CHECK POINT™

HEALTHCARE UNDER SEIGE

KEY SECURITY CHALLENGES FOR HOSPITALS, CLINICS, AND MEDICAL CENTERS

Kev Hau | Head of Security Engineering

Cyber Security Evangelist, Office of CTO

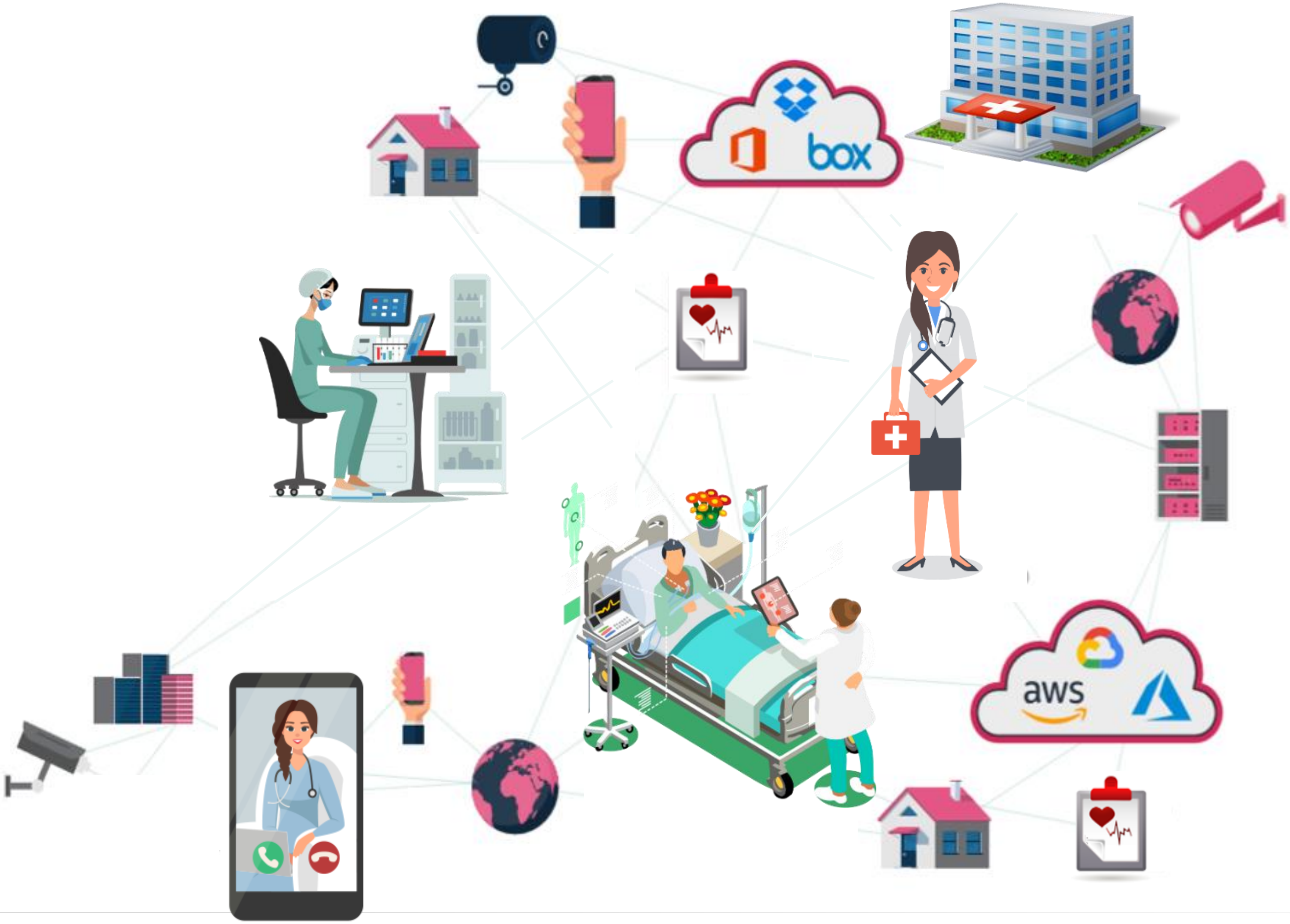
YOU DESERVE THE BEST SECURITY

THE HOSPITAL ENVIRONMENT IS CHANGING

ATTACK SURFACES ARE WIDENING

HOSPITALS YESTERDAY

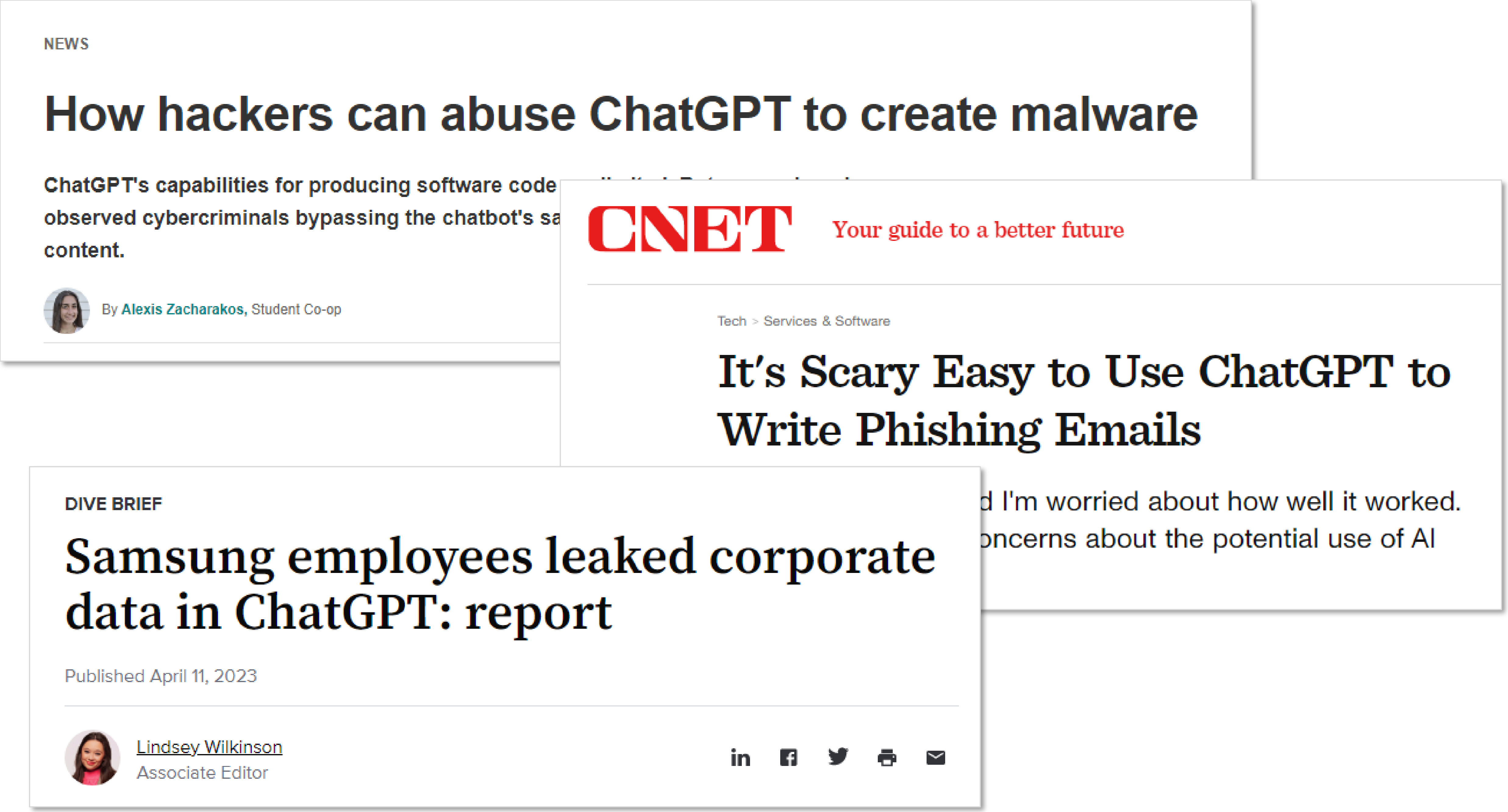
HOSPITALS TODAY



TECHNOLOGIES ADOPTION IN HEALTHCARE

- Network-connected medical devices
- Medical IoT such as wearable health devices
- 5G-enabled remote healthcare
- Mobile devices access
- Cloud and Big Data Analytics, and AI
- Blockchain Technology

2023
THE YEAR OF AI



NEWS

How hackers can abuse ChatGPT to create malware

ChatGPT's capabilities for producing software code

observed cybercriminals bypassing the chatbot's sa

content.

By Alexis Zacharakos, Student Co-op

CNET Your guide to a better future

Tech > Services & Software

It's Scary Easy to Use ChatGPT to Write Phishing Emails

d I'm worried about how well it worked.

oncerns about the potential use of AI

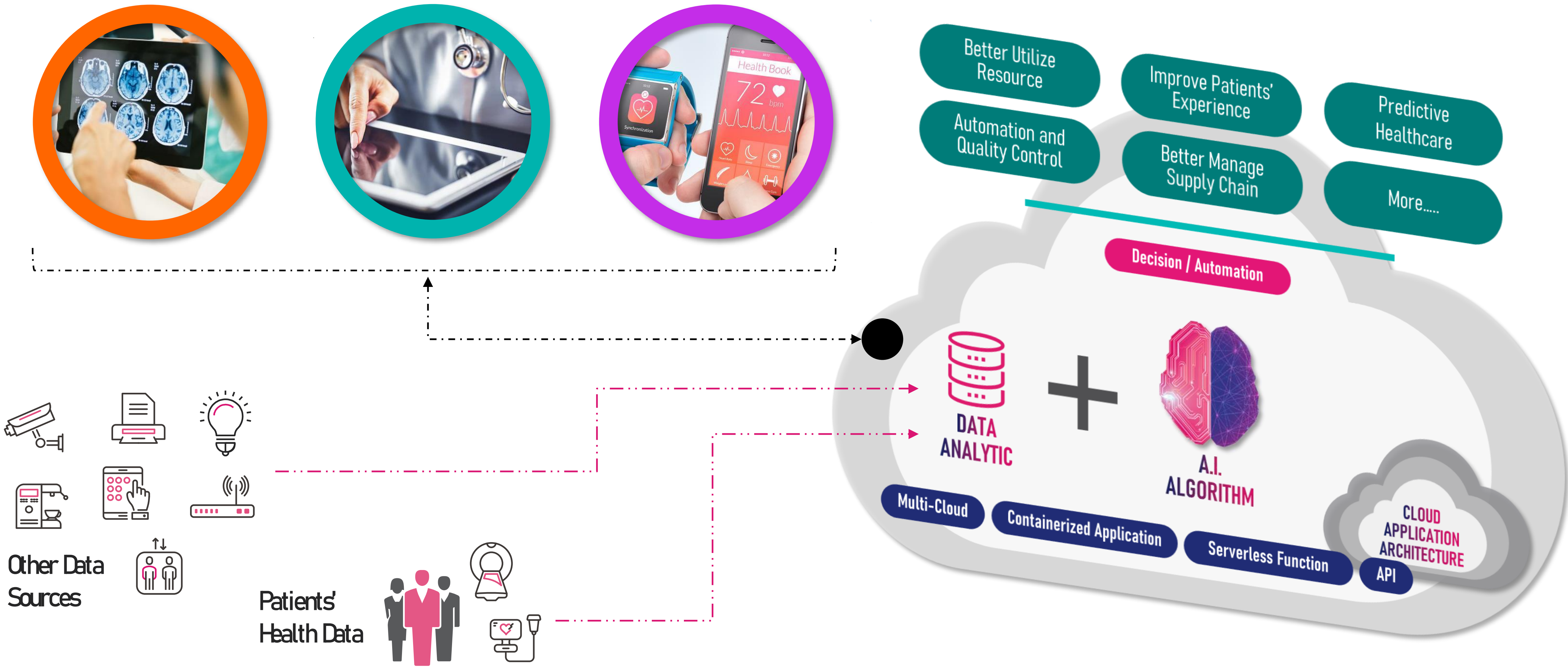
DIVE BRIEF

Samsung employees leaked corporate data in ChatGPT: report

Published April 11, 2023

Lindsey Wilkinson
Associate Editor

DATA-DRIVEN HEALTHCARE PLATFORM



Better Utilize Resource

Improve Patients' Experience

Predictive Healthcare

Automation and Quality Control

Better Manage Supply Chain

More.....

Decision / Automation

DATA ANALYTIC

A.I. ALGORITHM

Multi-Cloud

Containerized Application

Serverless Function

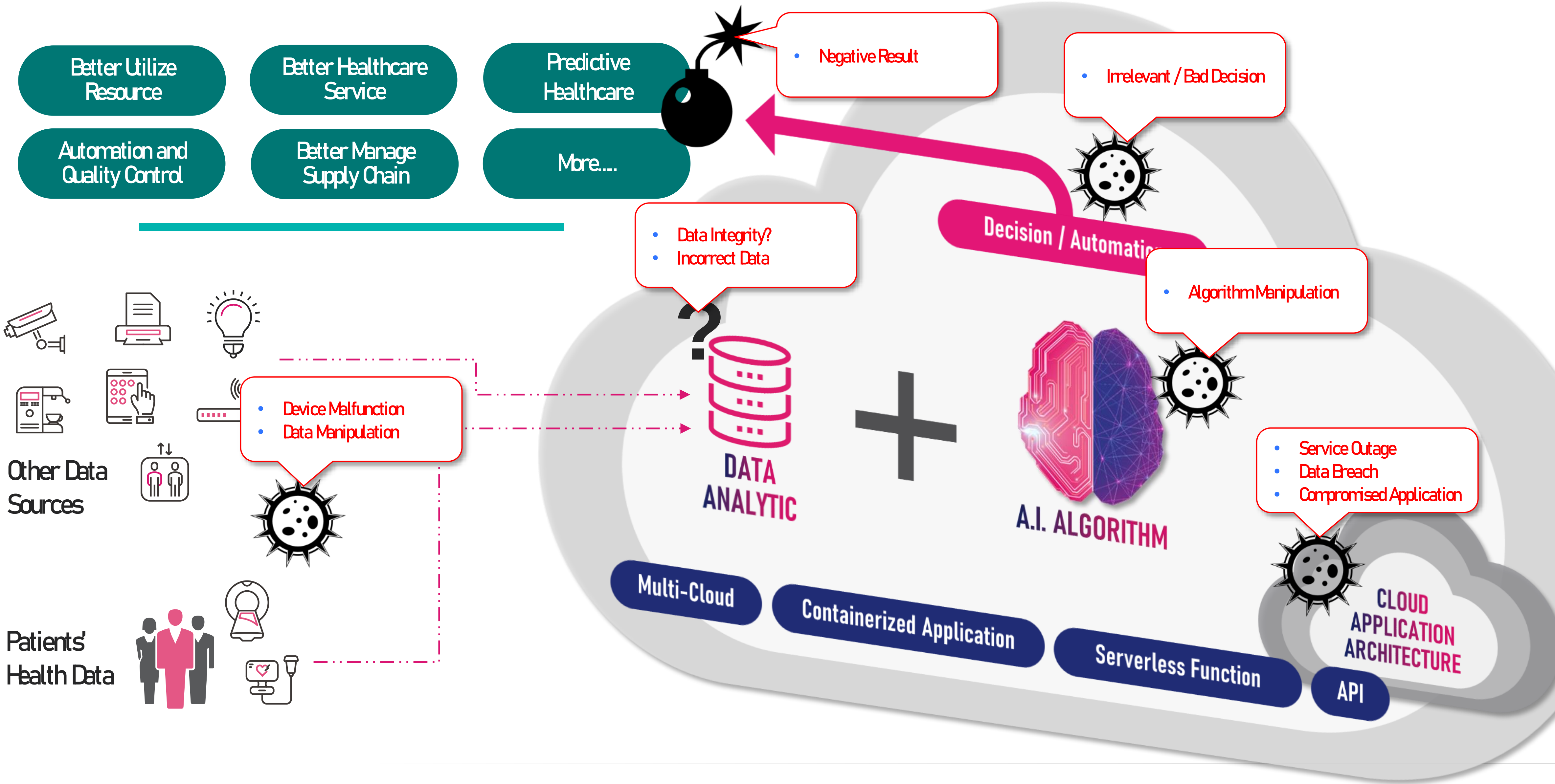
CLOUD APPLICATION ARCHITECTURE

API

Other Data Sources

Patients' Health Data

THE RISKS.......



- Better Utilize Resource
- Better Healthcare Service
- Predictive Healthcare
- Automation and Quality Control
- Better Manage Supply Chain
- More....

- Negative Result

- Irrelevant / Bad Decision

- Data Integrity?
- Incorrect Data

- Algorithm Manipulation

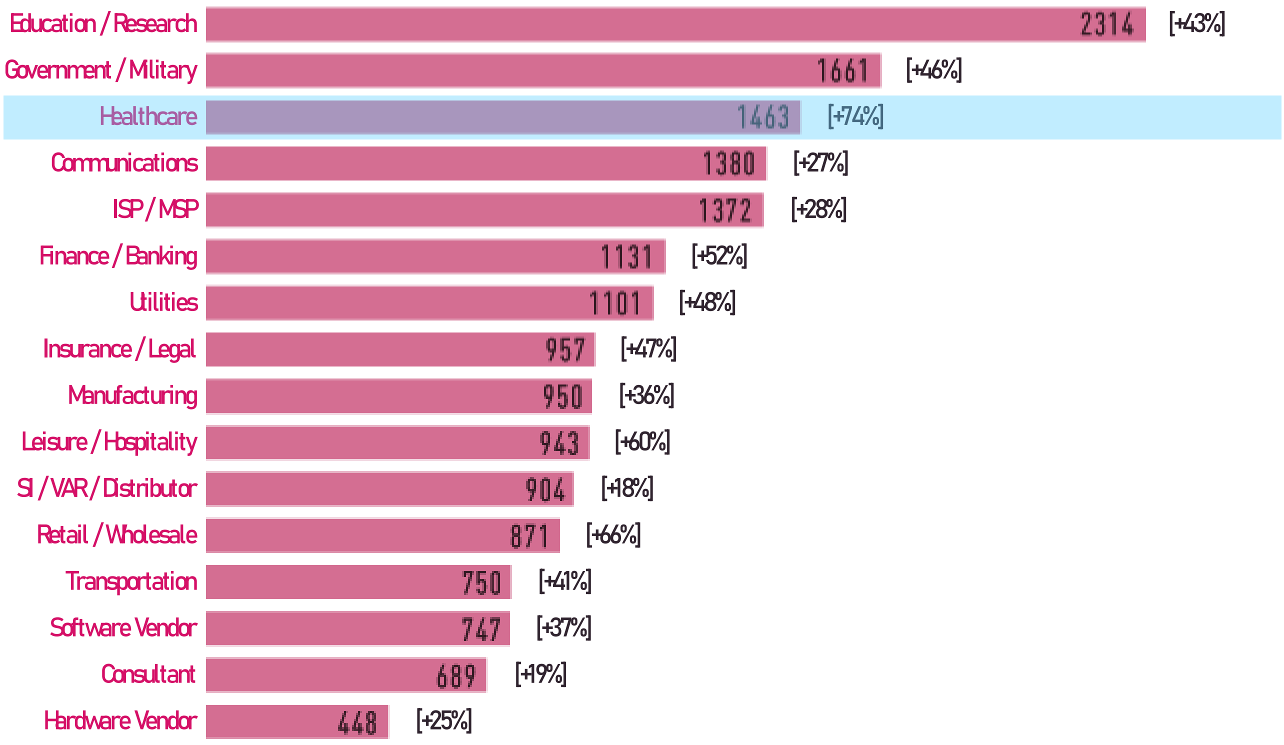
- Device Malfunction
- Data Manipulation

- Service Outage
- Data Breach
- Compromised Application

AVERAGE WEEKLY ATTACKS PER ORGANIZATION BY INDUSTRY 2022, COMPARED TO 2021

CYBER
SECURITY
REPORT

2023



Global Average of weekly attacks per organization by Industry in 2022 [% of change from 2021]

SECURITY THREATS TO HEALTHCARE INSTITUTIONS

Community Health Systems Impacted by Data Breach Tied to GoAnywhere MFT Vulnerability

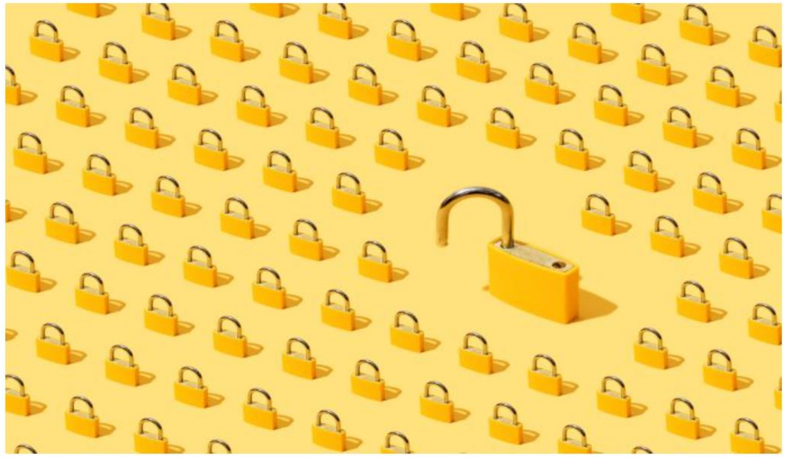
In an SEC filing, Community Health Systems, one of the country's largest healthcare providers, disclosed a third-party data breach involving Fortra's GoAnywhere managed file transfer solution that impacted one million individuals.

Highmark Health Suffers Phishing Attack, 300K Individuals Impacted

Highmark Health notified 300,000 individuals of a phishing attack that potentially compromised protected health information.

Maryland Hospital Suffers Ransomware Attack

Atlantic General Hospital is currently investigating a ransomware attack that occurred earlier this week.



WHY HEALTHCARE INSTITUTIONS ARE BEING TARGETED?

PH has higher value than PII

Connected medical devices are easy to hack

Hacktivist groups

DATA IS THE NEW OIL IN 21ST CENTURY

$1,000

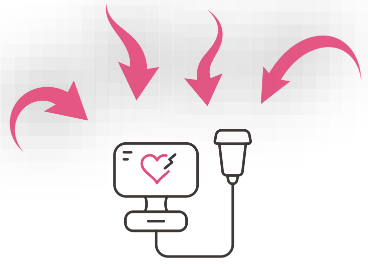
Average value of a medical record on the darknet

Credit card information and PII sell for $110*

MEDICAL IOT ASSETS ARE INHERENTLY VULNERABLE

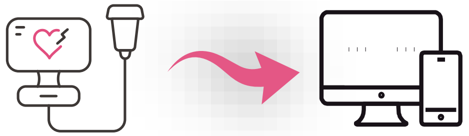
- Run on Legacy OS
- Difficult to Patch
- No Built-in Security
- **** Unchanged Password

EXPLOIT
IOT VULNERABILITIES



Risk to IOT Devices

Manipulation, Downtime, Damage



Network Backdoor

Lateral movement to other network elements

CYBERSECURITY IS NOT SOMETHING; IT IS EVERYTHING TODAY

SECURING MEDICAL CENTERS, HOSPITALS AND CLINICS

Key
Security
Challenges

Ransomware / Advanced Threat
blocking, containing and remediating

Connected devices
securing IoMT to protect the network

Protecting data and records
in the cloud

Enabling medical staff
with secured internet access from anywhere

Protecting patients
when they are using medical services

PROTECT CONNECTED MEDICAL DEVICES

VISIBILITY

- Device Type and Nature
- Device Security Flaw
- Communication Flow
- Network Threat Detection

- Devices Discovery Engine
- Firmware Security Assessment
- Network Threat Detection

ENFORCEMENT

- Zero Trust Access Control
- Threat Prevention
- Virtual Patching
- Device Run-time Protection

- Network Security
- Nano Agent

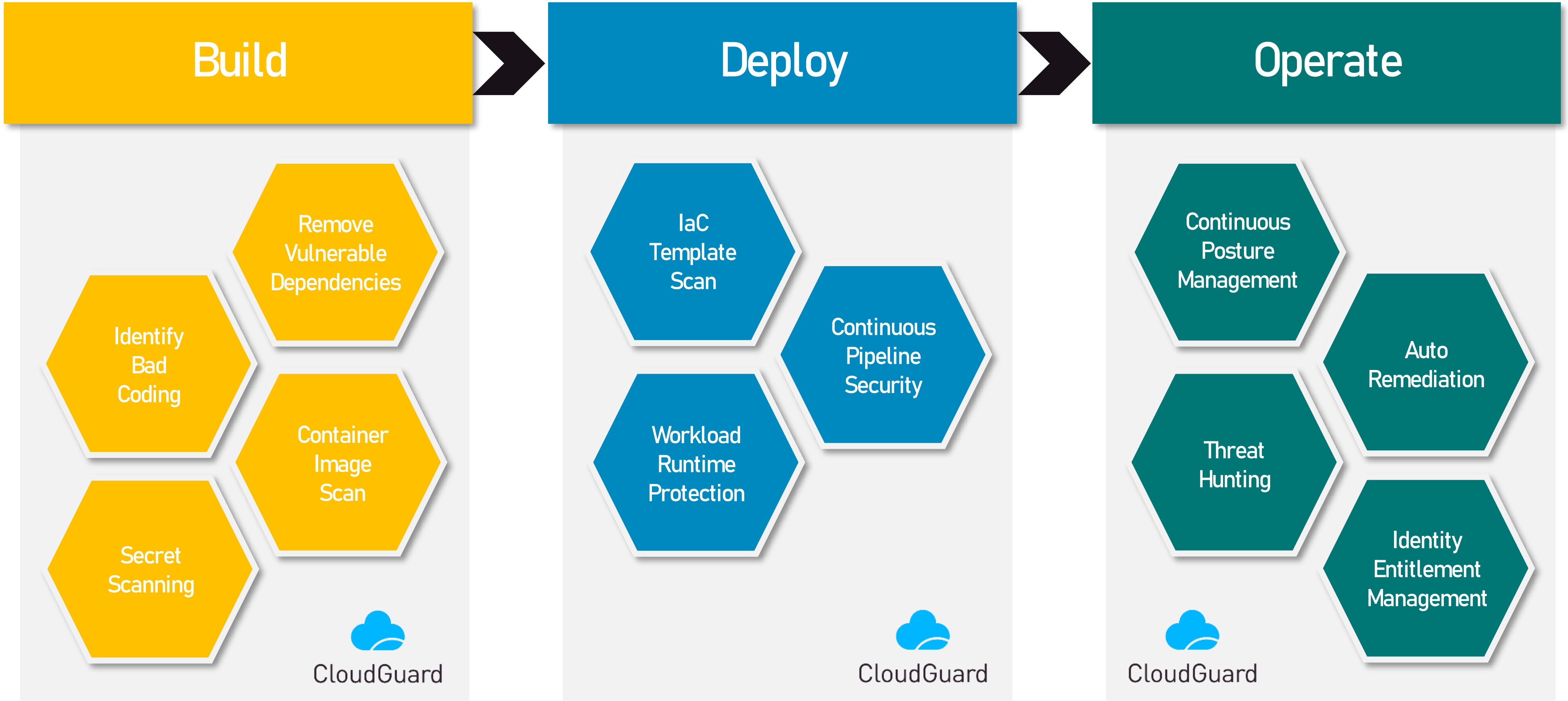
RESPONSE

- Automated Triage
- Incident Investigation
- Automated Response
- Expertise

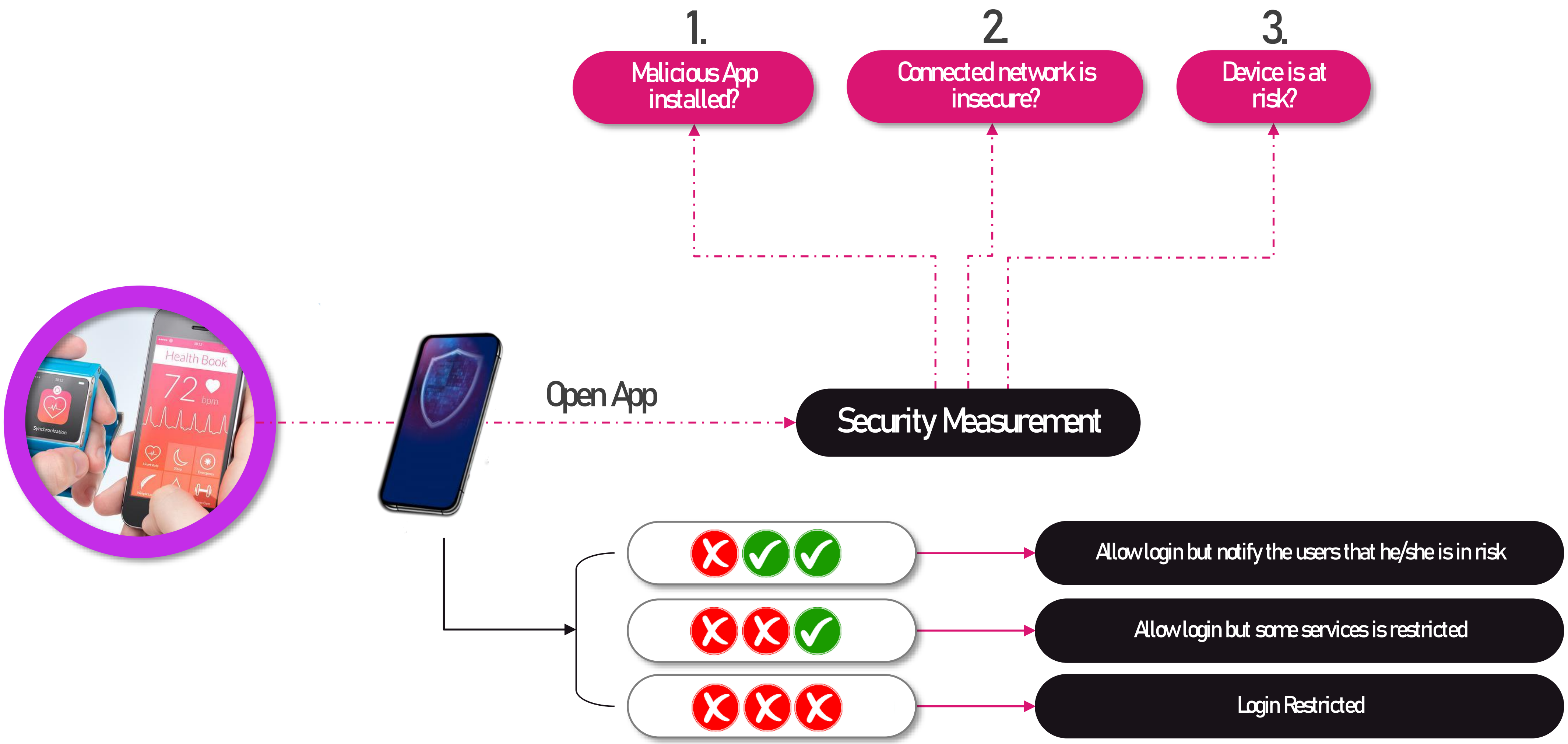
- AI-Powered Analysis – XDR
- Incident Response Team

PROTECT THE CLOUD APPLICATION

Security measurement at every stage of SDLC with CloudGuard



PROTECTING PATIENTS
WHEN THEY ARE USING MEDICAL SERVICES



1. Malicious App installed?

2. Connected network is insecure?

3. Device is at risk?

Open App

Security Measurement

✗ ✓ ✓	Allow login but notify the users that he/she is in risk
✗ ✗ ✓	Allow login but some services is restricted
✗ ✗ ✗	Login Restricted

CHECKPOINT INFINITY PRINCIPLES

COMPREHENSIVE

CONSOLIDATED

COLLABORATIVE

PREVENTION FIRST

ACCURATE VERDICT = PRECISE PREVENTION

THREATCLOUD

THE BRAIN BEHIND CHECK POINT'S POWER

AI Technology

Infected hosts detection
Sandbox static analysis
Sandbox dynamic analysis

Email static analysis
Mobile zero-phishing detection
Anti-Phishing AI engine

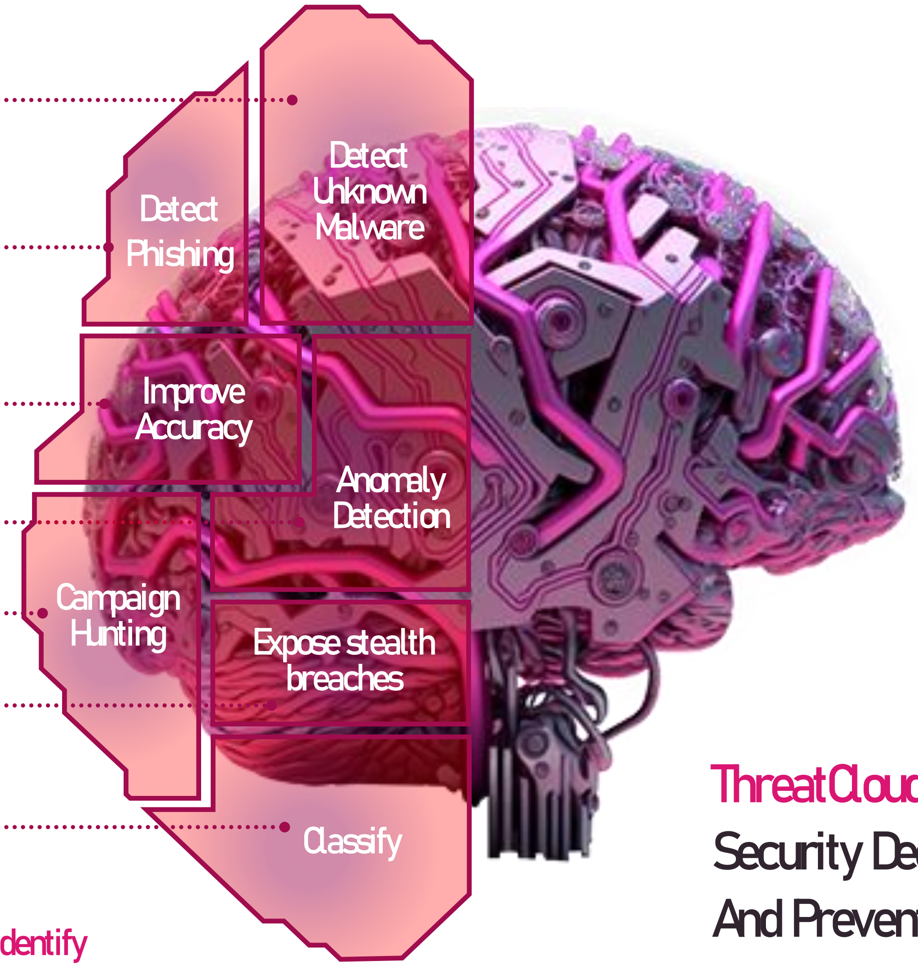
Network AI engines aggregator
Mobile AI engines aggregator
Machine validated signature

Cloud networks anomaly detection

ThreatCloud Campaign Hunting

Analyst Mind
Malicious activity detection

Documents meta classifier Vectorization family classifier
ML Similarity Model
MRAT Classifier



Detect Unknown Malware

Detect Phishing

Improve Accuracy

Anomaly Detection

Campaign Hunting

Expose stealth breaches

Classify

40+ AI and Machine Learning technologies that identify and block emerging threats that were never seen before

Big Data Threat Intel

Always acquires the most recent IoCs and protections of latest attacks seen in the wild

150,000 Connected networks

Millions of Endpoint devices

2,000,000,000 Websites and files inspected daily

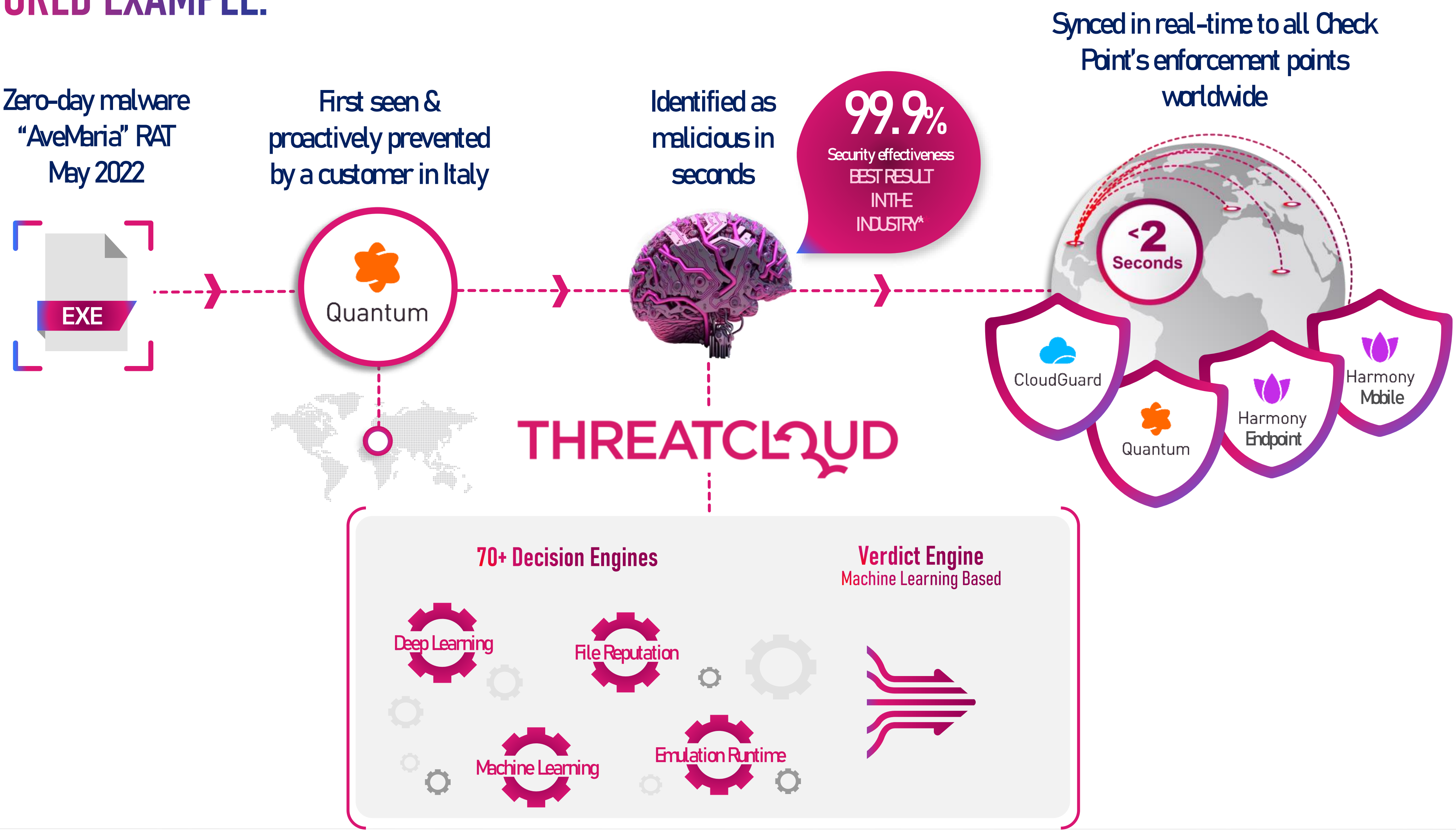
Dozens of external feeds and crawling the www and social media

Unique ML algorithms detecting 650,000 suspicious domains daily

ThreatCloud Makes 2 Billion
Security Decisions Every Day
And Prevents 2.5 Billion attacks every year!

THE POWER OF REALTIME SHARED INTELLIGENCE

REAL WORLD EXAMPLE:



Zero-day malware "AveMaria" RAT May 2022

First seen & proactively prevented by a customer in Italy

Identified as malicious in seconds

99.9% Security effectiveness BEST RESULT IN THE INDUSTRY*

Synced in real-time to all Check Point's enforcement points worldwide

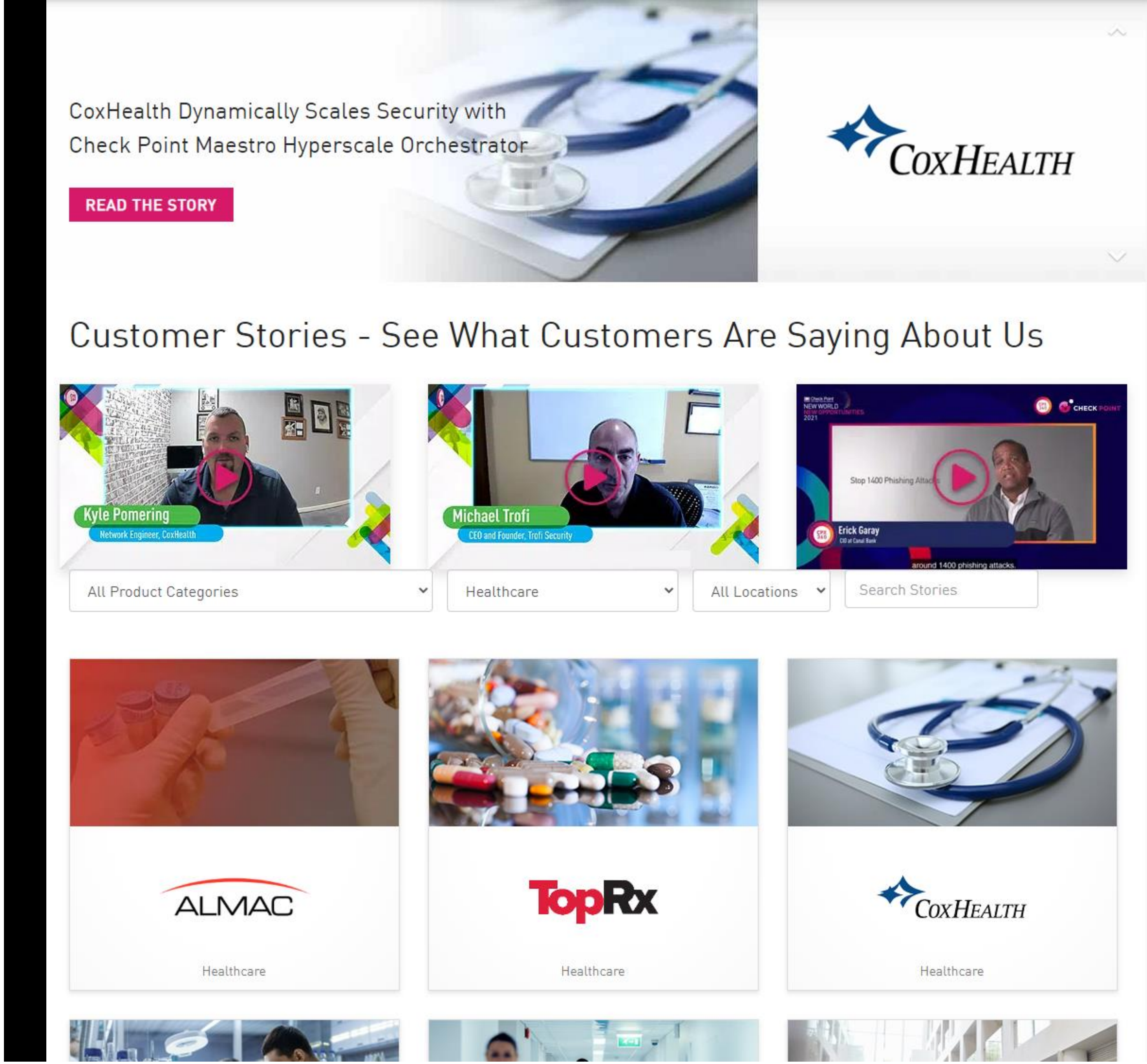
70+ Decision Engines

Verdict Engine

Machine Learning Based

CHECK POINT CUSTOMER STORIES

https://www.checkpoint.com/customer-stories/ -



CoxHealth Dynamically Scales Security with Check Point Maestro Hyperscale Orchestrator

Customer Stories - See What Customers Are Saying About Us

CHECK POINT™

THANK YOU

YOU DESERVE THE BEST SECURITY