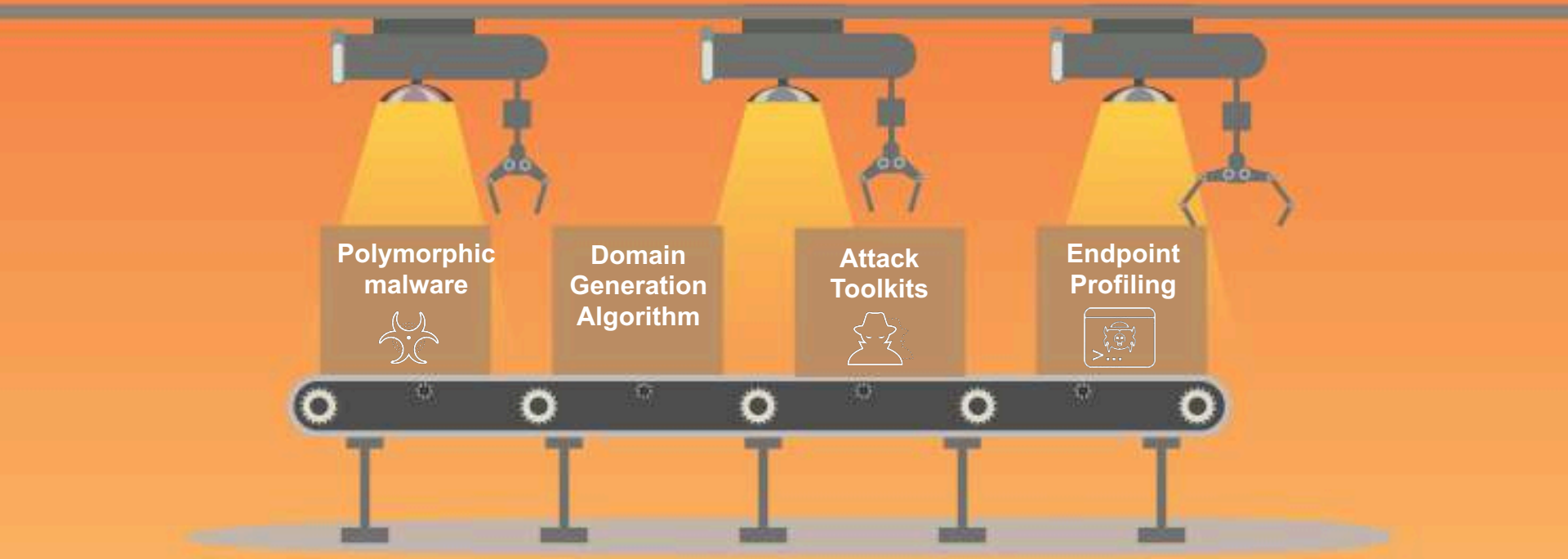
*GUANCHAO CYBER FORUM*
*Beijing, China*
*21 August 2019*

# Artificial Intelligence is Critical for Effective Cybersecurity

*Major General (Retired) John Davis*
*Federal Chief Security Officer*
*Palo Alto Networks*

# CYBER THREAT ACTORS USE AUTOMATION FOR ATTACKS & EVASION



# CHALLENGES OF A DYNAMIC CYBER THREAT LANDSCAPE

## No Known Bad

Once attackers have infiltrated the organization, they use benign tools

## Attackers Aim to Bypass Security

With polymorphism, DGA, 2FA bypass

## Static Rules Generate Many False Positives

As they are not automatically derived from the data, static rules are error prone

## Static Rules Are Labor Intensive

Static rules require constant adapting and maintenance

# DEFENDERS NEED ARTIFICIAL INTELLIGENCE TO OUTPACE ATTACKERS

## Stop Attacks Faster

Automatically analyze unknown files and domains to block threats

## Detect Stealthy Threats

Uncover threats that would be virtually impossible to find manually

## Reduce Manual Errors

Avoid overlooking risks and alert fatigue with consistent analysis

## Simplify Operations

Eliminate repetitive tasks and make your life easier

# ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

# MACHINE LEARNING BACKGROUND

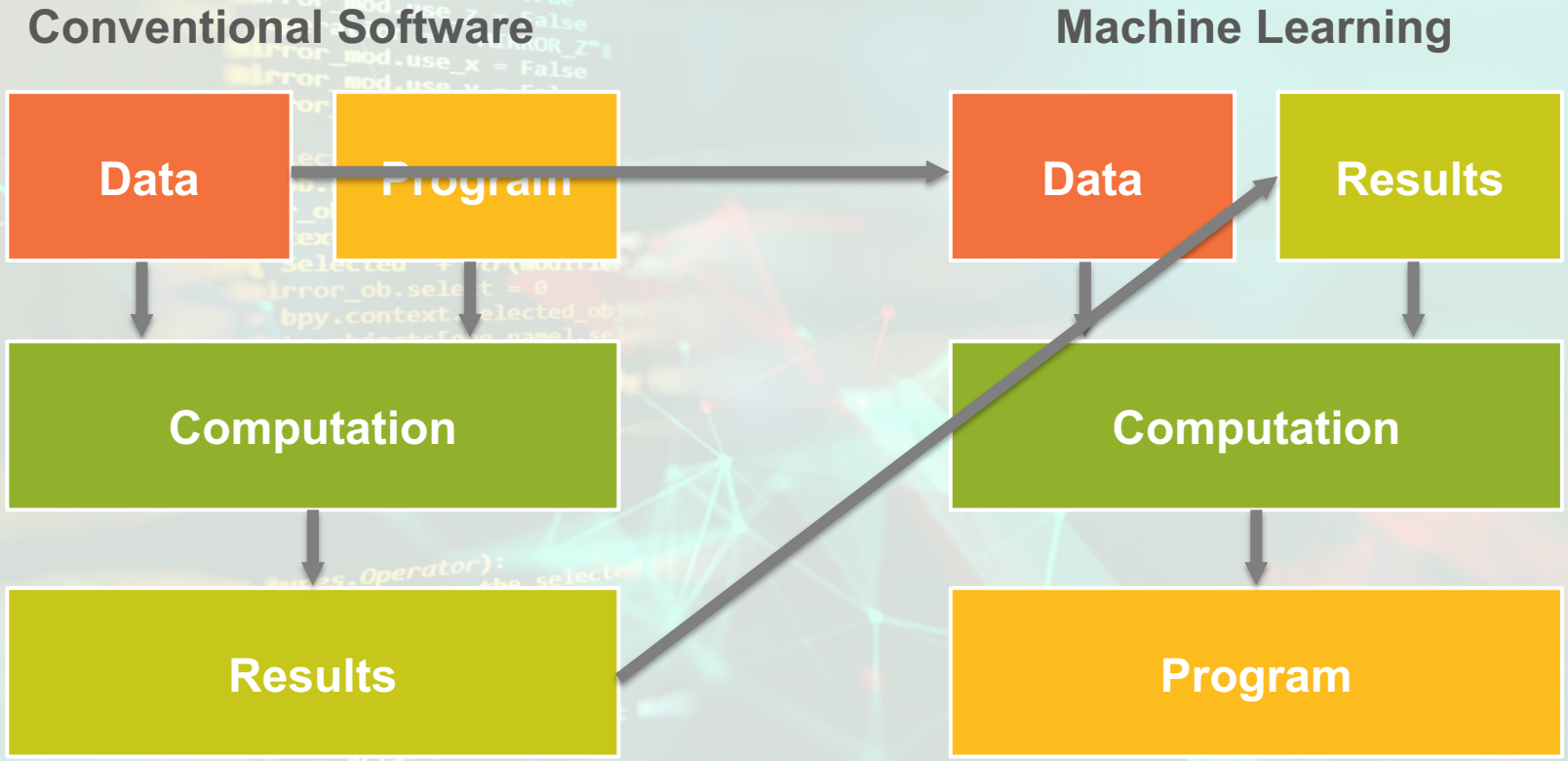
# MACHINE LEARNING BACKGROUND

## Conventional Software


## Machine Learning

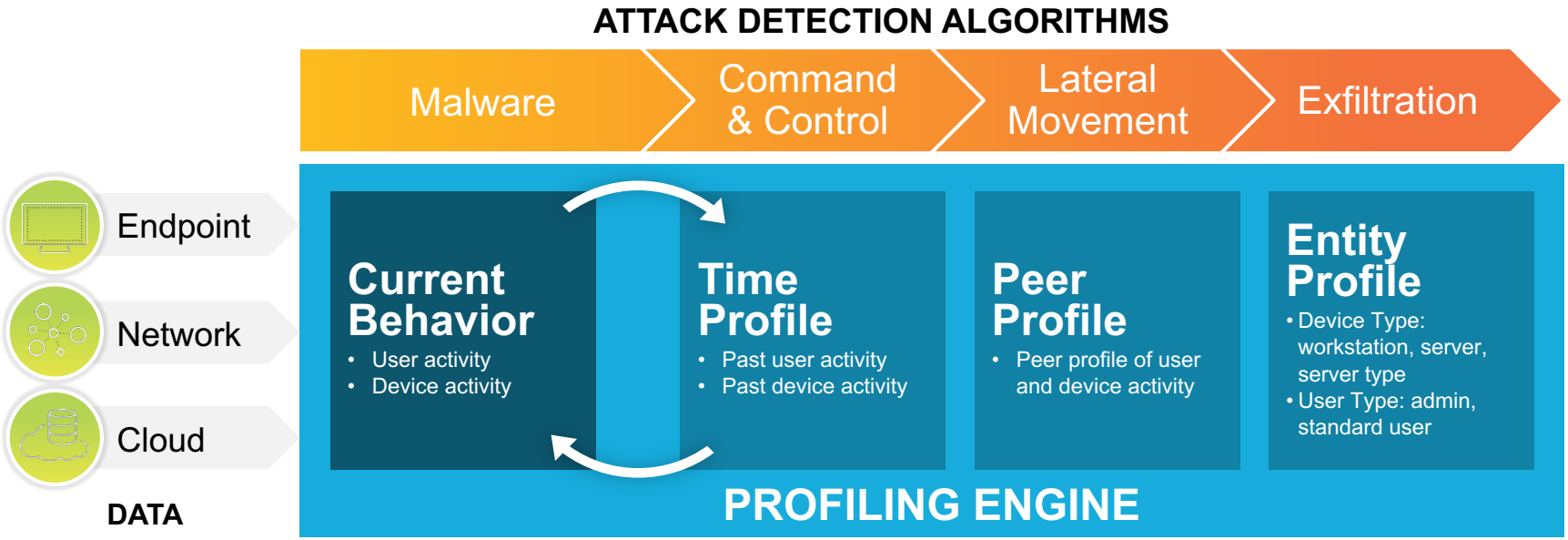
 

# MACHINE LEARNING BACKGROUND



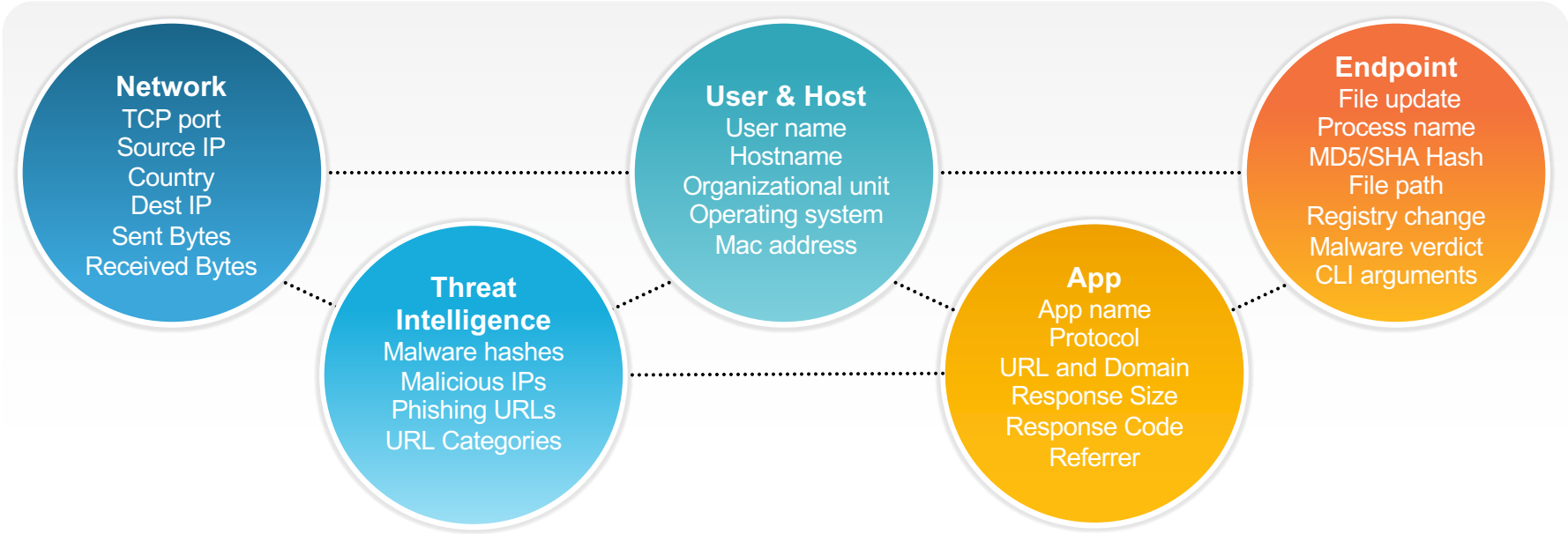

 

# MACHINE LEARNING AUTOMATES ATTACK DETECTION




Profile behavior & detect anomalies indicative of an attack

# COMPREHENSIVE, CORRELATED DATA POWERS MACHINE LEARNING




Collect rich data for behavioral analytics & AI

Automatically correlate data to gain context for investigations

# AI and ML provide an advantage to the *defense* …and make it harder for the *offense* to succeed!

# *THANK YOU*