CYBERSECURITY'S FUTURE

A VC CISO'S BLUEPRINT FOR A QUANTUM POWERED AI WORLD

WHO AM I?

A little about me…

Bil Harmer
Operating Partner
& CISO
Craft Ventures
@wilharm3

1990 — SONY — IT Operations

1997 — Virtual Service Mgr Info Sec

2000 — DocSpace Inc — Dir IT Security — Acquired $650M

2004 — Manulife — AVP Architecture & Technology

2007 — SuccessFactors — VP Security — IPO $500M & Acquired $3.4B

2014 — SAP — VP Security & Global Privacy Officer

2014 — GoodData — CSO

2020 — Zscaler — CISO — IPO'd @ >$3B

2020 — SecureAuth — CISO & CIO

2022 — CRAFT — Craft Ventures — Operating Partner & CISO

2025

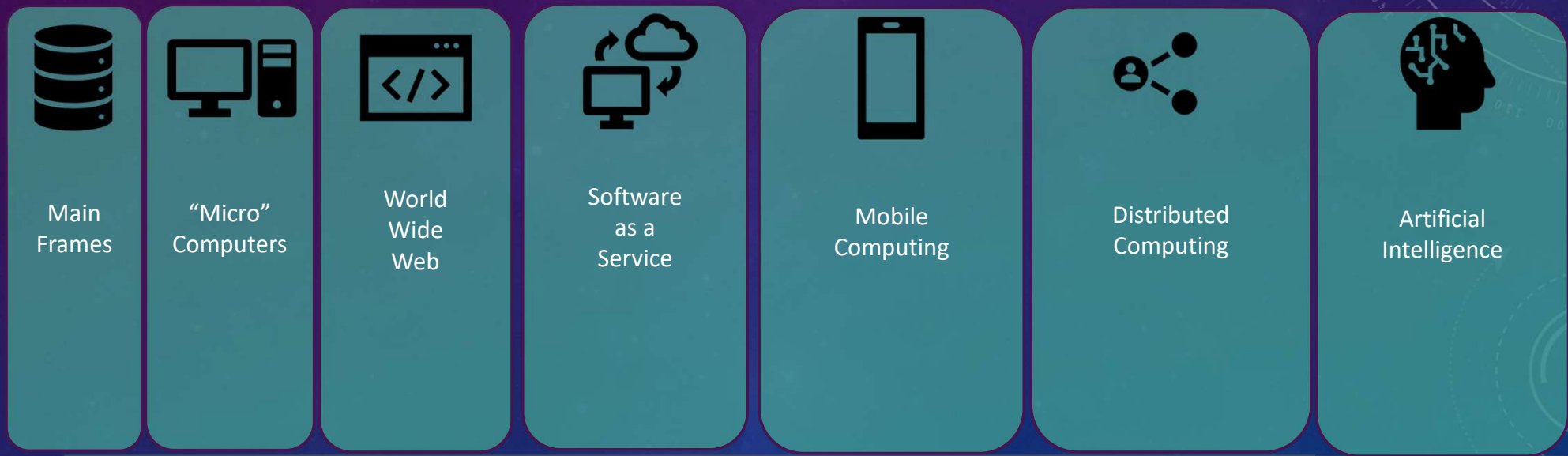
Board Member

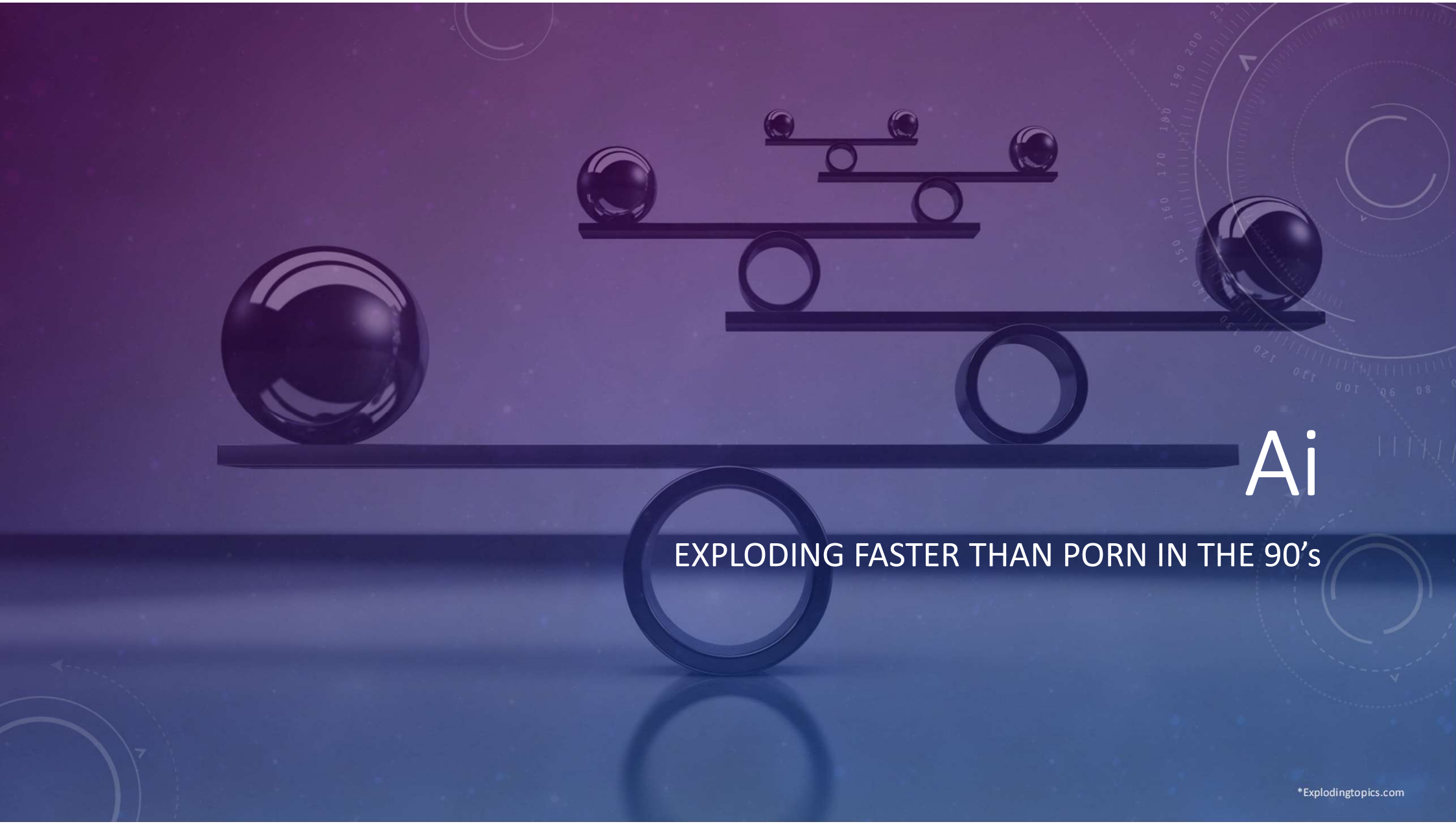
Current: SecurityPal
Prior: SuccessFactors Canda

Advisory Boards

Current: Dune Security, Weagle.AI, SiberX, Trust Science, SecureX.ai
Previous: SheildX Networks, Resolve Systems, GoodData, Adallom

The tech changes I've seen…




Ai
EXPLODING FASTER THAN PORN IN THE 90’s
*Explodingtopics.com

BY THE NUMBERS

AI Growth Rates Globally

67,200 AI COMPANIES

25% IN THE USA

35% USING AI

42% EXPLORING AI

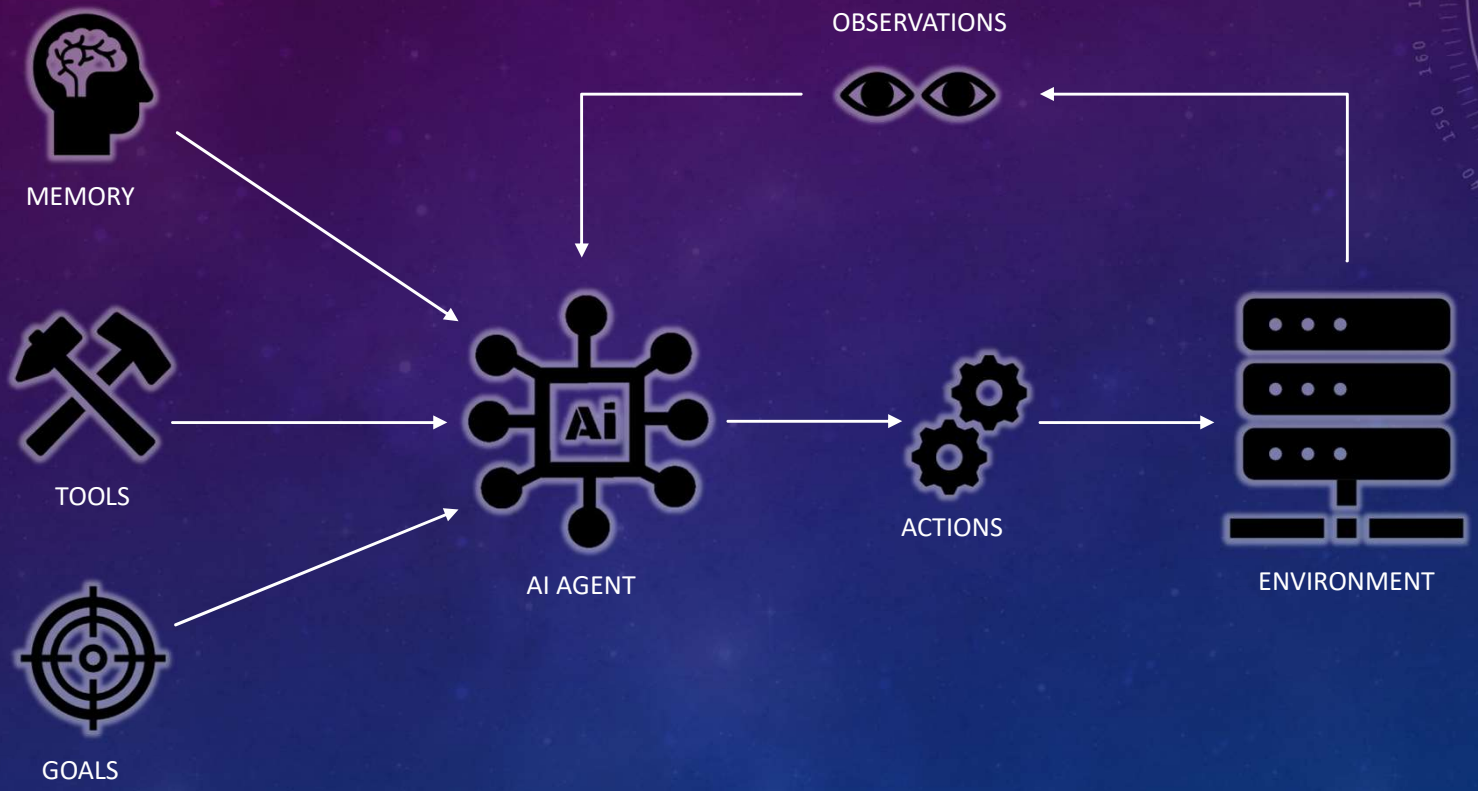
$93.5B IN FUNDING

$1.874T IN REVENUE

*Explodingtopics.com

THE FUTURE WILL BE Ai TO Ai

WELCOME TO AGENTIC AI



*TARUN SHARMA IBM

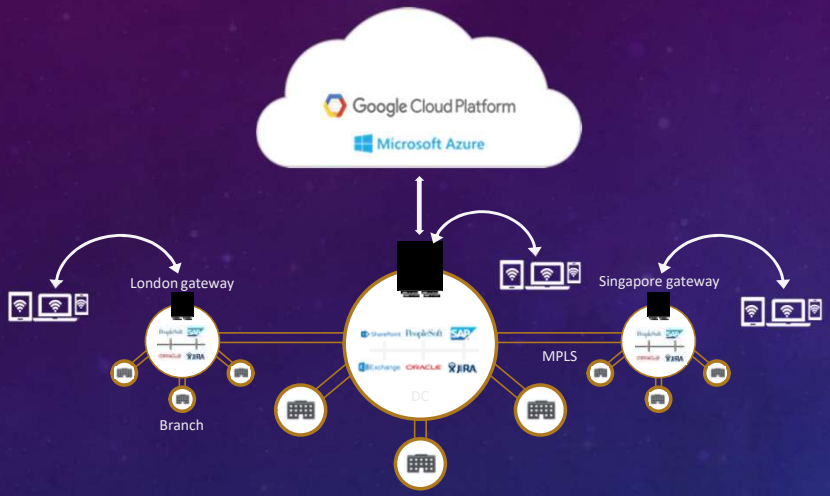
WELCOME TO SHADOW AI

WHAT DOES THIS MEAN TO
CYBERSECURITY?

HEADACHES!!!

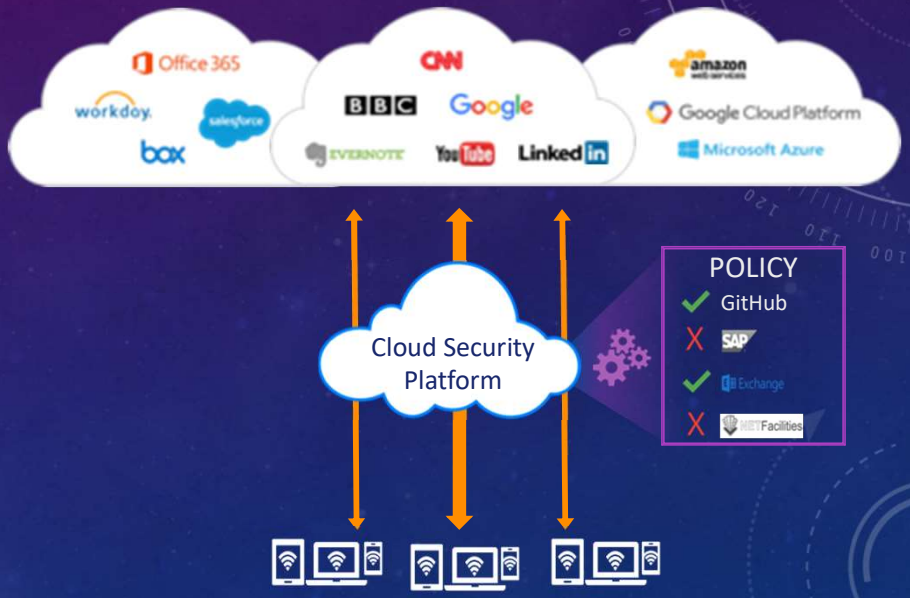
SECURITY TRANSFORMATION: 10 YEARS AGO

FROM: NETWORK-BASED SECURITY



Required users to be on the network

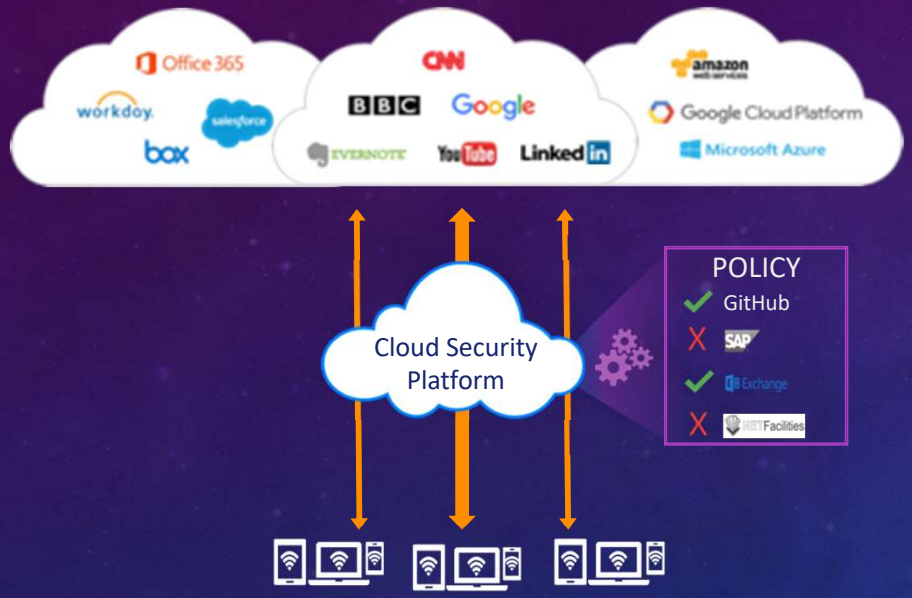
TO: POLICY-BASED ACCESS



Communications were secured, network is irrelevant

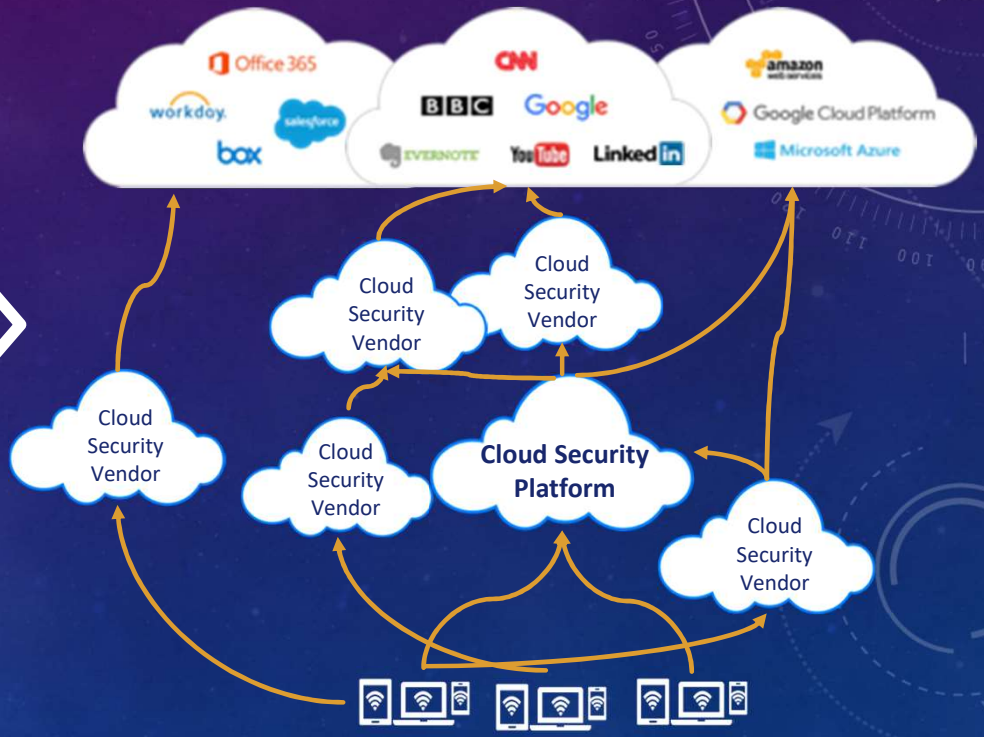
SECURITY TRANSFORMATION: THE LAST 5 YEARS

FROM: POLICY-BASED ACCESS



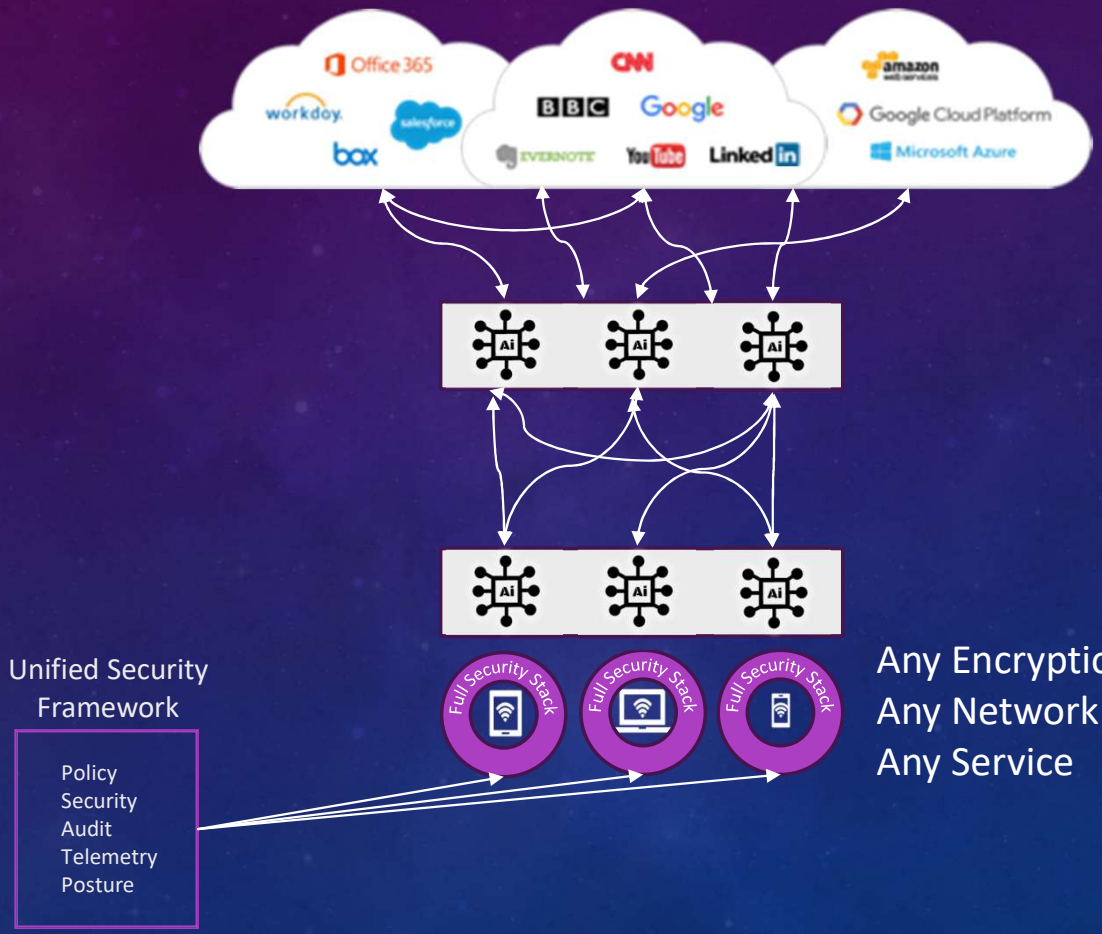
Communications are secured, network is irrelevant

TO: FULL ON CLOUD HOPPING



Traffic is a mess and we're back to where we started

AGE OF THE HYPER CONVERGED ENDPOINT



WHAT HAPPENS WHEN WE ADD QUANTUM SAFE ENCRYPTION?

MORE HEADACHES!!!

UNTIL THEN, WHAT DO WE DO?

WEAK CRYPTOGRAPHY

DATA CLASSIFICATION

QUANTUM RESISTANCE

FUTURE BREACHES

VENDOR READINESS

WHAT ABOUT THE AI STACK?

*Explodingtopics.com

BLINDING MIGRAINES!!!

BAD Ai

PHISHING AND VISHING AT SCALE

*Explodingtopics.com

DEEPFAKES

Vishing, Smishing & Phishing

1,265% ATTACK INCREASE

1,740% INCREASE IN DEEPFAKE

53% SHARE THEIR VOICE

76% LACK FRAUD PROTECTION

3 OUT OF 4 FREE TOOLS FAIL

$2.7B LOST

*Explodingtopics.com

MY NAME IS WERNER BRANDES. MY VOICE IS MY PASSPORT. VERIFY ME

Ai VOICE CLONING

70% CAN'T TELL THE DIFFERENCE

77% LOST MONEY

10% SPOKE TO A ROBOT

36% LOST UP TO $3K

7% LOST $5K-$15K

*Explodingtopics.com

IT GETS WORSE

$25M DEEPFAKE VIDEO CALL

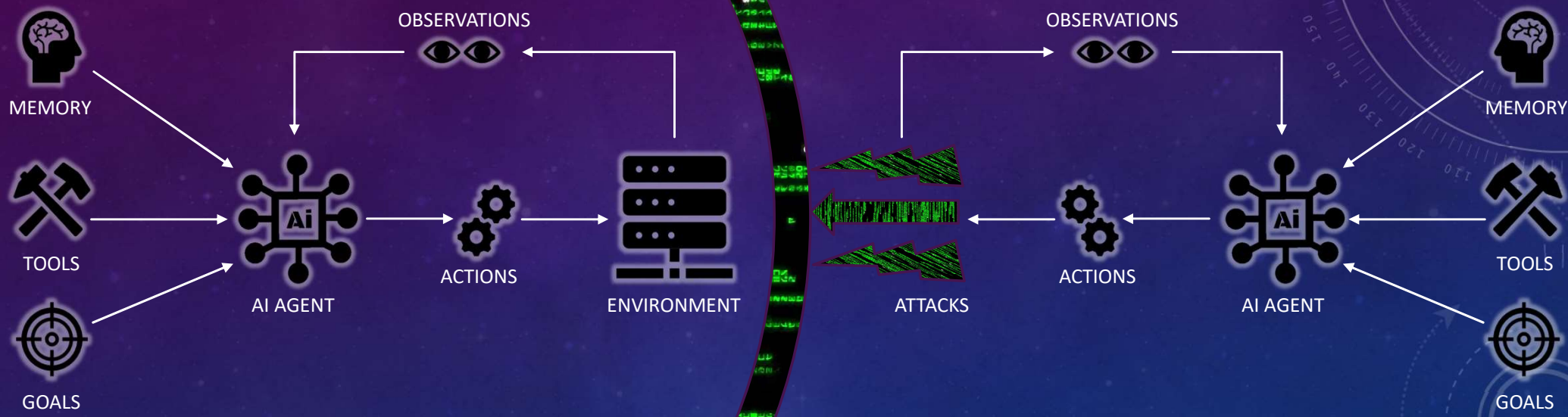
$1M RANSOM

KNOWB4 HIRED A NORTH KOREAN

*Explodingtopics.com

WHEN Ai ATTACKS - Ai DEFENDS

THE FUTURE OF CYBER WILL BE Ai vs Ai



IDENTITY AGENTS

AI SOC

AI CODE ANALYZERS

AI POWERED THREAT INTEL

AI USER RISK MANAGMENT

AI PEN TESTING

WHAT DO THESE ALL HAVE IN COMMON?

THE SOC DEFENSE TODAY

- INCONSISTENT
- SCALABILITY ISSUES
- EXPERTISE DEPENDANT
- SLOWER RESPONSE TIMES
- INCORRECTLY INCENTIVISED

THE SOC DEFENSE TOMORROW

- CONSISTENT ANALYSIS
- INFINITELY SCALABLE
- ENDLESS EXPERIENCE
- FASTER THAN HUMAN
- AI DOESN’T REQUIRE INCENTIVES…YET

WHAT AM I LOOING AT THIS YEAR?

IDENTITY AGENTS

AUTONOMOUS TESTING

RE-IMAGING THE SIEM

RUNTIME SENORS

SOC AGENTS

AI (PRODUCT) SECURITY

*Explodingtopics.com

ART OF THE POSSIBLE

NEURALINK
TESLA
THE BORING COMPANY
STARLINK
Powered by
SPACEX

STARLINK
CONNECTED

Neuralink

X Ai
INTELLIGENCE

TELSA VISION

TESLA BATTERY
POWER

BORING COMPANY ARMED!!!

THANK YOU !