RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

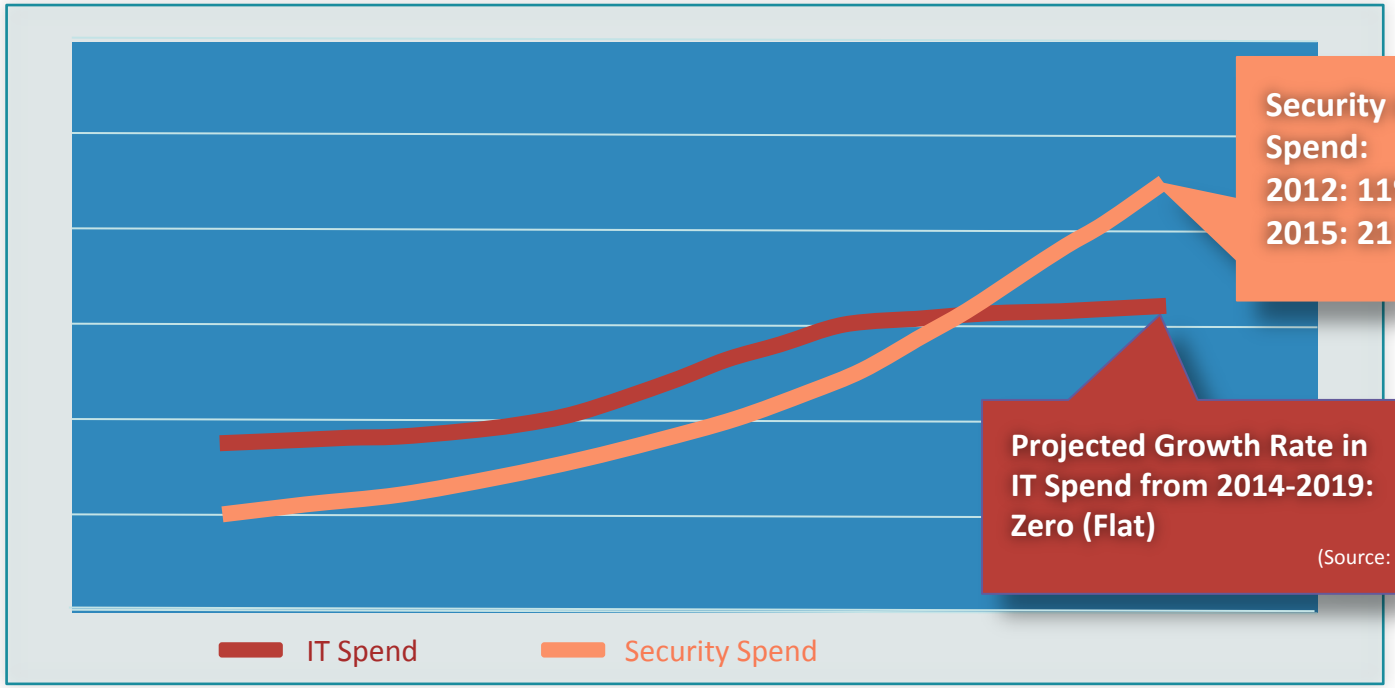
SESSION ID: SEM-M04

DATA SCIENCE– HOW IT'S BECOMING A PIVOTAL PART OF IT SECURITY, AUTOMATION & ORCHESTRATION

Vijay Ganti

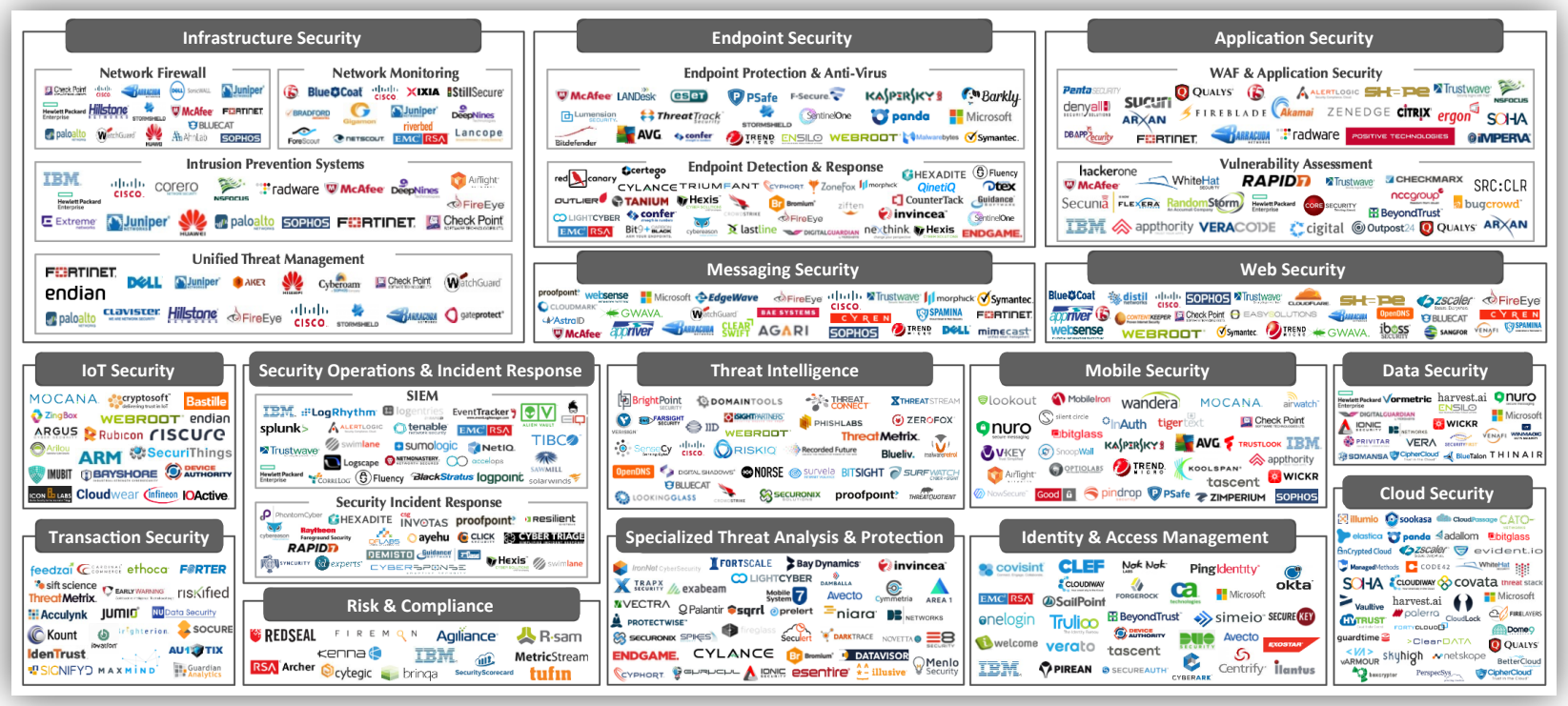
Head of Product & ML/AI Research
Security Products Group
VMware

Security spend: outpacing IT spend 2:1

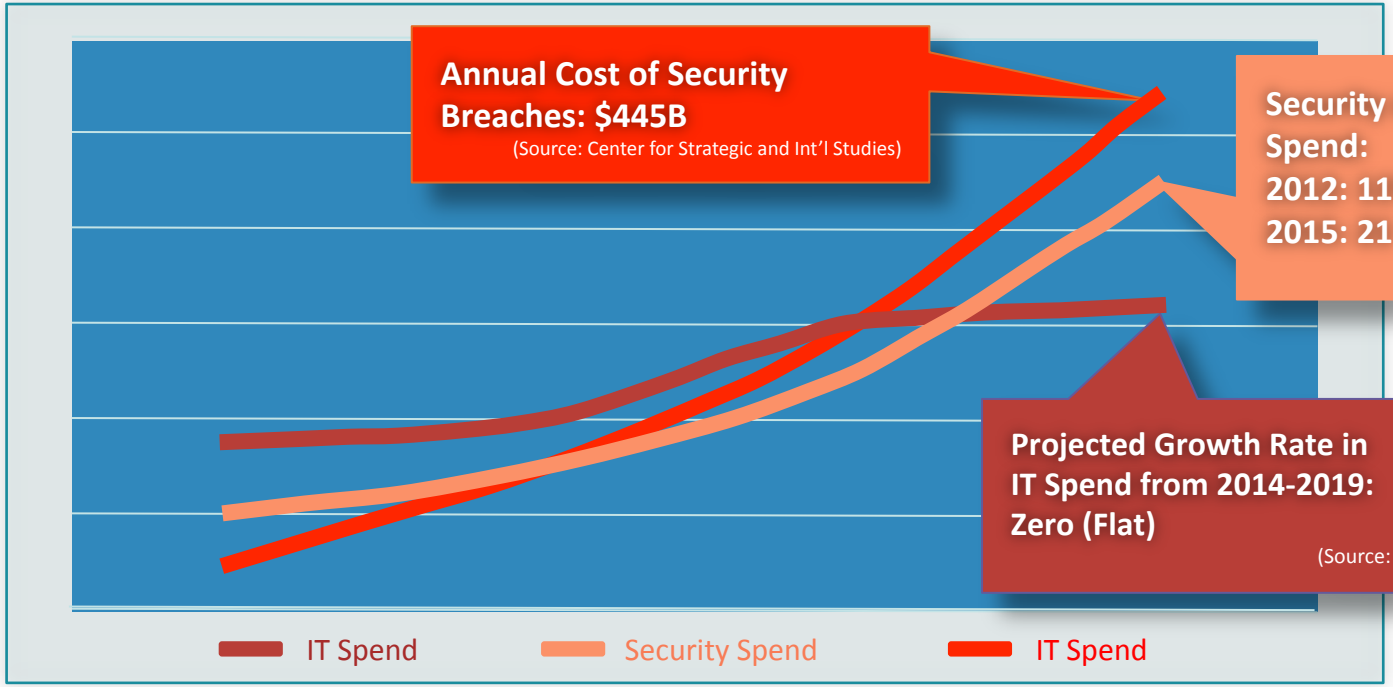


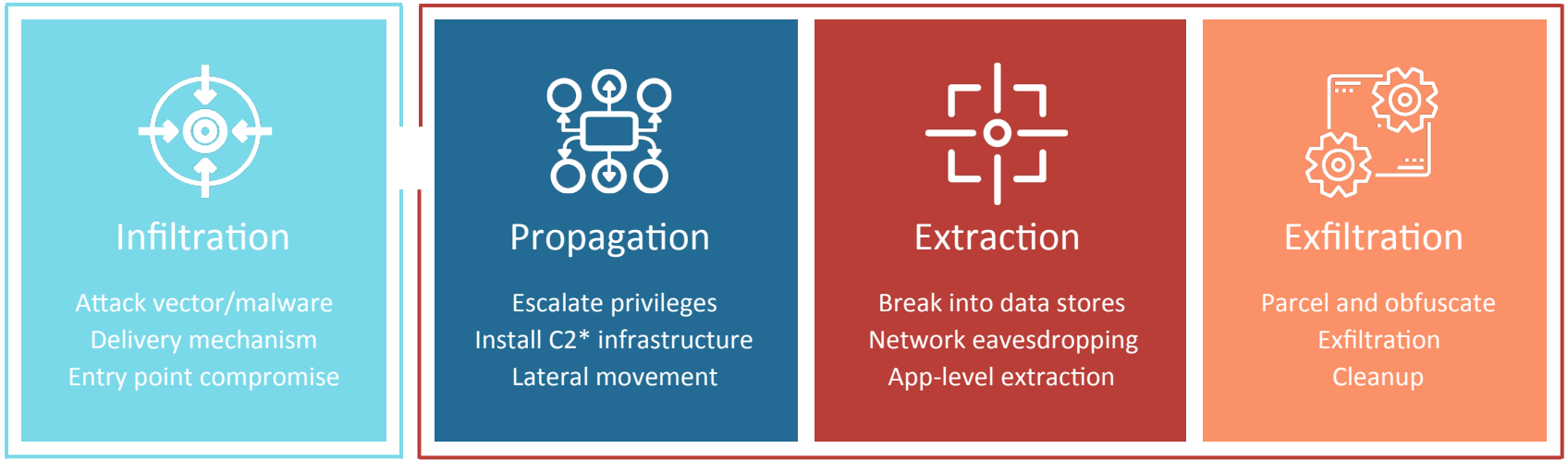
Source: IDC

Information Security Spending >$80B in 2016*



A Picture of Diminishing Returns





We over invest in Infiltration Prevention

We under invest in Resilience

Propagation

Escalate privileges
Install C2* infrastructure
Lateral movement

Extraction

Break into data stores
Network eavesdropping
App-level extraction

Exfiltration

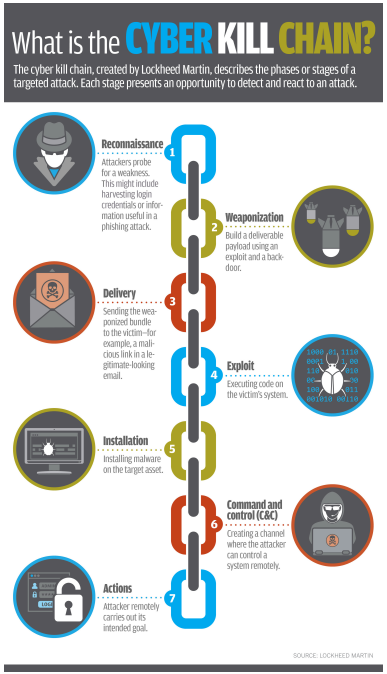
Parcel and obfuscate
Exfiltration
Cleanup

We’re Watching The Wrong Thing

vmware®

NOT LEVERAGING

ASYMMETRY



HOME COURT ADVANTAGE

Infiltration

Attack vector/malware
Delivery mechanism
Entry point compromise

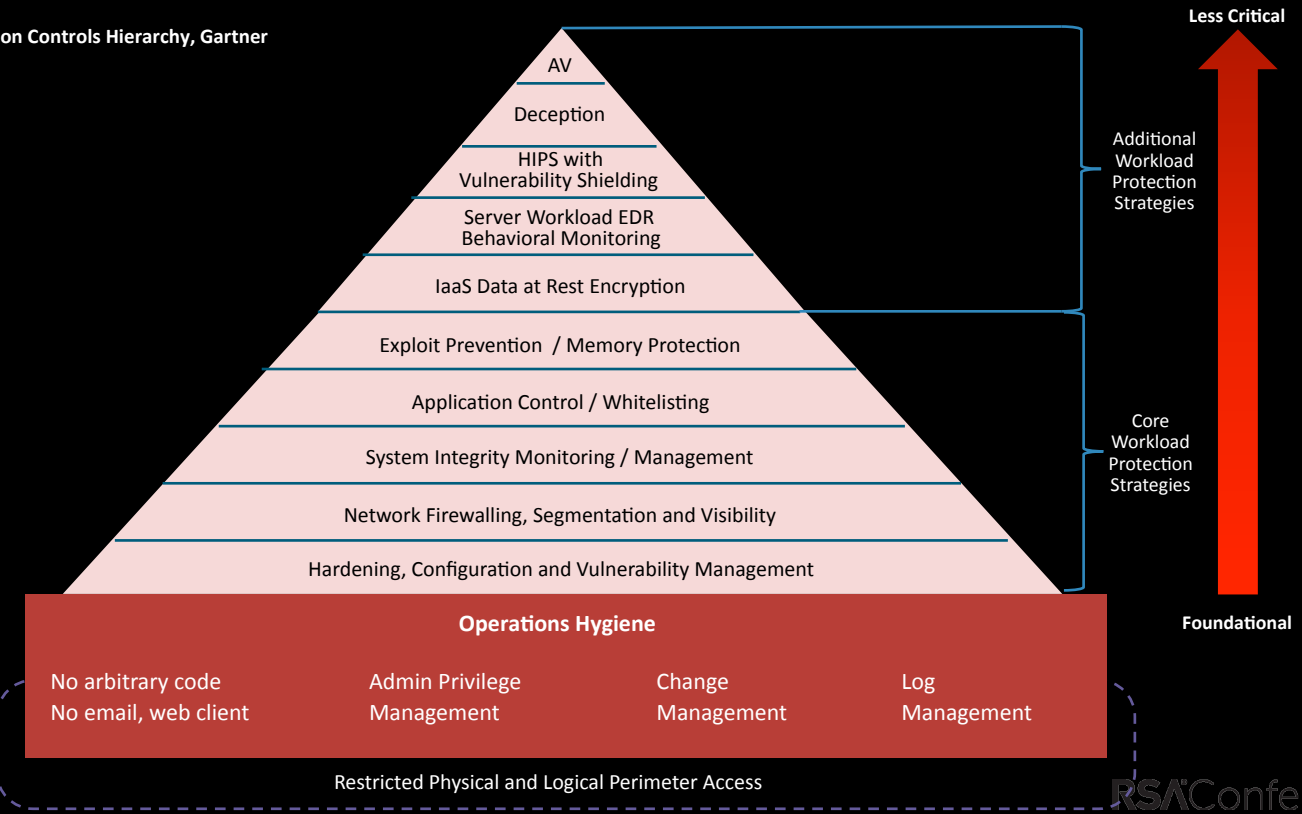
We over invest
in
Chasing Threats

We under invest
in Shrinking
the Attack Surface

Focus on shrinking the attack surface

Shrinking the Attack Surface

Figure 1. Cloud Workload Protection Controls Hierarchy, Gartner



Source: Gartner (March 2017)

Cyber Threats
Residual Risk

Cyber Hygiene
Attack Surface

Infiltration

Attack vector/malware
Delivery mechanism
Entry point compromise

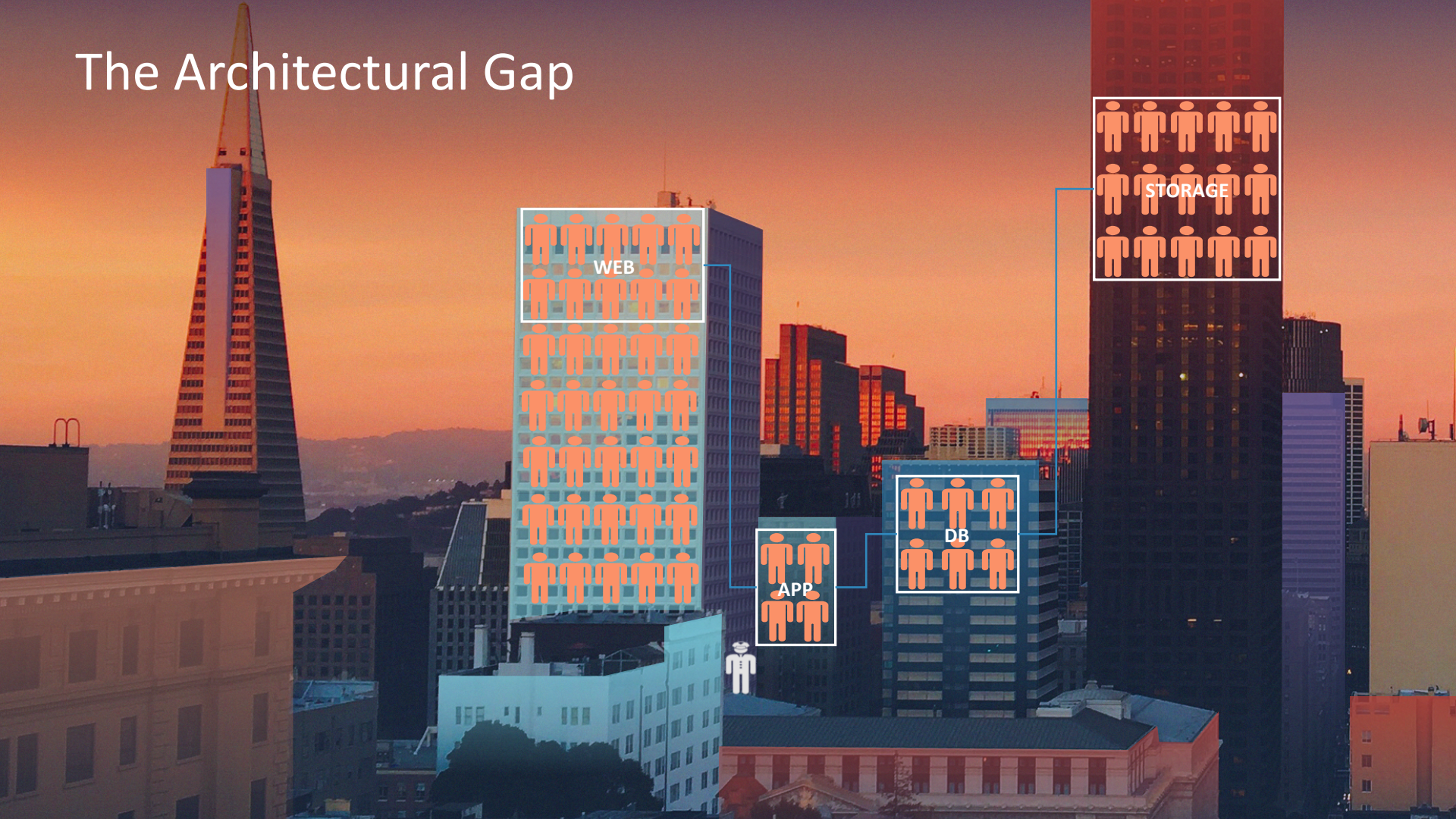
We over invest
in
Chasing Threats

We under invest
in Shrinking
the Attack Surface

We Align Security
To
Infrastructure

Rather than Align
To
Applications & Data

The Architectural Gap



Rethinking CYBER Security

Cyber Threats
Residual Risk

Network Controls | Data Controls | Compute Controls

GRC | SIEM/SOC

Integrated Ecosystem

Users | Devices | Network | Storage | Compute

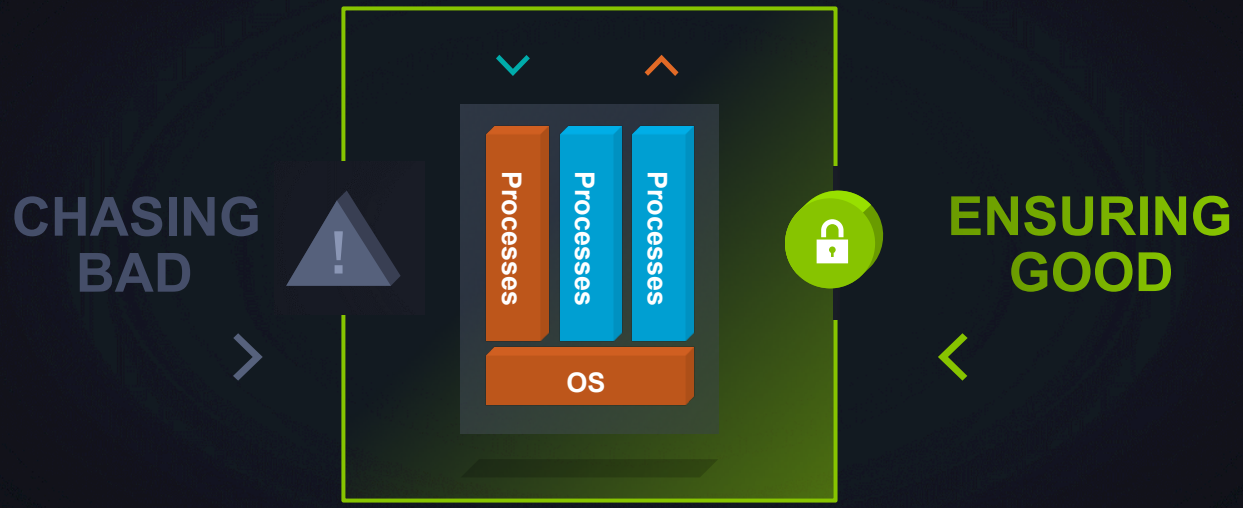
Securable Infrastructure

Least Privilege | Micro-Segmentation | Encryption | Multi-Factor Authentication | Patching

Cyber Hygiene
Attack Surface

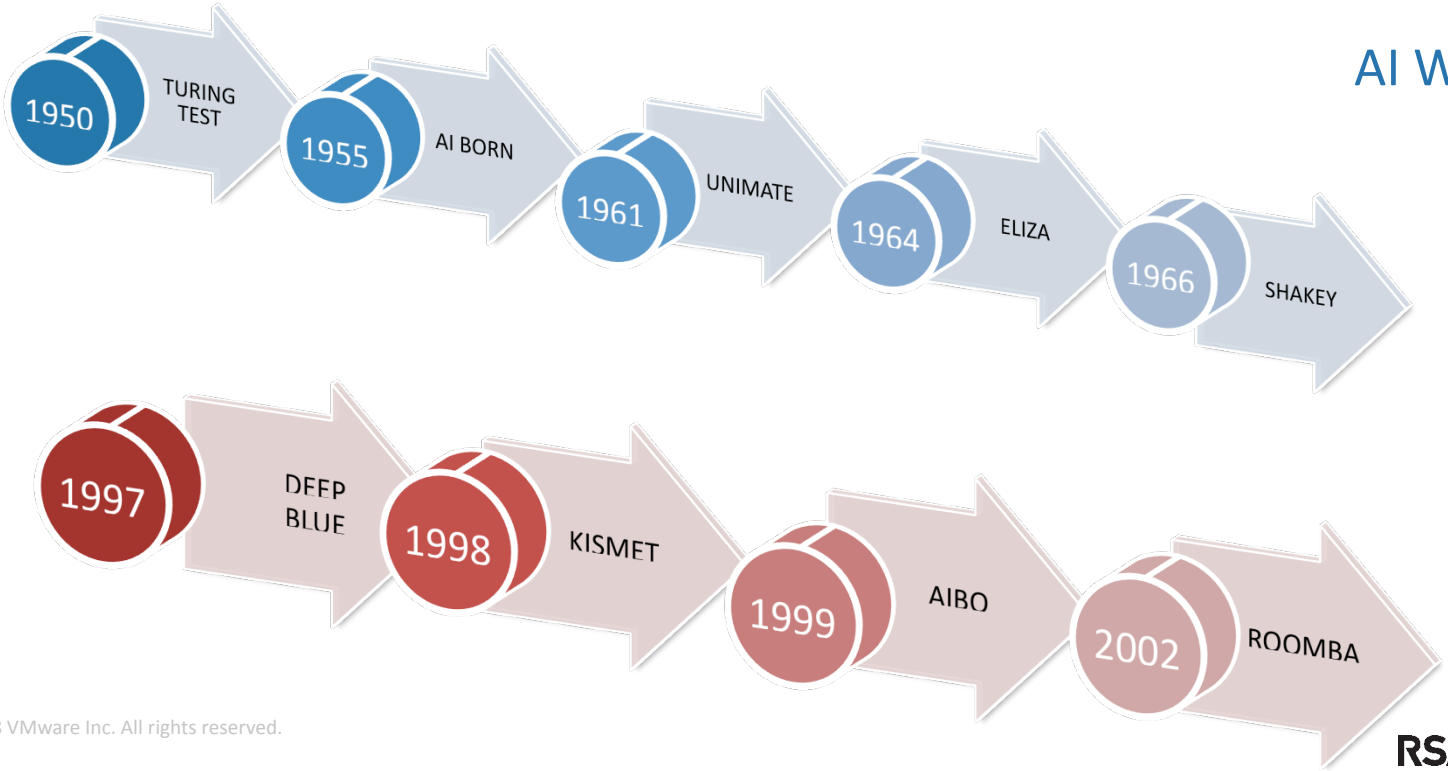
CHASING BAD…

CHASING BAD… VERSUS ENSURING GOOD



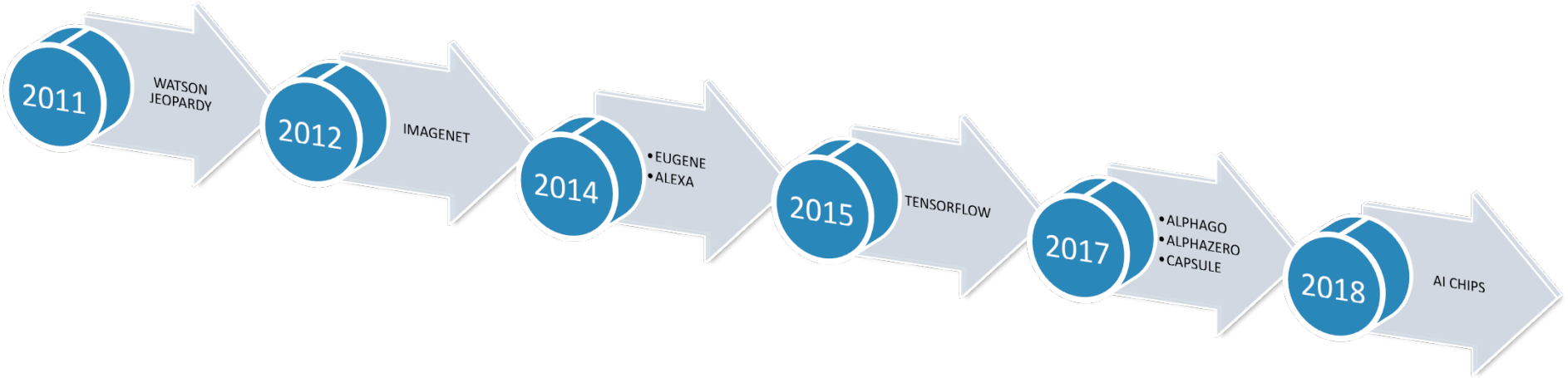
How can AI help with, Threat detection, cyber hygiene and modern security operations?

A brief history of AI

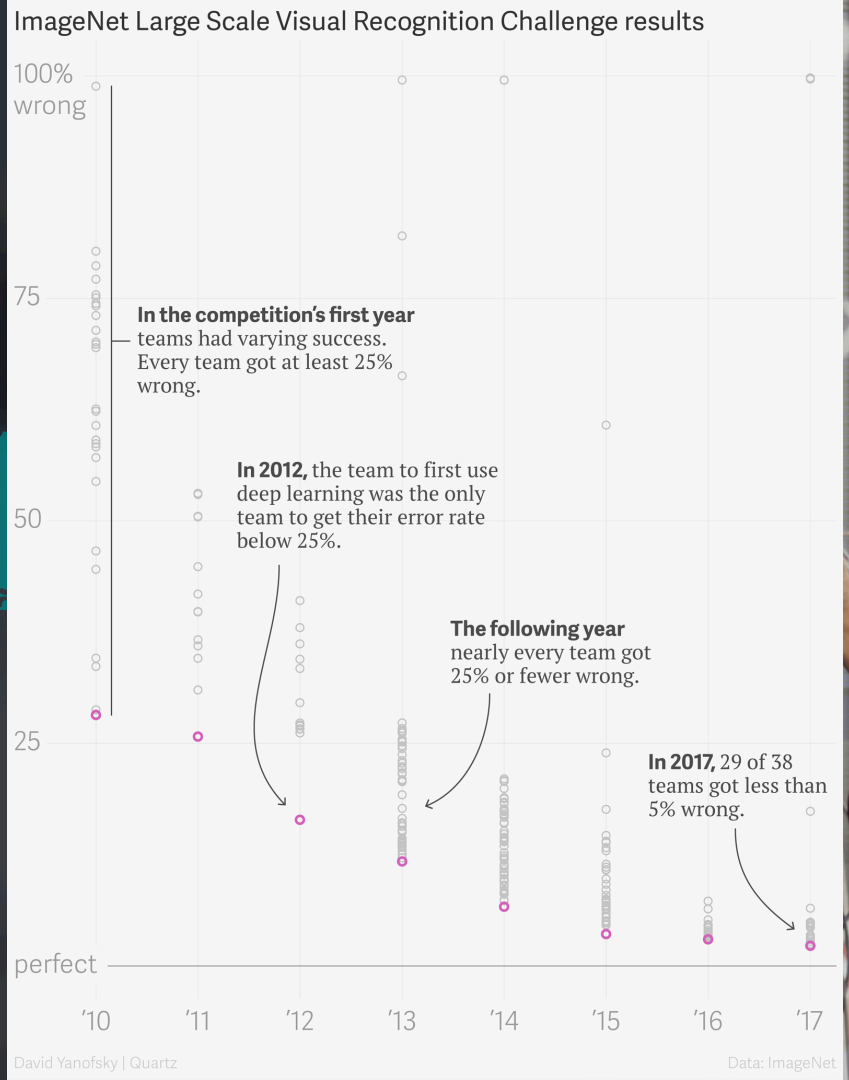


AI WINTER

A brief history of AI



2012



RECENT AI ACCOMPLISHMENTS

JANUARY 25, 2017

Deep learning algorithm does as well as dermatologists in identifying skin cancer

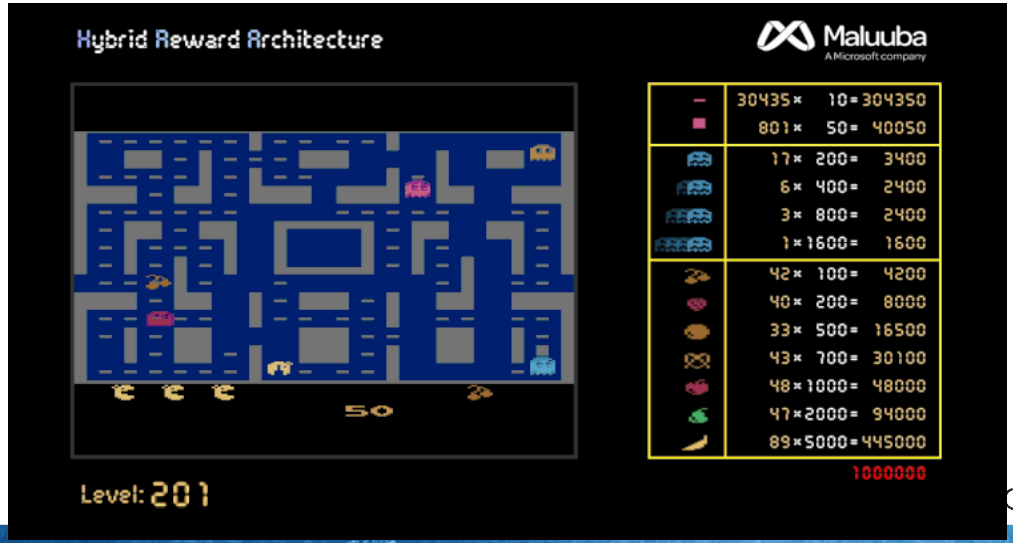
In hopes of creating better access to medical care, Stanford researchers have trained an algorithm to diagnose skin cancer.

www.theguardian.com

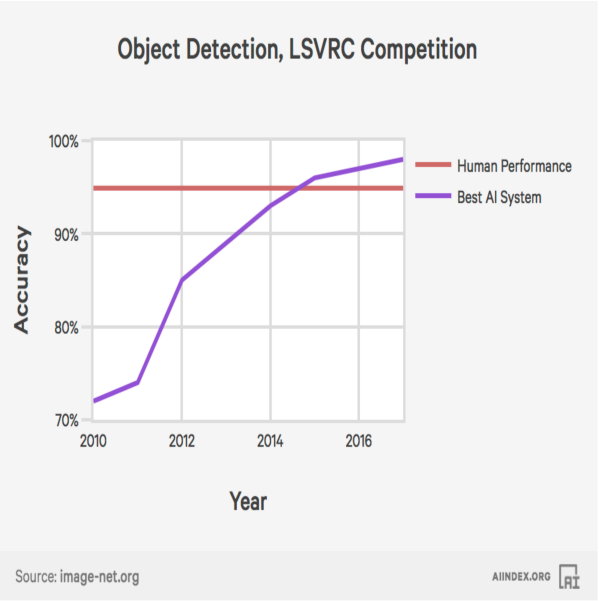
AlphaZero AI beats champion chess program after teaching itself in four hours

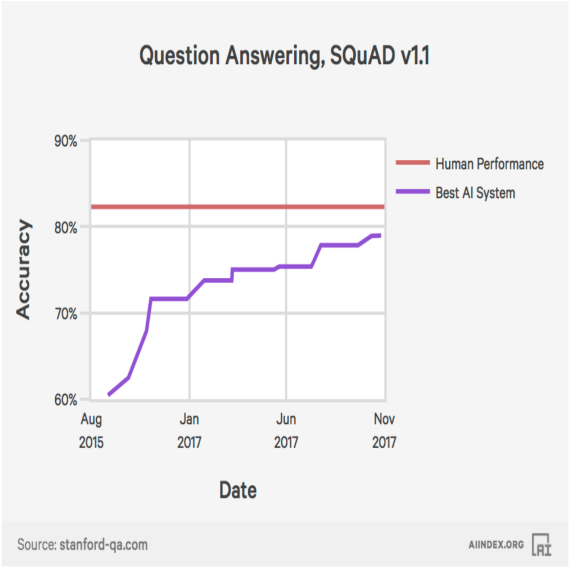
Microsoft's AI beats Ms. Pac-Man

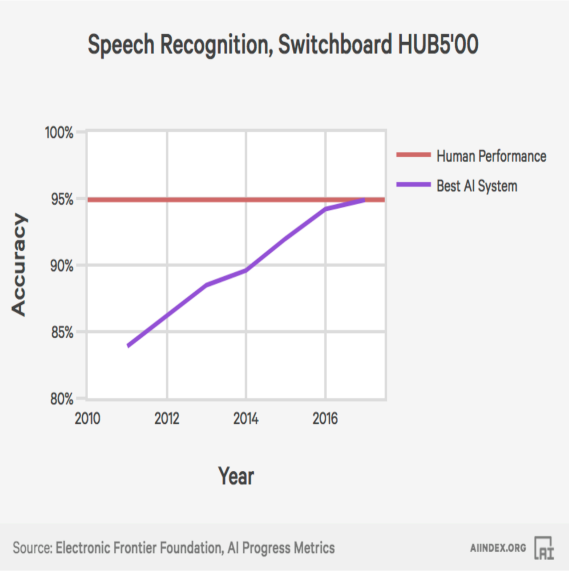
*Posted Jun 15, 2017 by **Brian Heater** (@bheater)*



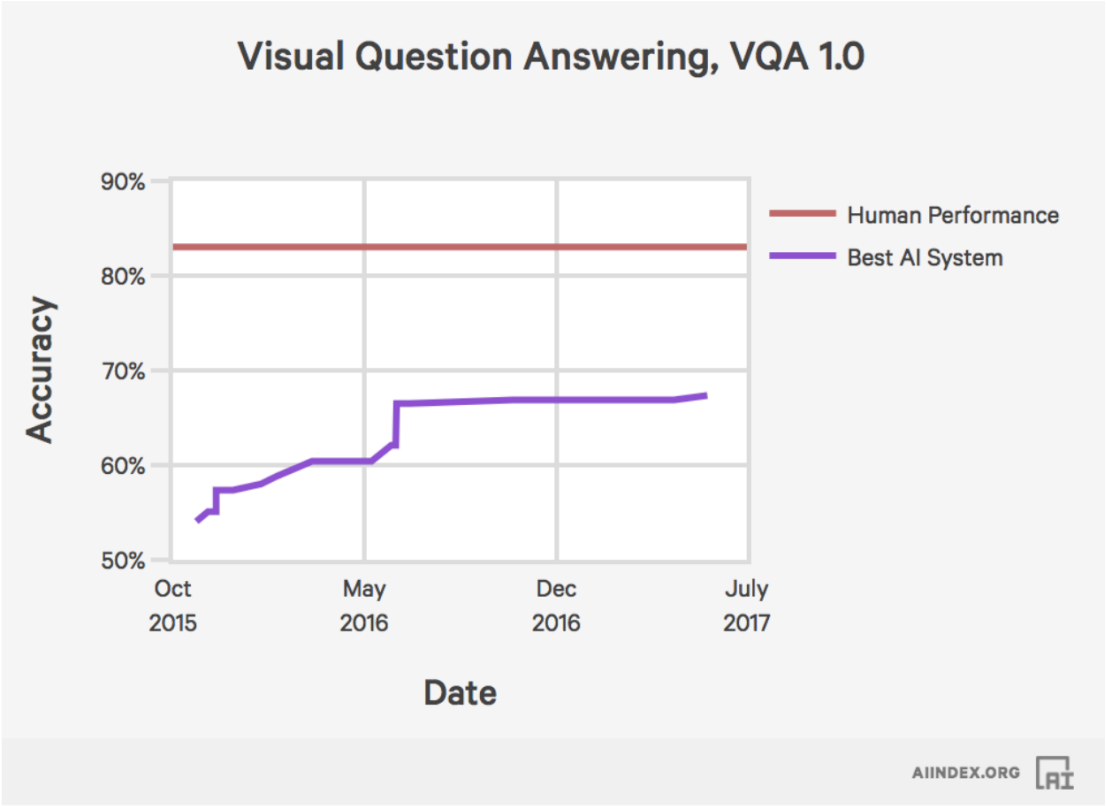
RECENT AI ACCOMPLISHMENTS WITH TECHNICAL PERFORMANCE







Long way to go before generalized AI

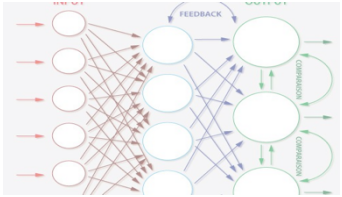


What changed in AI since last time round ?

Lots of Data

Lots of Compute

Use cases /w lots of money



Algorithmic Innovation

Challenges in Applying AI/ML to chasing the bad guys

A PERFECT STORM

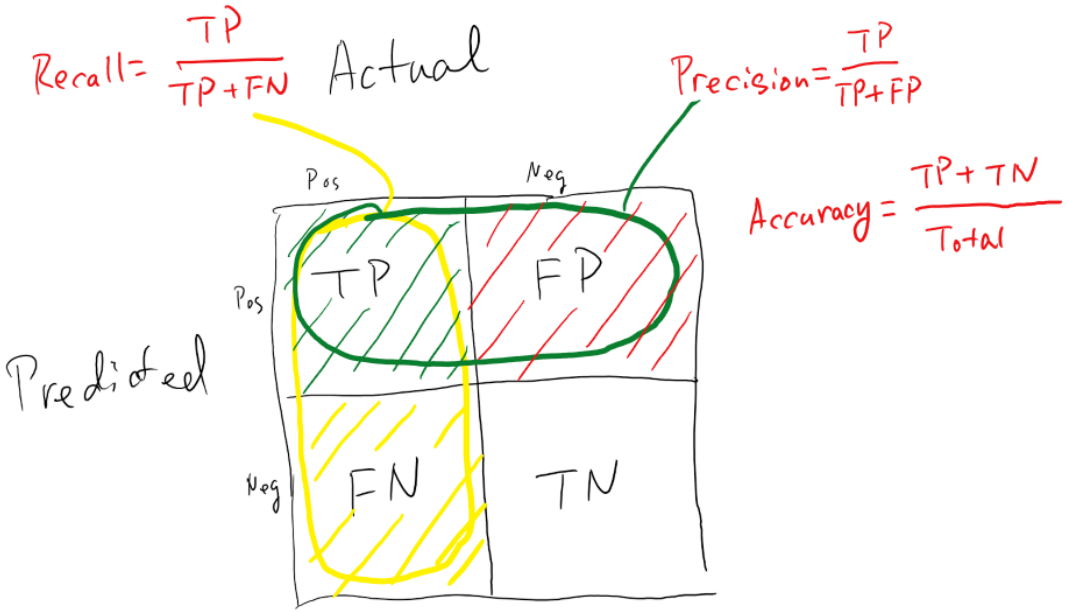
Adversarial

No Rules

Data Scarcity

CHASING BAD IS HARD FOR EVEN AI/ML

False positives vs false negatives - Cost



- Huge focus on false negatives
  - Is the software able to detect attacks or malware?
- Little focus on false positives
  - Is your software throwing alerts when it should not ?
  - 10,000 to 150,000 alerts per day.

Deep Learning vs Traditional Machine Learning

- What is the interpretability of the predictions?
- Performance – Accuracy (Precision & Recall)
- Amount of data needed for training models
- Where does the domain expertise go? (feature engineering vs designing networks)

What About ensuring Good?

AI is a must to help achieve cyber hygiene in dynamic environments, at scale

- Understand Intended Application Composition
- Understand Intended Application Behavior
- Understand Intended Operational Changes

THIS IS NOT ADVERSARIAL, HAS RULES & THERE IS DATA

Understanding application composition

- Service/Application Identification or Discovery
- Distributed Application Component Identification
- VM Composition

Understanding application Behavior

- Coarse Grain Network Behavior
- Fine Grain Network Behavior
- System Calls
- File System Organization

Understanding OPERATIONAL processes and CHANGES

- Routine application changes (upgrades/patches)
- Routine infrastructure changes
- Operational activities (backup/restore, monitoring, troubleshooting, administering)

What more can AI do?

AI should be the fabric of your security operations

- Empower security analysts with contextual information for quick resolution
- Use analysis bots for reducing burden on security analysts with deeper, targeted, automated and non-disruptive analysis in response to high-level anomalies

Takeaways

AI should be the fabric of your security operations

- AI is eating the world but it's not likely to be the silver bullet for threat detection
- Cyber hygiene is foundation for cybersecurity & AI will transform cyber hygiene at scale
- AI will make security analysts super human

Thank you

VMware

@vijayganti
Head of Product and ML/AI Research