5th HVM New Materials
Conference Summit 2019
Cambridge, UK 6-7 November 2019
www.cir-strategy.com/events

AI-Based Autonomous Response: Are Humans Ready?

Ben Gompes

Cyber Security, Darktrace

Company Overview

World-leading artificial intelligence for cyber defense

Creator of **autonomous response** technology

Headquartered in **San Francisco and Cambridge, UK**

1.65 BN
VALUATION

3000
CUSTOMERS

1000
EMPLOYEES

40
OFFICES

Forbes THE 2018 Cloud100

CNBC DISRUPTOR 50 2018

FT FINANCIAL TIMES 1000 Europe's Fastest Growing Companies

FAST COMPANY THE WORLD'S MOST INNOVATIVE COMPANIES 2018

DARKTRACE

Evolving Threats in the Digital Age

- Increasing speed and sophistication
- Zero-days, IoT, insiders, ‘low and slow’
- Digital complexity and diversity expands attack surface and limits predictability
- AI-powered threats in near future - will deliver targeted attacks at scale

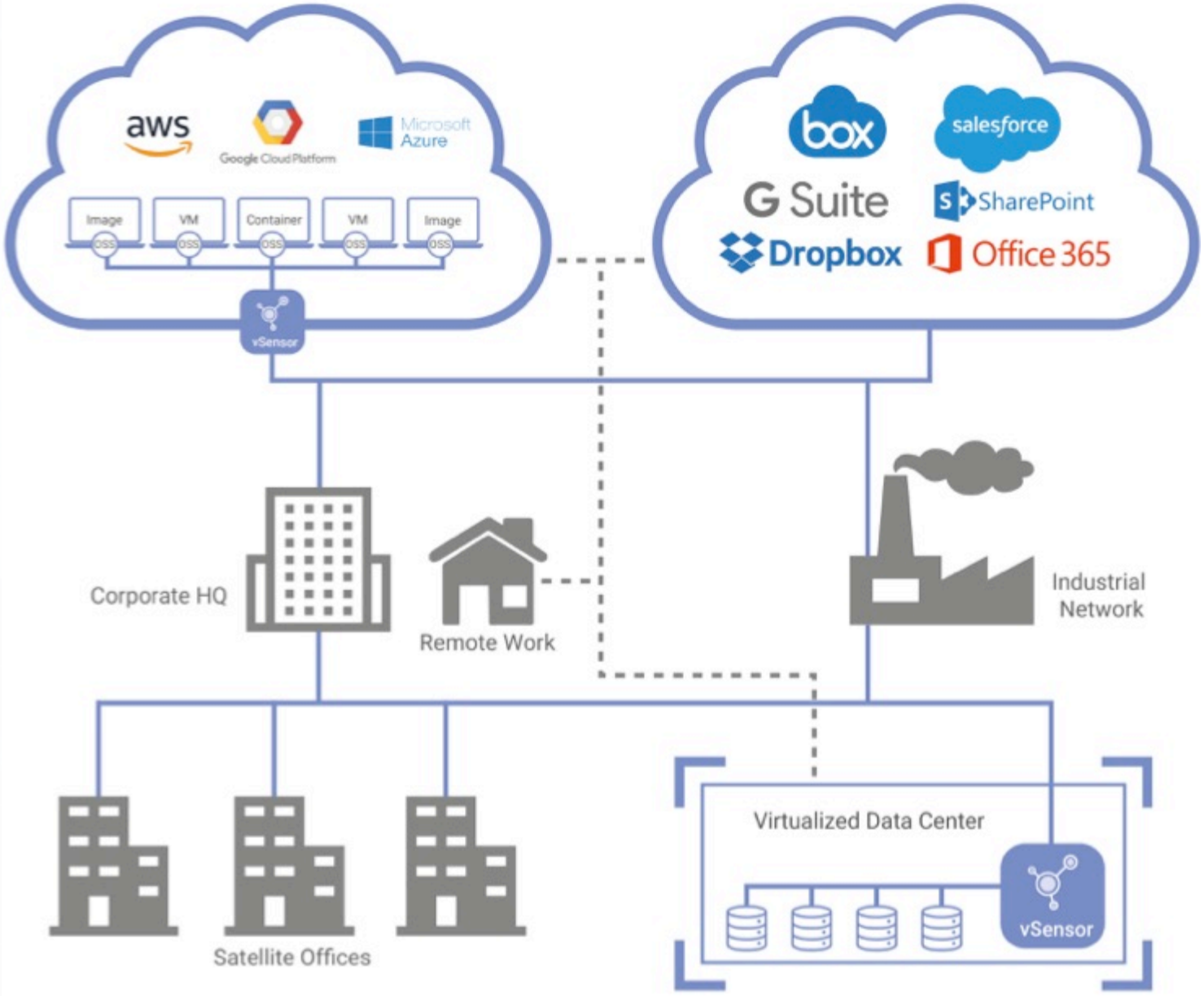
Legacy security is *constantly* outpaced

DARKTRACE

AI-Based Cyber Immune System

- Learns ‘self’ in real time
- Detects all forms of cyber-threat
- Works on cloud, SaaS, enterprise, industrial
- Fights back autonomously
- Scales up or down in diverse environments
- 100% visibility

Self-Learning AI For Your Entire Infrastructure



DARKTRACE

Cyber AI Response

Modern Attacks Outpace Human Teams

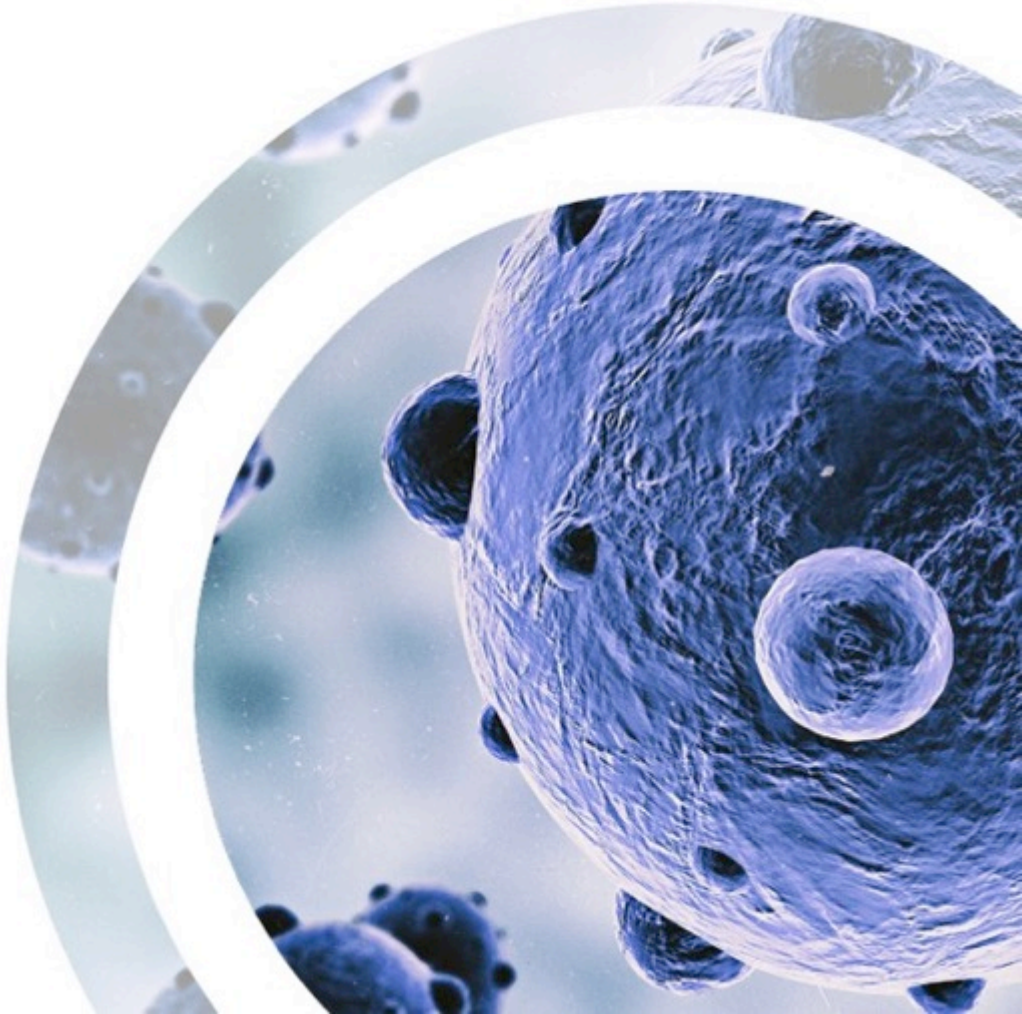
DARKTRACE

- Destructive attacks target data or operational systems
- Aim for maximum impact in minutes
- Majority of organizations work 9x5
- Even when present, teams cannot investigate threats in minutes let alone respond to them
- We need self-defending organizations that are safe by default
- Digital antibody, surgical AI response

Autonomous Response

DARKTRACE

- Fight back against in-progress attacks
- Automatically produces real-time active responses to potential threats
- Targeted and proportionate response
- Not reliant on signatures or prior knowledge
- Gives humans time to catch up
- Sustains normal operations during attacks



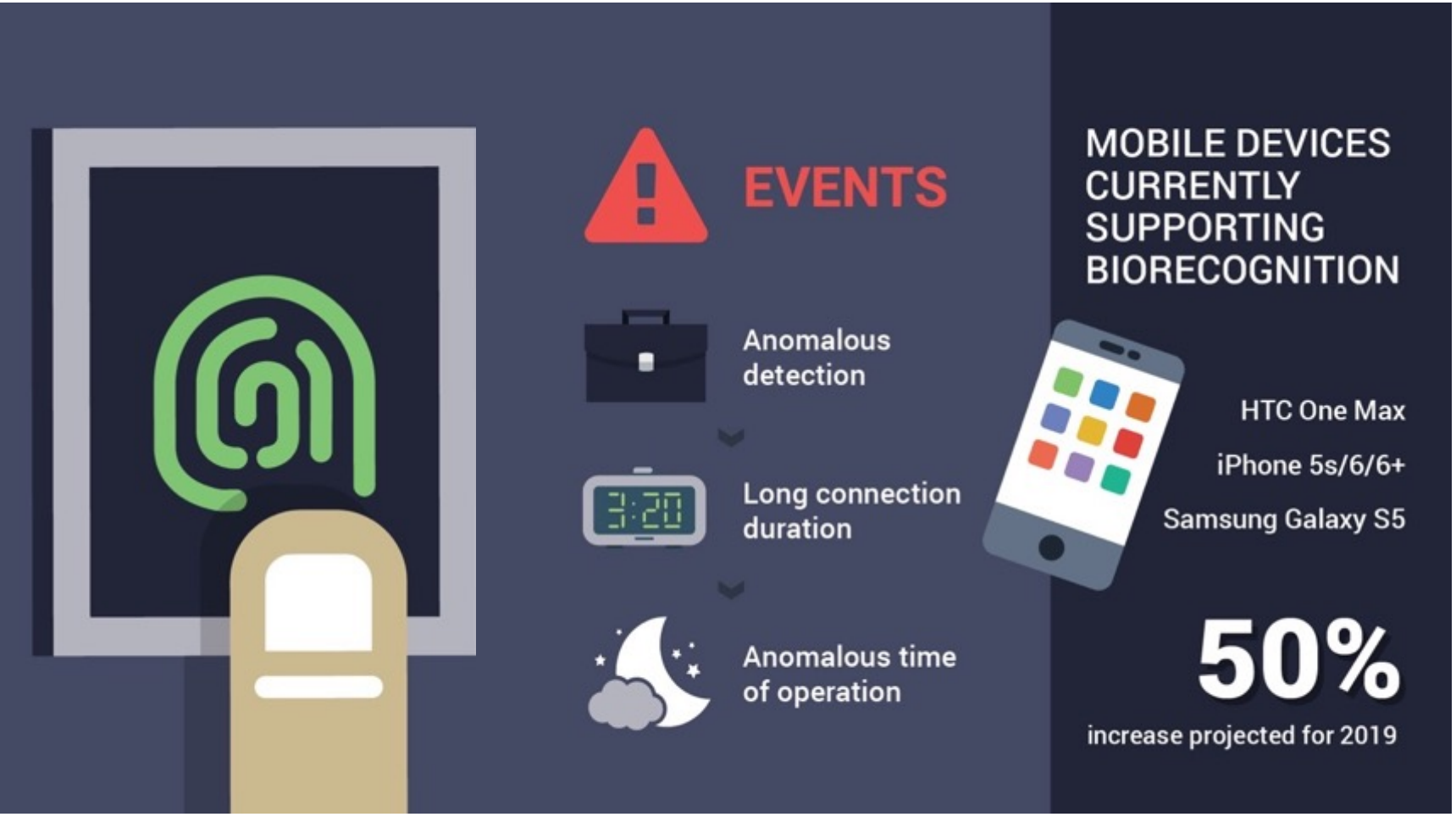
Thousands of Unknown Threats Caught Every Day

- Zero-day trojans
- Insider threats
- Hacked IoT devices
- Compromised credentials in Salesforce & Office 365
- Critical misconfigurations in AWS, Azure, & GCP
- Long-term, stealthy cyber espionage
- Malicious crypto-mining
- Machine-speed worms and ransomware
- ‘Low and slow’ data leaks
- ICS and SCADA compromises

DARKTRACE

Case Study: Compromise of Biometric Scanner

DARKTRACE



- Industry: Manufacturing
- Attacker successfully exploited known software vulnerabilities in fingerprint scanner
- Able to control information sent to and from the fingerprint scanner
- Went unnoticed by traditional anti-malware solutions
- If undetected, malicious actors would have gained access to physical machinery

Thank You