DARKTRACE ANTIGENA

AUTONOMOUS RESPONSE

TechDefcon (Defcon ISC Limited)
info@techdefcon.com www.techdefcon.com

Background & Growth

DARKTRACE

- Fundamental technology innovation
- Powered by machine learning and AI algorithms
- 7,000+ deployments worldwide
- Over 30 global offices
- Founded by world-leading mathematicians
- HQs in San Francisco, and Cambridge, UK

“Darktrace detects threats without having to define the activity in advance”

CIO, **City of Las Vegas**

"Darktrace has reduced the mean time to detect intrusions by 40%.”

Head of Cyber Defense, **Blackhawk Network**

Gartner 2015 CoolVendor

IET AWARDS The Institution of Engineering and Technology

Info Security Products Guide 2017 GLOBAL EXCELLENCE FINALISTS

WORLD ECONOMIC FORUM Technology Pioneer 2015

INVESTOR Allstars 2016

2017 BEST PRODUCT ENTERPRISE SECURITY SOLUTION CDM

Bloomberg Business Innovators 2016

CYBER SECURITY EXCELLENCE AWARDS WINNER 2017

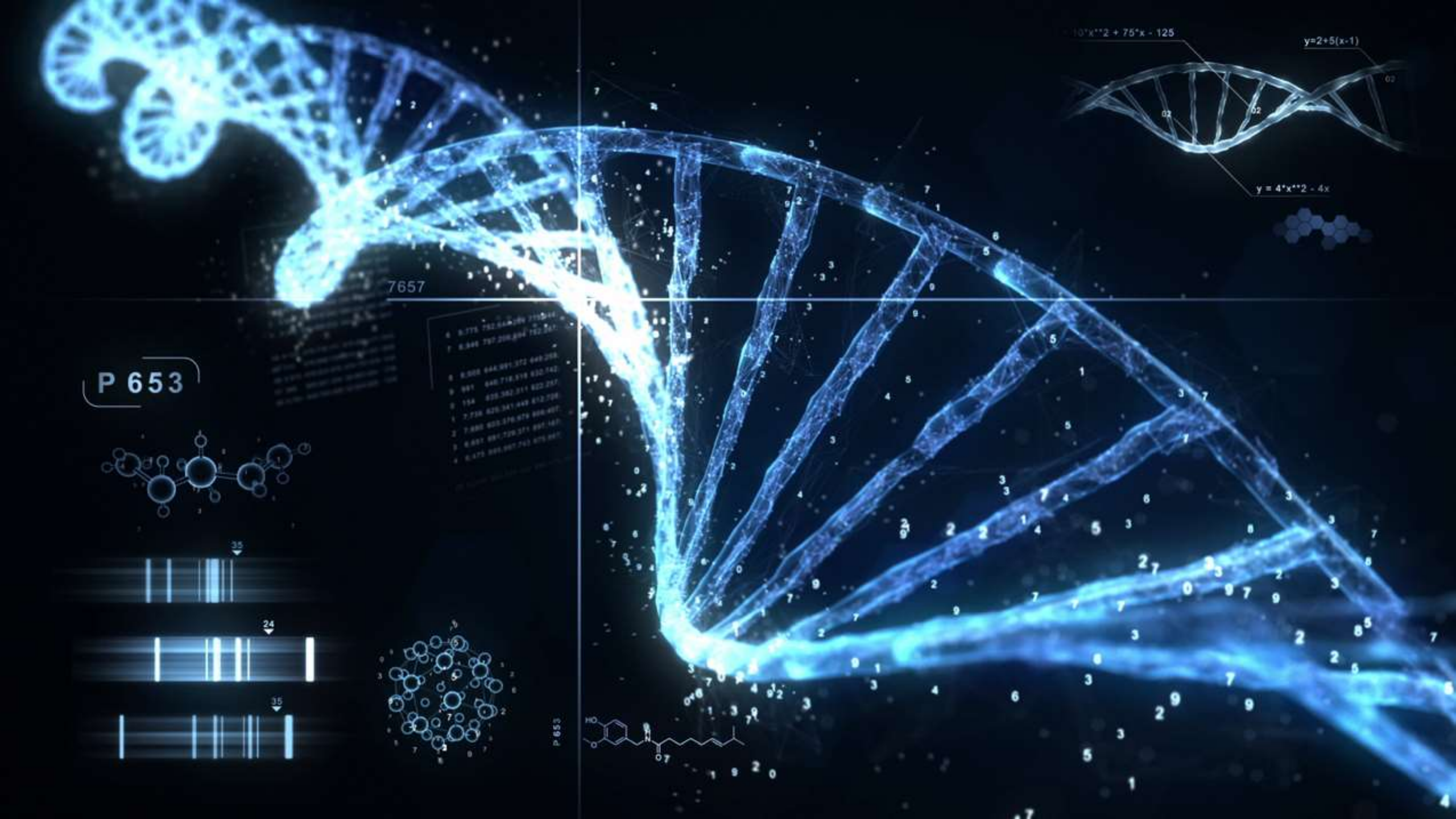
Over 7,000 Deployments: From SMEs to Global Banks

DARKTRACE

Evolving Threats in a New Business Landscape

- Business digital complexity is exploding:
  - Outsourced IT, SaaS, cloud, virtual, supply chain, IoT
- Not just website, DoS & credit card breaches
- Insider threat is constant – whether malicious or non-malicious
- Integrity of data is at risk
- Ransom attacks are fast and debilitating
- Smarter malware can change its capabilities when inside the business

Security teams cannot keep up with ever-increasing pace and complexity


y=2+5(x-1)
y = 4*x**2 - 4x
7657
P 653
35
24
35
P 653

Darktrace Antigena: Autonomous Response

DARKTRACE

Enterprise Immune System takes action

Extends Darktrace's proven AI technology by taking autonomous action

Adaptive mechanics

Takes targeted, proportionate, responsive action based upon activity and nature of threat

Time for humans to catch up

Slows down or stops attacks in real time, providing critical time for security teams to catch up

100% visibility

Integrates with the Threat Visualizer, API, alerting.

Across any digital architecture & devices

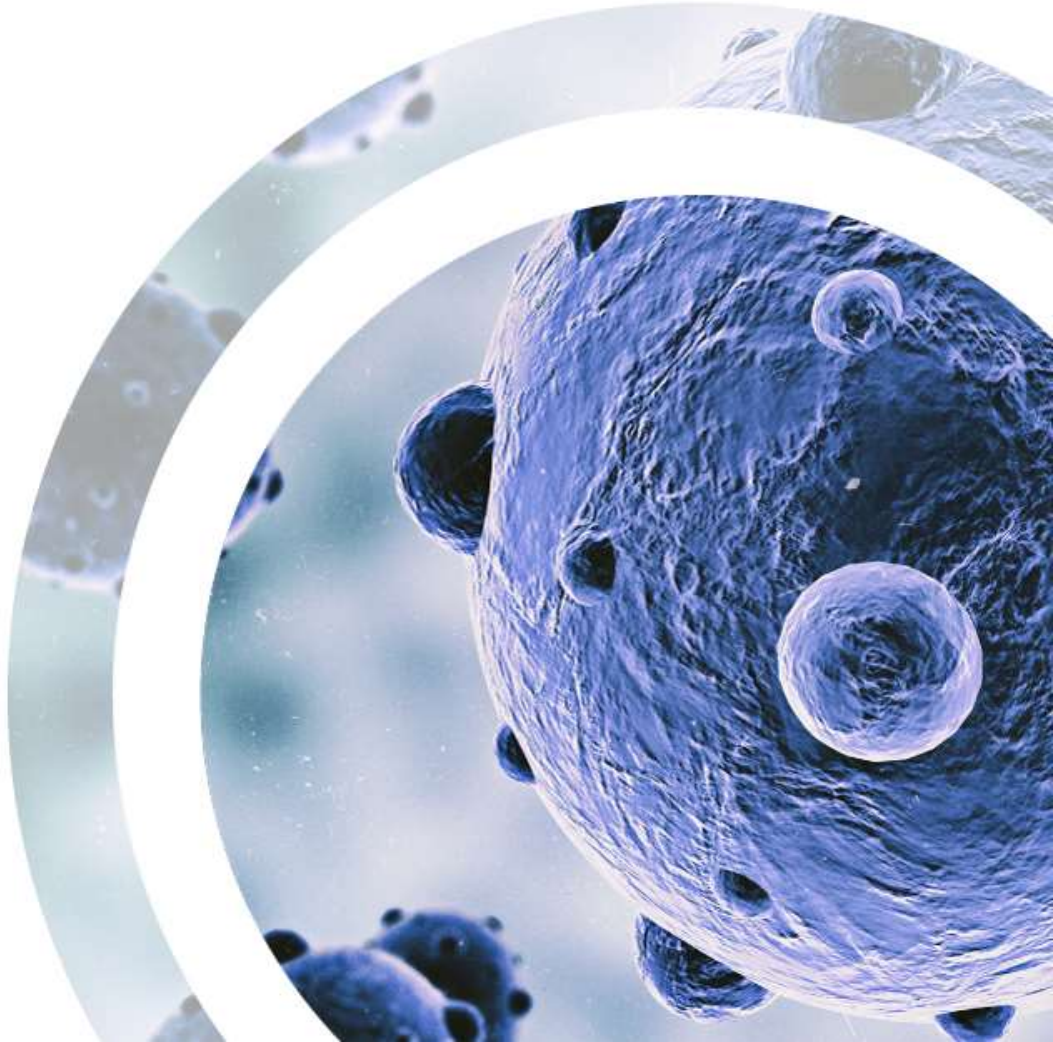
Works across physical and virtual environments: campus, datacentre, industrial, IoT, Cloud.

Darktrace Antigena Network

- Deployed worldwide across multiple industries
- Takes actions at the network level
  - Specifically disrupt targeted connections between source/destination pair
  - Enforce a device's normal 'pattern of life'
  - Buy security teams time
- Initially deployed in Human Confirmation Mode
- No additional hardware required

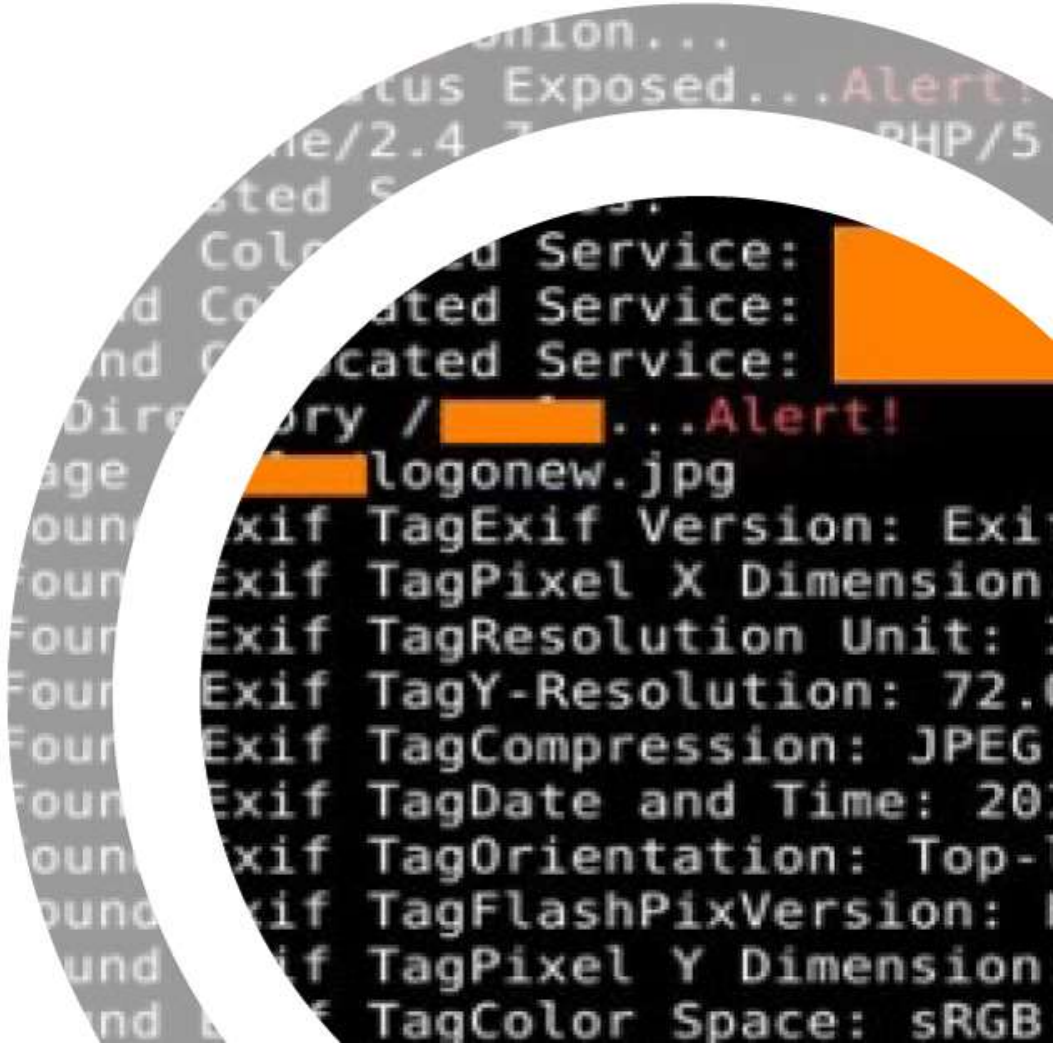
"Darktrace Antigena is the only automated cyber defense technology on the market that is capable of fighting the most important battles for us."

Michael Sherwood, CIO, **City of Las Vegas**



Case Study: Ransomware

- Abnormal activity detected
  - Talking to unusual domains
  - Querying Windows fileshare (SMB)
- Antigena suspected ransomware
- Real-time response
  - Suspect connections are stopped
  - Action taken within 15 seconds
  - Ransom demand averted



Darktrace Antigena Proof of Value

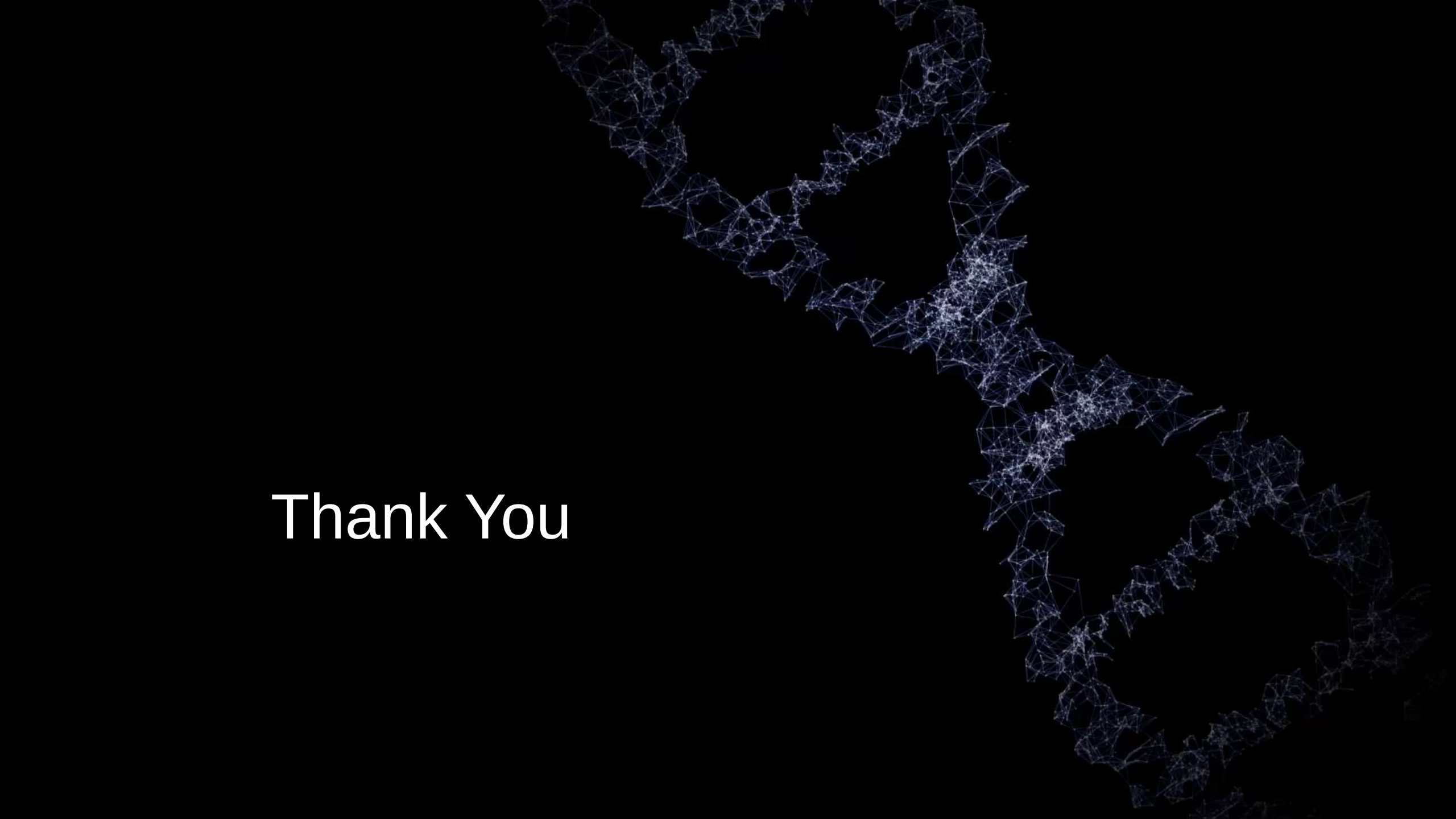
- No additional hardware, installed on existing Darktrace Appliance
- Installation can be performed remotely for environments opting for Call Home
- 3 week trial, no obligation
- Analysis of Darktrace Antigena's recommended actions
- Active Defense Reports from world-leading analysts

Conclusion

- Immune system technology is the first proven AI for cyber security
- Powered by machine learning and mathematics
- Self-learning & now self-defending
- Stops or slows threat whilst security team catches up
- Actions are measured and proportionate
- No disruption to normal business activity

“Antigena represents an important step… It’s evolving to an active defense that traditional systems cannot match.”

Michael Sherwood, CIO, **City of Las Vegas**


Thank You

Proof of Value Schedule

Schedule	Steps	Darktrace resource	Your company resource
Pre POV	• Installation of Antigena onto existing Darktrace appliance(s) • Human Confirmation Mode is activated; no Antigena modules are activated	Account Executive (AE), Cyber Technologist (CT)	Technical sponsor
Week 1	• First Active Defence Report	CT, AE	Technical sponsor
	• On-site Cyber Technologist testing and familiarization (optional) to deliberately trigger Antigena within your environment	CT	Technical sponsor
Week 2	• Second Active Defense Report	CT, AE	Technical sponsor, executive sponsor
	• Network module from Human Confirmation Mode to Active Mode	CT	Technical sponsor
Week 3	• Final Active Defense Report	CT, AE	Technical sponsor, executive sponsor
	• POV finishes	CT, AE	Technical sponsor, executive sponsor