ARTIFICIAL INTELLIGENCE. REAL THREAT PREVENTION.

Jan Tietze, Senior SE DACH at Cylance

WHO?
WHY?
WHAT?
HOW?

2012

Made in Irvine, California

Stuart McClure
CEO and Founder

Ryan Permeh
Founder and Chief Scientist

2014

Next-Gen AV "CylancePROTECT"

CYLANCE

70+

850

130M

2x

CYLANCE

>4000

>14M

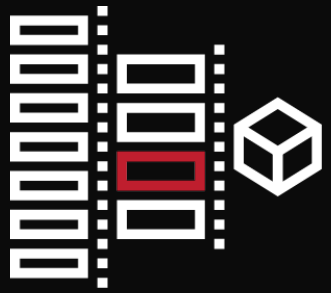
CYLANCE

WHO?
WHY?
WHAT?
HOW?

The definition of insanity is trying the same thing over and over again and expecting different results.

Albert Einstein

THE CASE FOR AI IN CYBERSECURITY



Threat Actors	AV Industry Analyst	Cylance AI Model
Infect your devices	**Creates malware definitions**	**Protect device from infection**
~1/10th of a second to mutate	~2h per AV definition	~30 ms to device for a file
~1-2M files/day	~5 AV definitions/day	Infinite – decision on endpoint
Work for free + make you pay	€ € €	€
Scale increases every day	Diffcult to scale	No scalability limit

WHY?
WHO?
WHAT?
HOW?

CYLANCE APPROACH TO TOTAL ENDPOINT SECURITY

TARGETED
THREAT
HUNTING

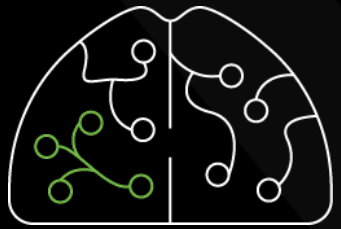
ROOT
CAUSE
ANALYSIS

IMMEDIATE
INCIDENT
RESPONSE

CylancePROTECT

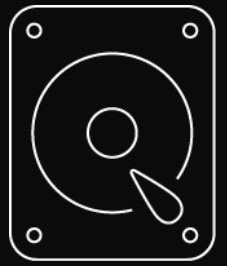
AI-DRIVEN ADVANCED THREAT PREVENTION

CylancePROTECT®



EFFECTIVENESS

SIMPLICITY



PERFORMANCE

CYLANCE

EFFECTIVENESS

CylancePROTECT

No patient zero

True zero-day malware prevention

Needs no prior knowledge of threat

Offline + online protection

Protects against exploits, payloads, memory attacks, file-less attacks

Additional hardening controls:

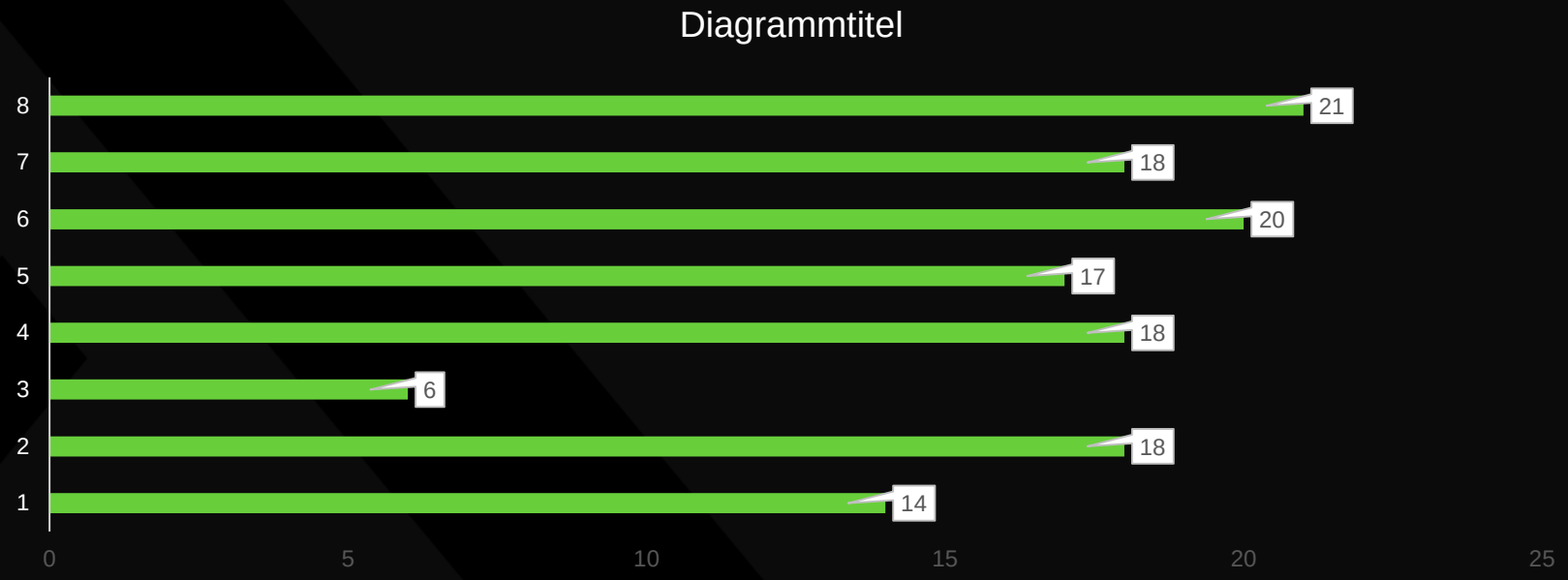
- USB Device Control
- Application Control

Microsoft Mac redhat. CentOS

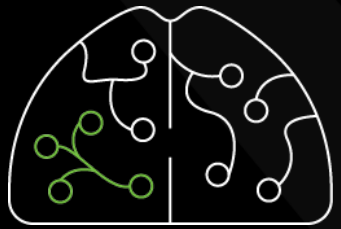
NSS LABS AV-TEST The Independent IT-Security Institute PCI DSS COMPLIANT

TEMPORAL PREDICTIVE ADVANTAGE

“Temporal Predictive Advantage”, *time in months* that CylancePROTECT was able to detect & block a new threat before it was first seen “in the wild” – without any updates or special configuration. Examples include:

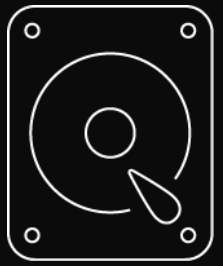


CylancePROTECT®



EFFECTIVENESS

SIMPLICITY



PERFORMANCE

CYLANCE

SIMPLICITY

ZERO

signatures and daily updates means easier administration

Protection is independent of connectivity or large, frequent updates

ZERO

on premise infrastructure reduces complexity

Low operating cost, no resources, no migrations

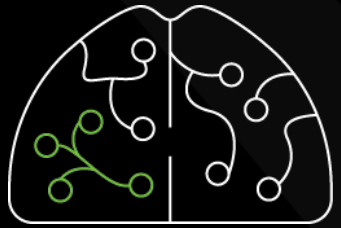
On-Prem Management is available if you need it (e.g. military, defence, finance, industrial control systems) and is 100% disconnected

EASY

policy management is something the team will love

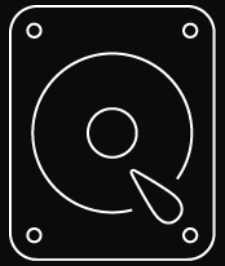
No need to manage 100s of policies, scanning exclusions etc.

CylancePROTECT®



EFFECTIVENESS

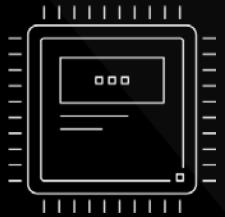
SIMPLICITY



PERFORMANCE

CYLANCE

PERFORMANCE



Measurable
CPU Reduction
(~1% of CPU average)

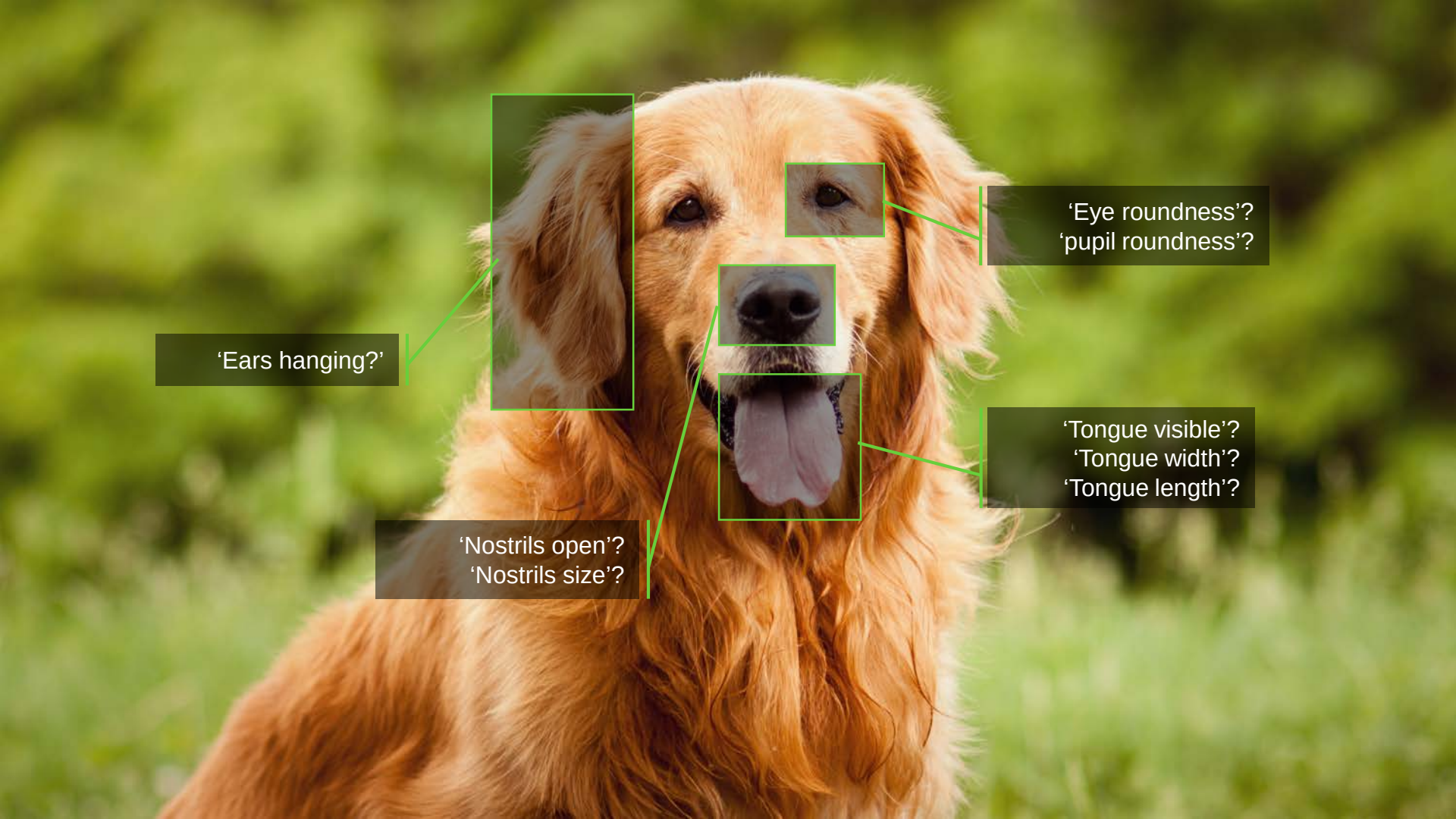
Measurable
Memory Reduction
(40-200 MB of RAM)

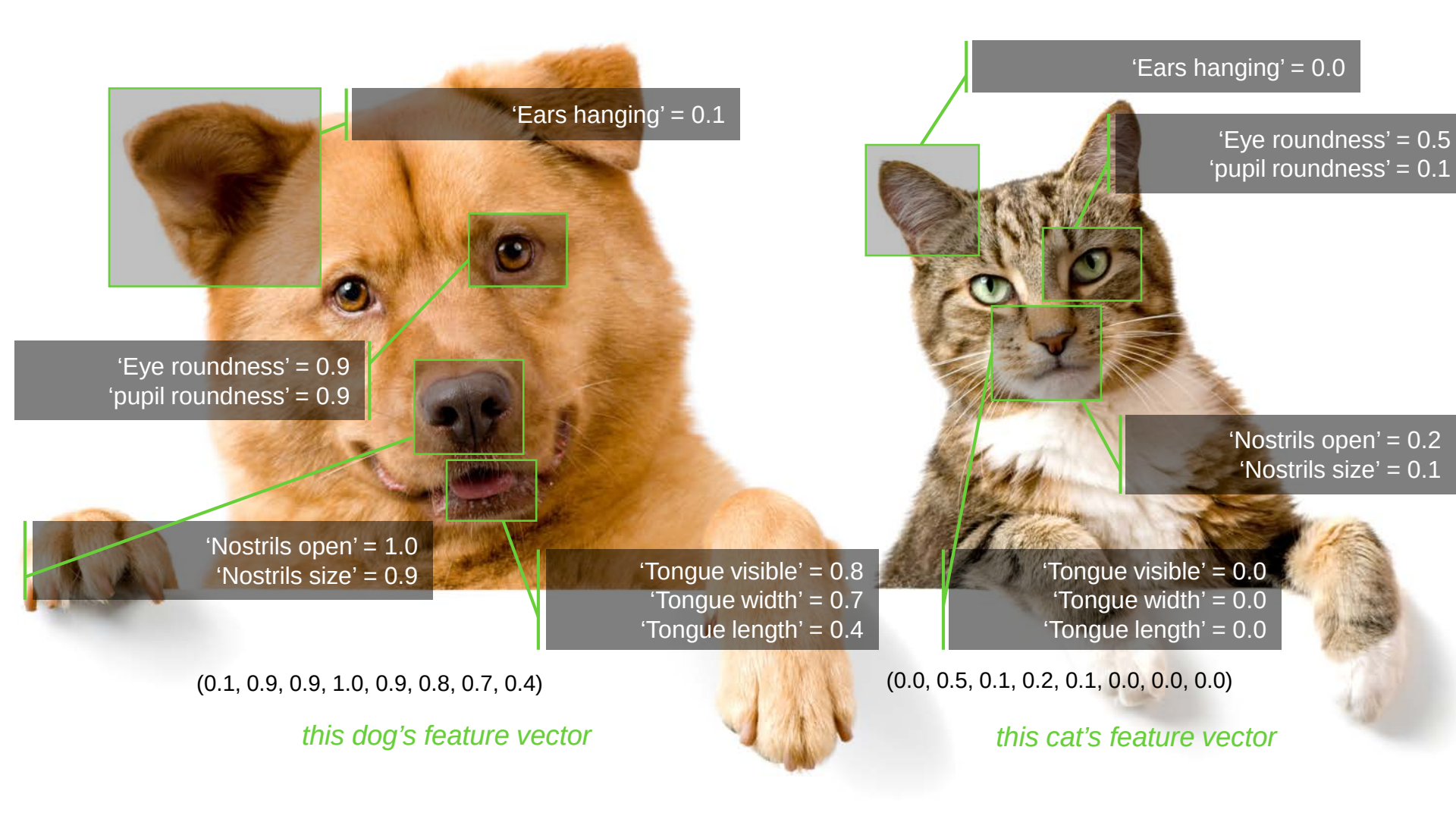
Measurable
Disk I/O Improvement
(~1/40th of I/O operations)

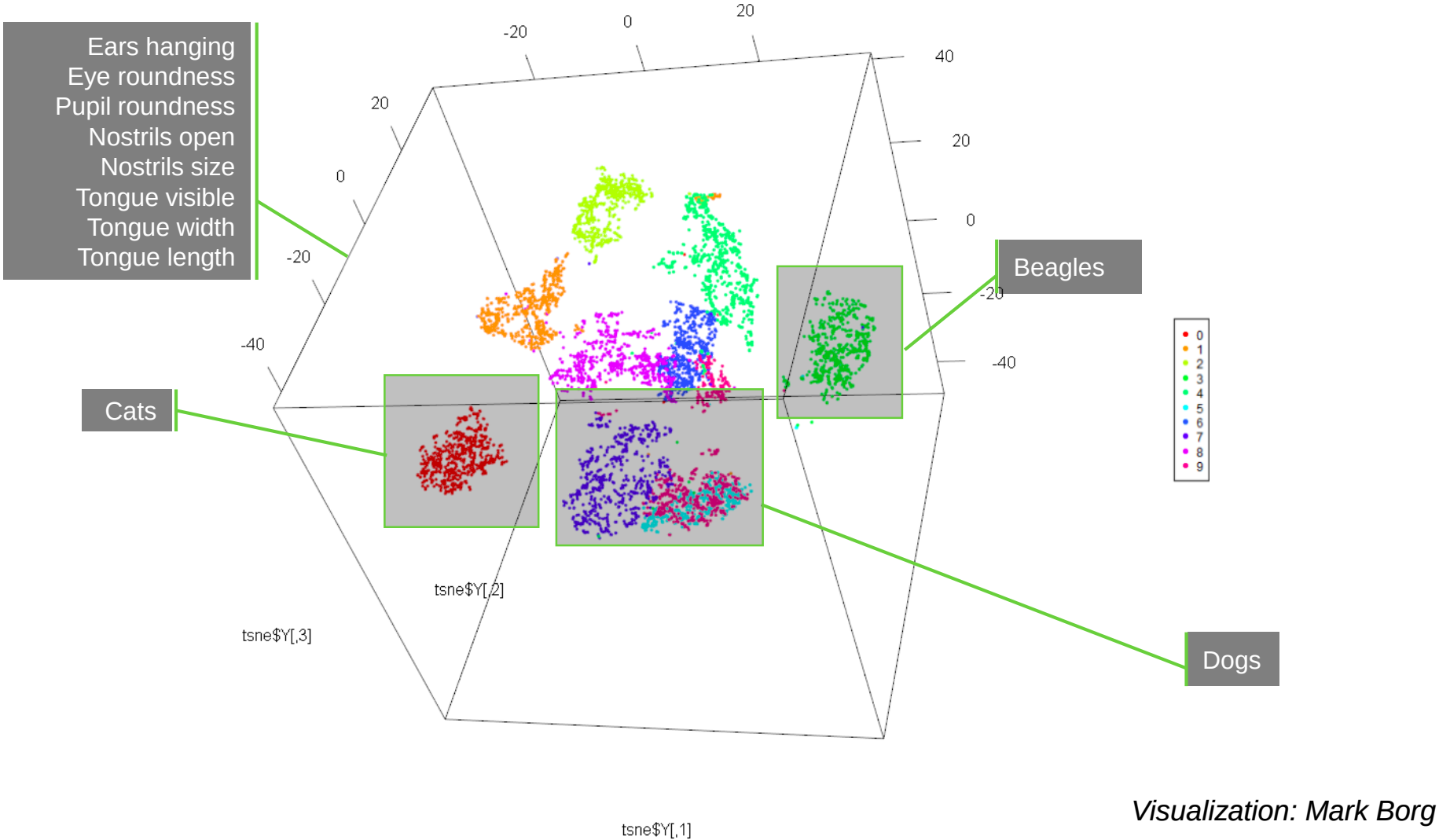
- Happier (& more productive) users!
- Improved response times, better scalability for VDI and Terminal Services
- Longer daily battery life
- Longer overall system life

WHO?
WHY?
WHAT?
HOW?

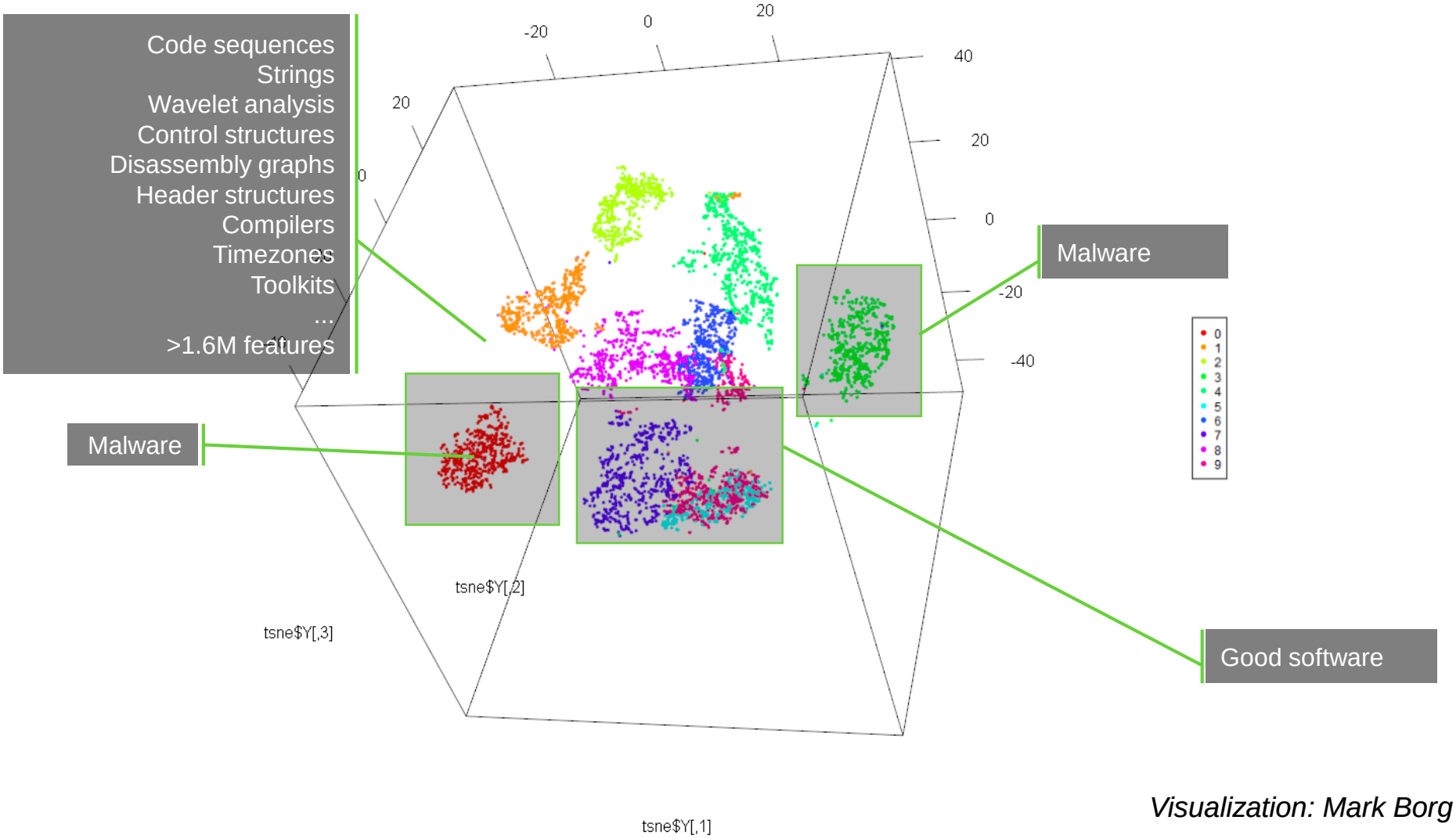

"If a typical person can do a mental task with less than one second of thought, we can probably automate it using AI either now or in the near future."
Prof. Andrew Ng, Stanford University
Former Chief Scientist, Baidu
Co-Founder of Coursera


‘Eye roundness’?
‘pupil roundness’?
‘Ears hanging?’
‘Tongue visible’?
‘Tongue width’?
‘Tongue length’?
‘Nostrils open’?
‘Nostrils size’?


‘Ears hanging’ = 0.1
‘Eye roundness’ = 0.9
‘pupil roundness’ = 0.9
‘Nostrils open’ = 1.0
‘Nostrils size’ = 0.9
‘Tongue visible’ = 0.8
‘Tongue width’ = 0.7
‘Tongue length’ = 0.4
(0.1, 0.9, 0.9, 1.0, 0.9, 0.8, 0.7, 0.4)
this dog’s feature vector
‘Ears hanging’ = 0.0
‘Eye roundness’ = 0.5
‘pupil roundness’ = 0.1
‘Nostrils open’ = 0.2
‘Nostrils size’ = 0.1
‘Tongue visible’ = 0.0
‘Tongue width’ = 0.0
‘Tongue length’ = 0.0
(0.0, 0.5, 0.1, 0.2, 0.1, 0.0, 0.0, 0.0)
this cat’s feature vector



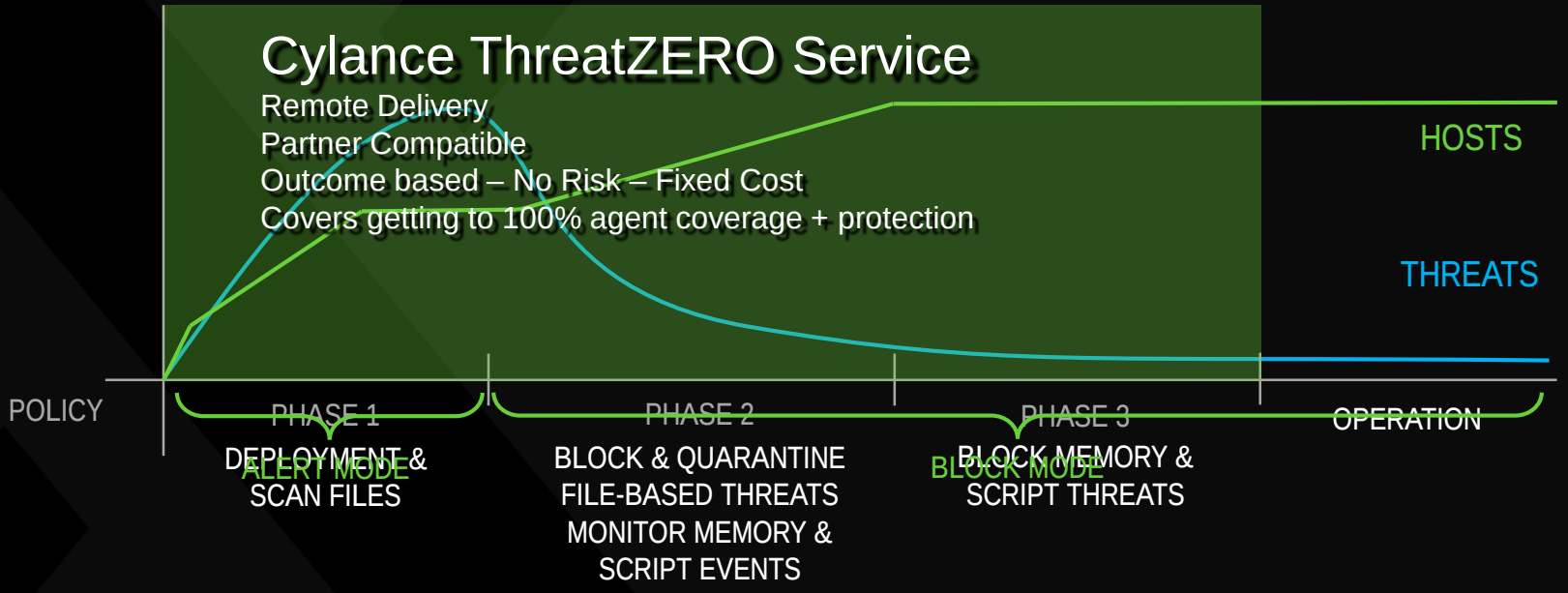
Visualization: Mark Borg



Visualization: Mark Borg

WHO?
WHY?
WHAT?
HOW?

POC & PRODUCTION DEPLOYMENT



CYLANCE


CYLANCE™