Cyber AI: A New Era of Defence

Emily Orton, CMO, Darktrace

at 10th anniversary Cleanpower Smart Grids Conference 2019
www.cir-strategy.com/events

CNBC DISRUPTOR 50 2018

Forbes THE 2018 Cloud100

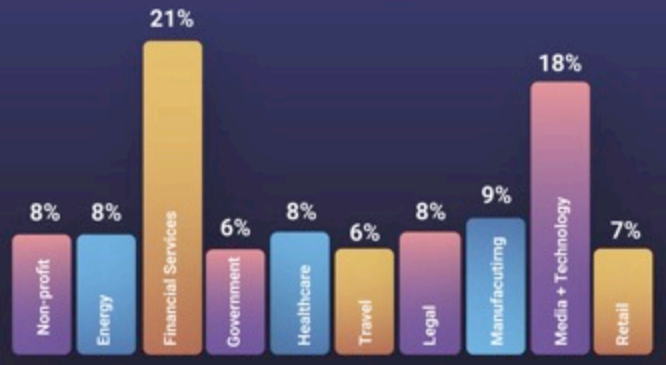
FT FINANCIAL TIMES 1000 Europe's Fastest Growing Companies 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD ★★★★★

DARKTRACE

DUAL HQs SAN FRANCISCO AND CAMBRIDGE, UK

CREATORS OF AUTONOMOUS RESPONSE



ACROSS ALL INDUSTRIES

$1.65 BN VALUATION

1,000 EMPLOYEES

44 OFFICES

$500M CONTRACT VALUE

DARKTRACE

ebay
Dreams
SUNCORP
bet365
Inphi
SAESL
DNK
MetroPath
Wesco Aircraft
Zpower
METRO BANK
Big West Oil
SingEx
HUNT&PALMER
BESPOKE AIR CHARTER
GEMFIELDS
charles river
TREK
SLAUGHTER AND MAY
summit DD
MACROSYNERGY
PARTNERS LLP
USPOWERGEN
Sackers
SUNSWEET
AIR MALTA
AXA
BT
IG
ocado
PEUGEOT
TAQA
Manchester Metropolitan University
LOS ANGELES LGBT CENTER
Arsene
RLC
HUMAN LONGEVITY, INC.
British Land
PRUDENTIAL
THE CHURCH OF ENGLAND
Dædalus Books
HUDSON PACIFIC PROPERTIES
SCIENCE MUSEUM GROUP
The Royal Mint MUSEUM
NW BROWN GROUP LIMITED
Public Health England
TRJ TÉLÉCOM
SuMi TRUST
drax
BASSADONE
Bunim/Murray Productions
FALCON GROUP
JACKSON
T-Mobile
Belfast Harbour
EVERSHOLT RAIL GROUP
Coca-Cola EUROPEAN PARTNERS
IM irwinmitchell solicitors
LEERINK
TRUCKEE DONNER PUBLIC UTILITY DISTRICT
POOL RE
spillman technologies, inc.
William HILL
IPREO
DAC beachcroft
International Baccalaureate
SHAWBROOK
Steelcase
open energi
KOHL'S
Mariner's Bank
StarTribune
paybay
DIRECTV
Allianz
Penguin Random House
CAMPARI
MACOM
SpencerStuart
PACIFIC DENTAL SERVICES
MARITIME NEW ZEALAND
SNS Bank
TruWest CREDIT UNION
STARHOTELS
Lanyon Bowdler SOLICITORS
Teachers Building Society
photobox
JUMEIRAH GROUP
TeleChoice
TSB Bank expect more
ShookLin&Bok
Kingston
BNP PARIBAS
SUZUKI
GROUP 1 AUTOMOTIVE
DOLPHIN ENERGY
CenterParcs
make MY trip
CORDENPHARMA
BRICK COURT CHAMBERS BARRISTERS
EDISON MISSION ENERGY
BLACKHAWK NETWORK
32Red online casino
Moneris SOLUTIONS
Saga
spoor • fisher
EPIC
elite insurance
UST Global
SB Simply Business
COLONIAL GROUP INTERNATIONAL
sodexo
The GLENMORANGIE COMPANY
session
AIRLINK
neustar
nominet
ALMA BANK
DENVER HEALTH
OCEAN FIRST
Plextek
TELSTRA
AIG
KEEN
Birmingham Airport
National Life Group
ADDISON LEE
ASTON MARTIN
QUICKPLAY
EPIC SCIENCES
Arbutus BIOPHARMA
TheCityUK
NORTHSIDE HOSPITAL FOUNDATION
Aqua
Massmart
AEGON Sony Life
Zappos
Catholic Charities of Santa Clara County
K&L GATES
APA NOVA
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Cyber Security: The Challenge

DARKTRACE

- Complexity: outsourced IT, cloud, supply chain, IoT
- Convergence of IT and OT environments
- Threat landscape getting more sophisticated
  - Nation state & criminal
  - Insider threat and misconfigurations
- Attacks move at machine speed
- Human teams overwhelmed

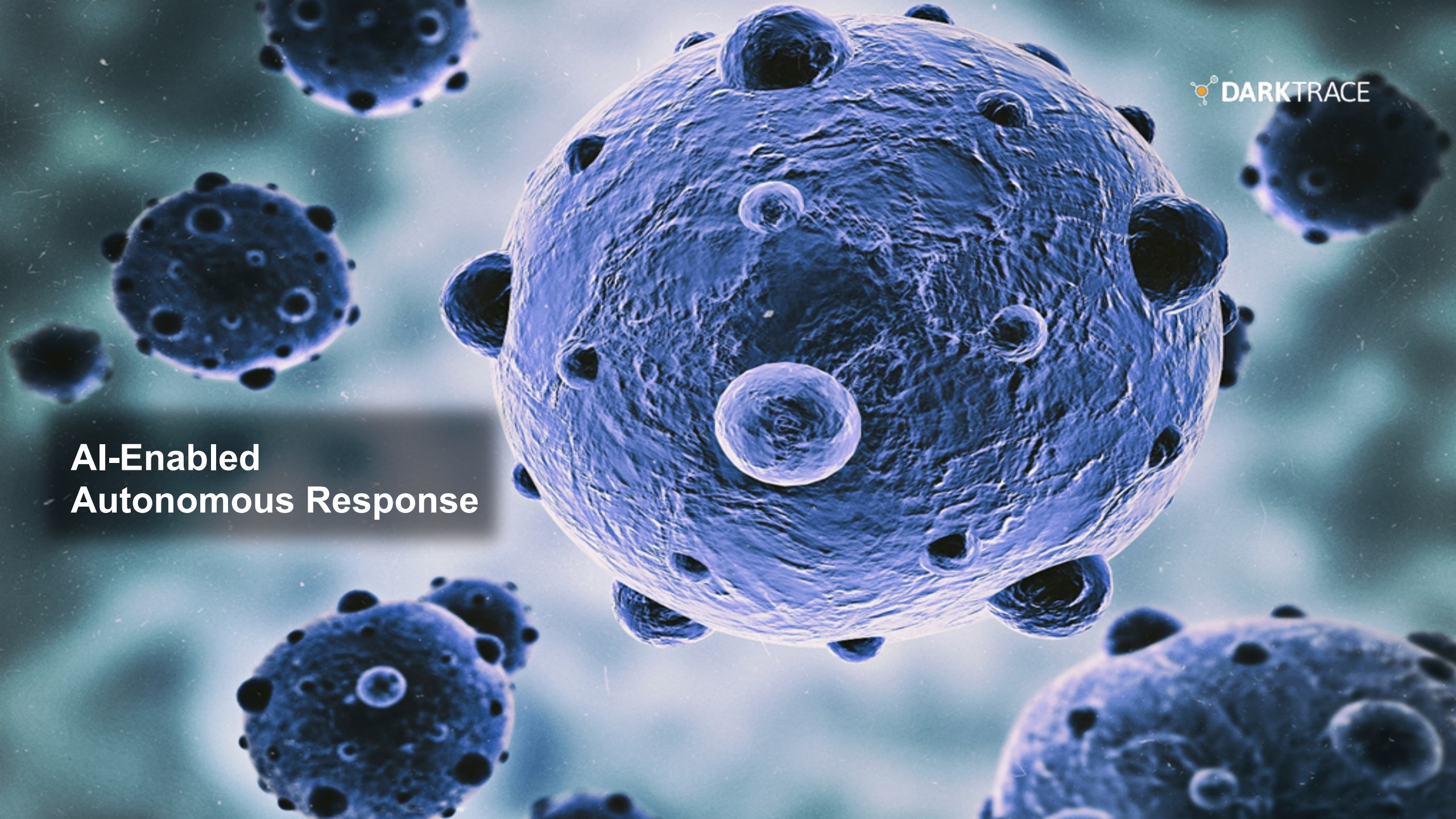
Legacy security is constantly outpaced.
The battleground is *inside.*

DARKTRACE

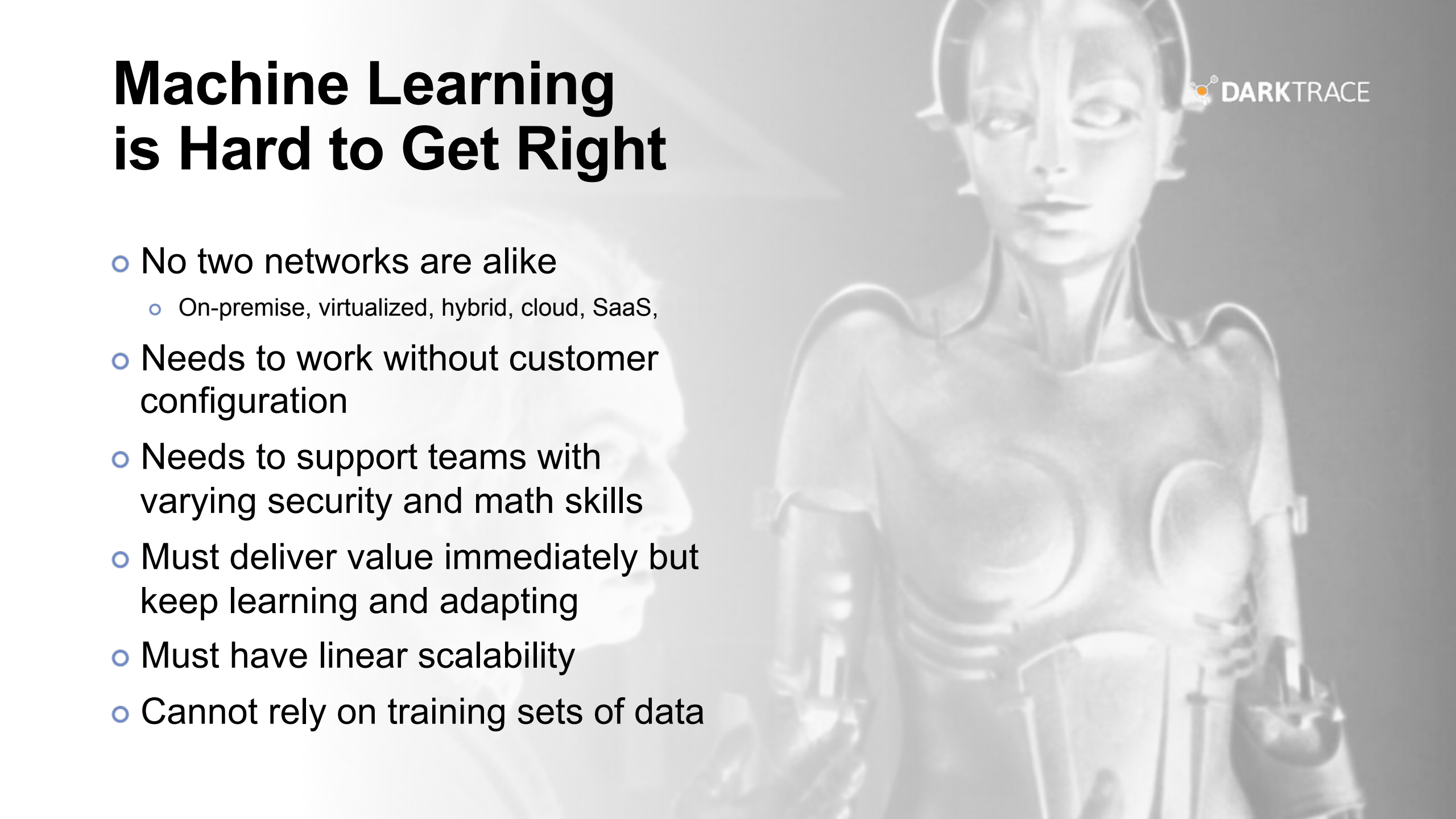
CYBER AI PLATFORM

AUTONOMOUS RESPONSE

The Enterprise Immune System


DARKTRACE
AI-Enabled
Autonomous Response

Machine Learning is Hard to Get Right



- No two networks are alike
  - On-premise, virtualized, hybrid, cloud, SaaS,
- Needs to work without customer configuration
- Needs to support teams with varying security and math skills
- Must deliver value immediately but keep learning and adapting
- Must have linear scalability
- Cannot rely on training sets of data

Intellectual Property Targeted by Malware

DARKTRACE

Point of entry:
Disguised malicious document

Objective:
Encrypt crucial system files and spread to subsequent victims

Anomalous activity:
Connections to a rare external destination, while trying to move laterally to other areas of the corporate network

- Malware designed to target intellectual property disguised in email as invoice
- Employee unintentionally downloaded fast-acting malware
- Darktrace Antigena responded preventing spread of malware to the assembly line

Video Conferencing Camera Attack

Point of entry:
Video Conference Camera

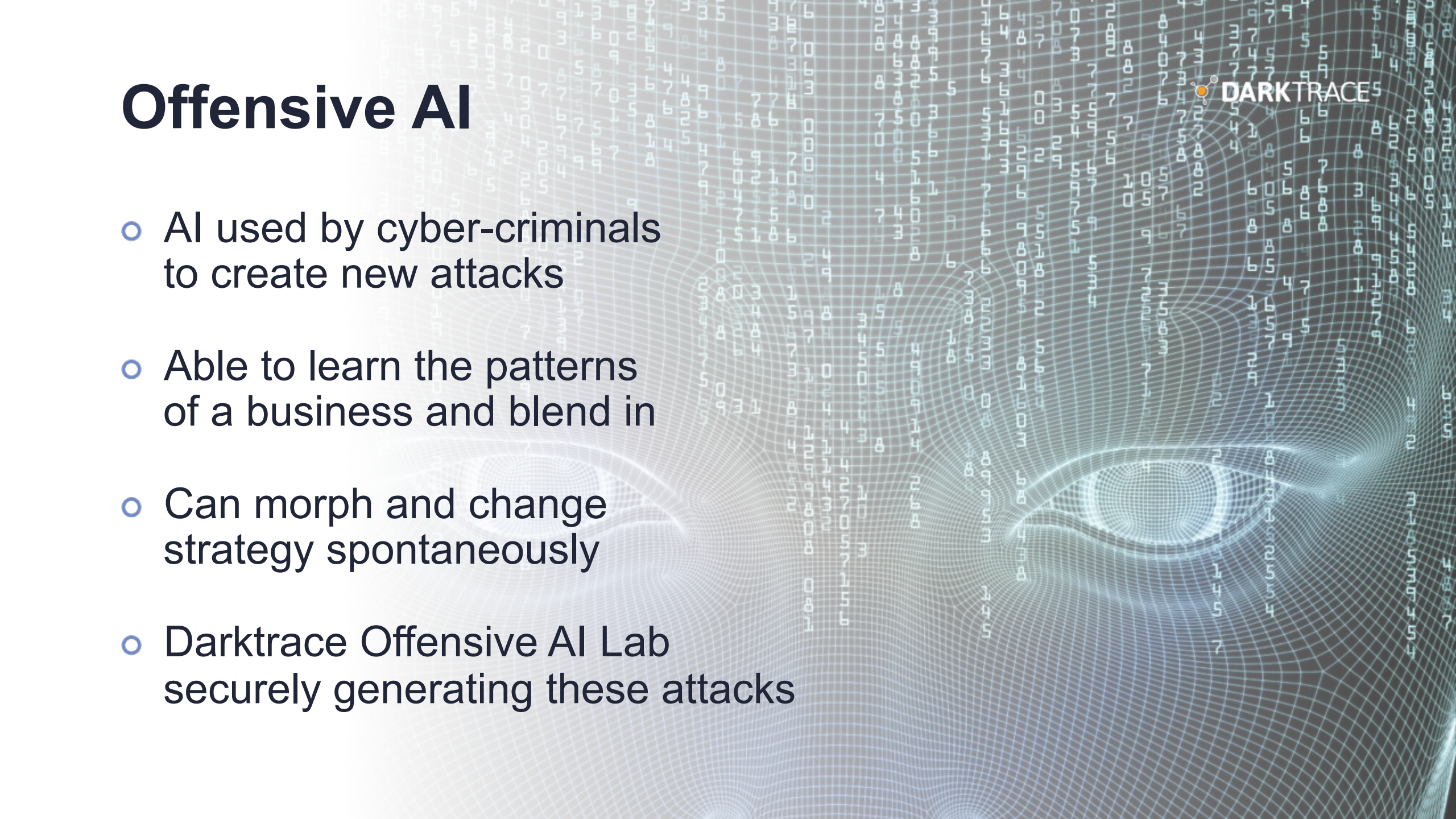
Objective:
Transmit data out of host network

Anomalous activity:
Video conferencing camera was transmitting data outside the network

- Attacker was aiming to either steal corporate information or take remote control of the device to launch a DDoS attack on another network
- Would not have been detected through signature-based defences – the activity was not inherently malicious
- Malware designed to target intellectual property disguised in email as invoice

Offensive AI

- AI used by cyber-criminals to create new attacks
- Able to learn the patterns of a business and blend in
- Can morph and change strategy spontaneously
- Darktrace Offensive AI Lab securely generating these attacks



DARKTRACE

When cyber-attackers employ AI as part of their attacks, cyber defenses will have to be capable of response.

Fast-moving and changing attacks will require defenses that move just as quickly, using AI and automation to augment the human.

FORRESTER®

Thank you