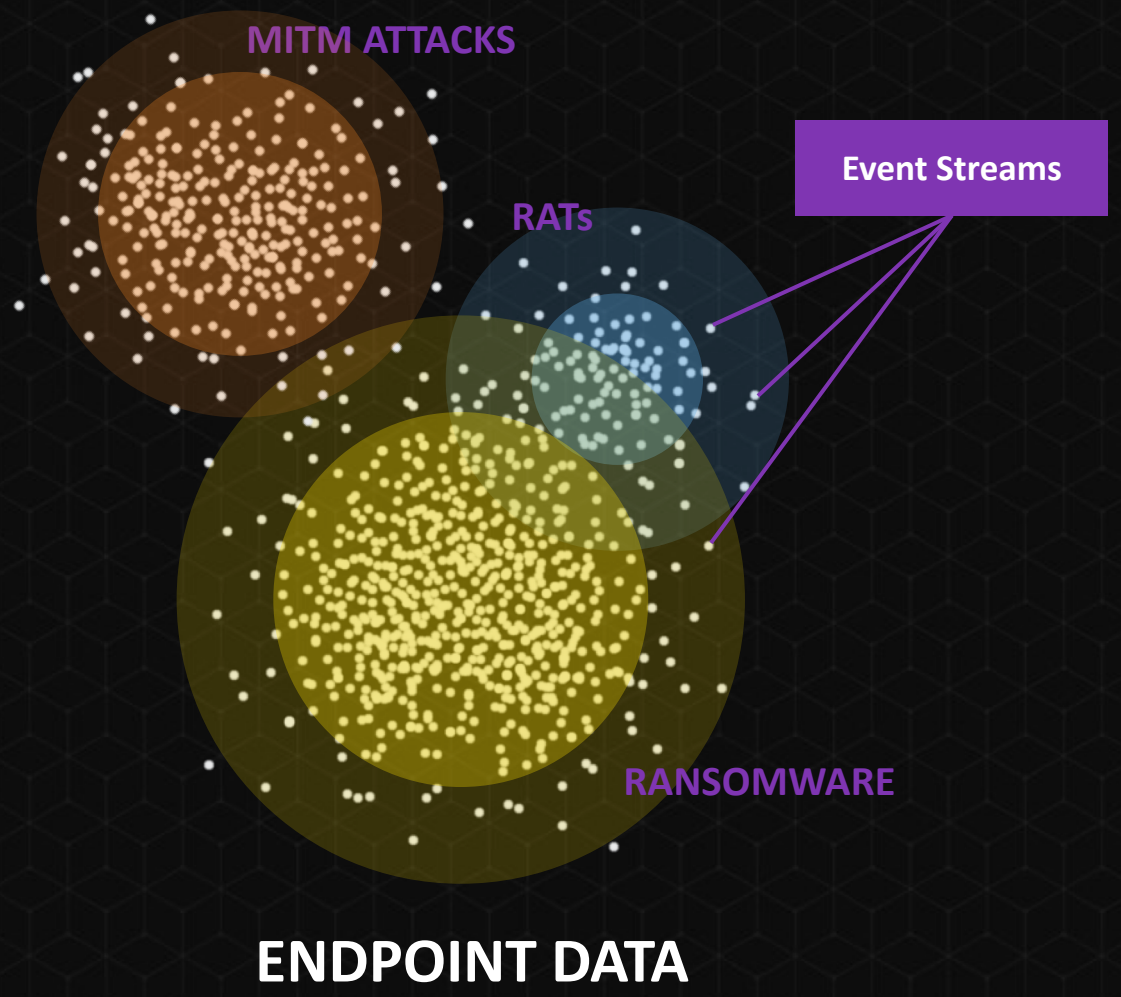
Carbon Black.

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.

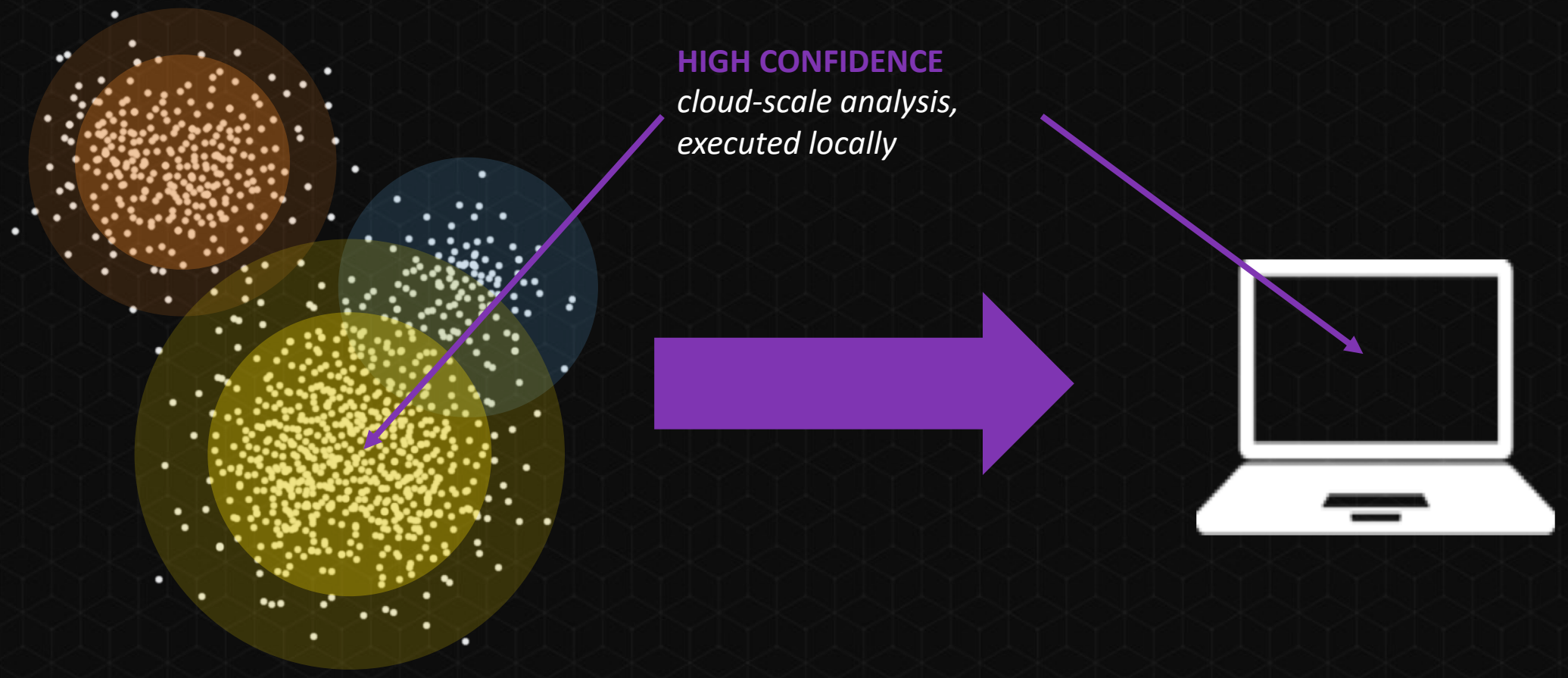


PREDICTIVE MODELS

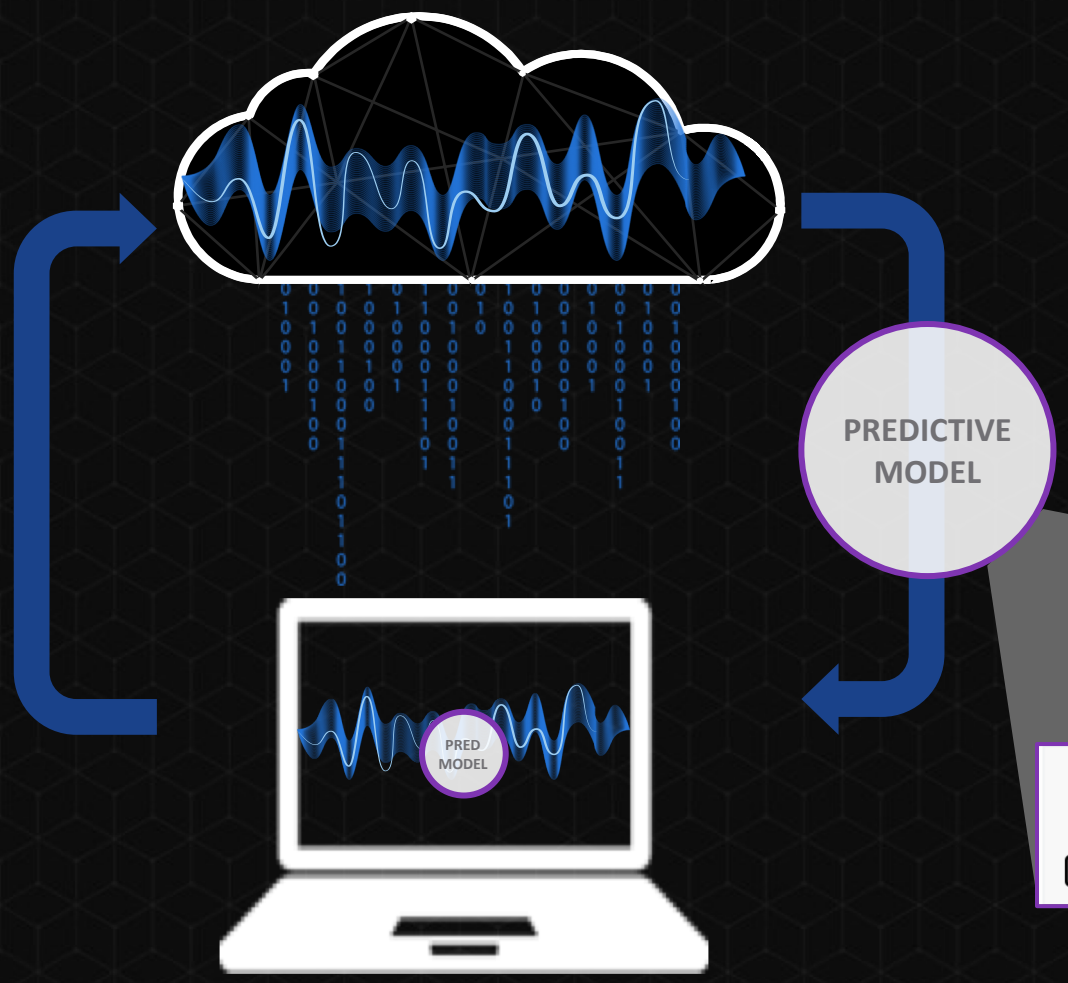
How the PSC Prevents

Carbon Black.

PREVENTING HIGH-CONFIDENCE BEHAVIORS



LOCAL PREDICTIVE MODEL



PREDICTIVE MODEL

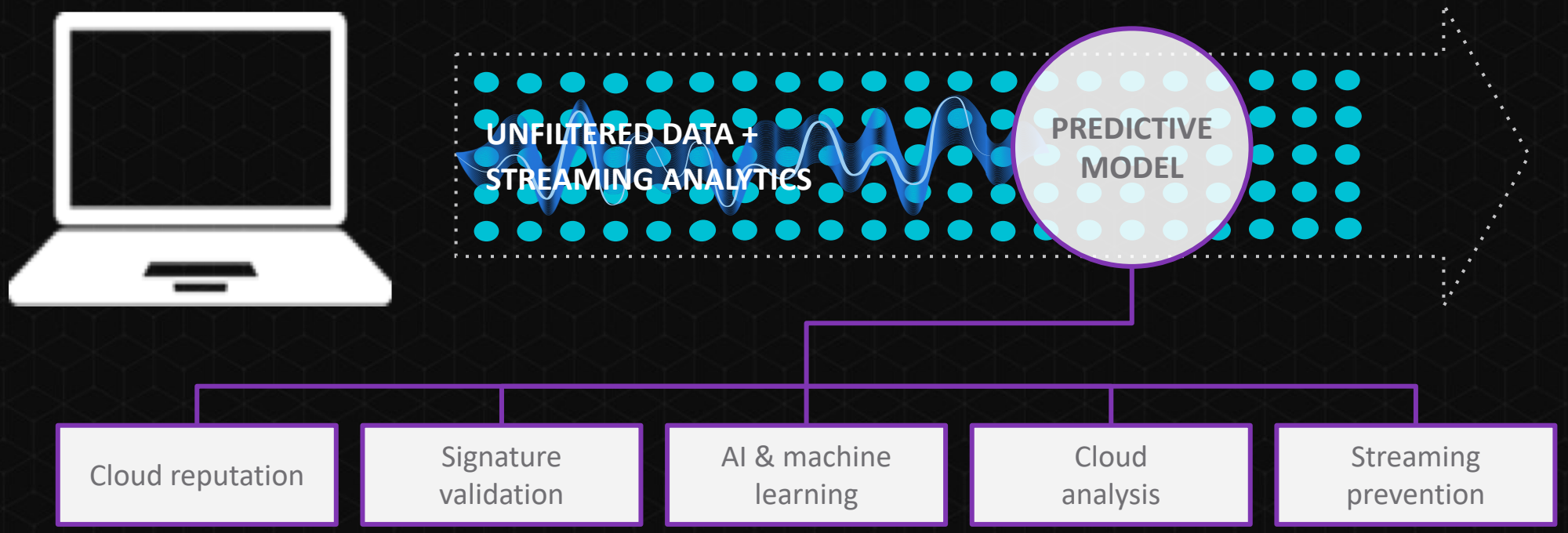
- High-confidence detection model
- Generated from cloud analysis
- Matches behaviors (TTPs) locally
- Customizable

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!

vmware®