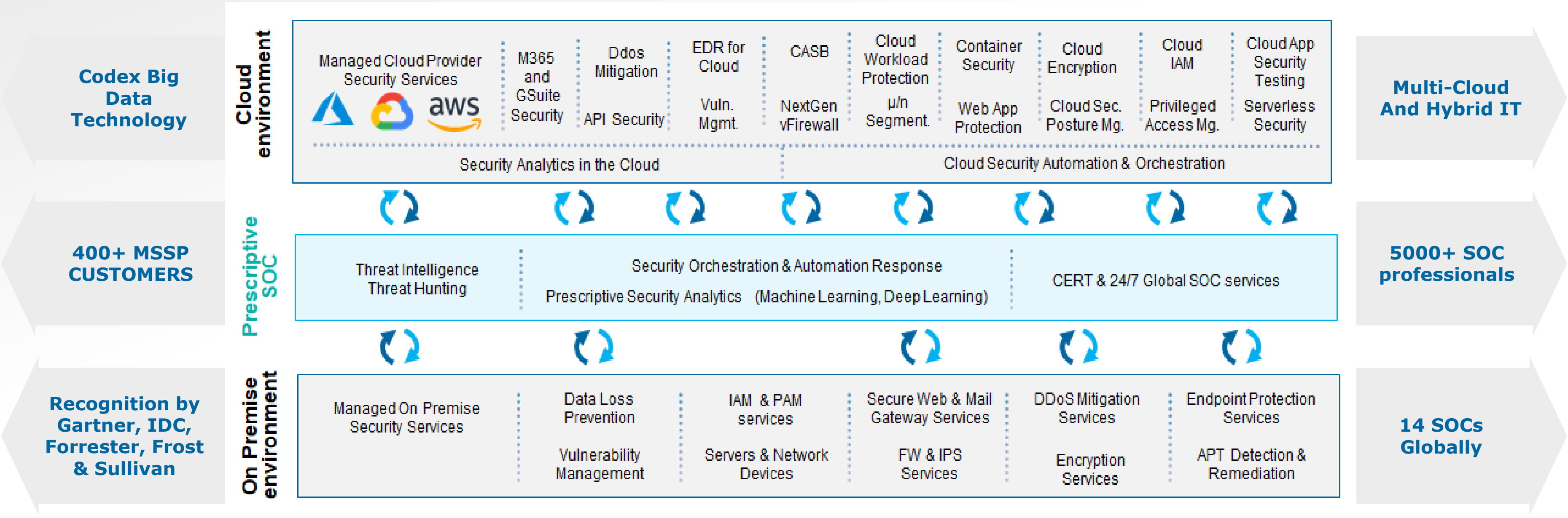
Genesis of **Atos MDR**

Farah Rigal
Global SOC Transformation Program Director

Vinod Vasudevan
Paladion Co-Founder & CTO

Atos Prescriptive SOC in the heart of Hybrid Cloud Security

Trust through a single pane of glass



Codex Big Data Technology

400+ MSSP CUSTOMERS

Recognition by Gartner, IDC, Forrester, Frost & Sullivan

Cloud environment

Managed Cloud Provider Security Services

M365 and GSuite Security

Ddos Mitigation

API Security

EDR for Cloud

Vuln. Mgmt.

CASB

NextGen vFirewall

Cloud Workload Protection

µ/n Segment.

Container Security

Web App Protection

Cloud Encryption

Cloud Sec. Posture Mg.

Cloud IAM

Privileged Access Mg.

Cloud App Security Testing

Serverless Security

Security Analytics in the Cloud

Cloud Security Automation & Orchestration

Prescriptive SOC

Threat Intelligence
Threat Hunting

Security Orchestration & Automation Response

Prescriptive Security Analytics (Machine Learning, Deep Learning)

CERT & 24/7 Global SOC services

On Premise environment

Managed On Premise Security Services

Data Loss Prevention

Vulnerability Management

IAM & PAM services

Servers & Network Devices

Secure Web & Mail Gateway Services

FW & IPS Services

DDoS Mitigation Services

Encryption Services

Endpoint Protection Services

APT Detection & Remediation

Multi-Cloud And Hybrid IT

5000+ SOC professionals

14 SOCs Globally

Paladion MDR

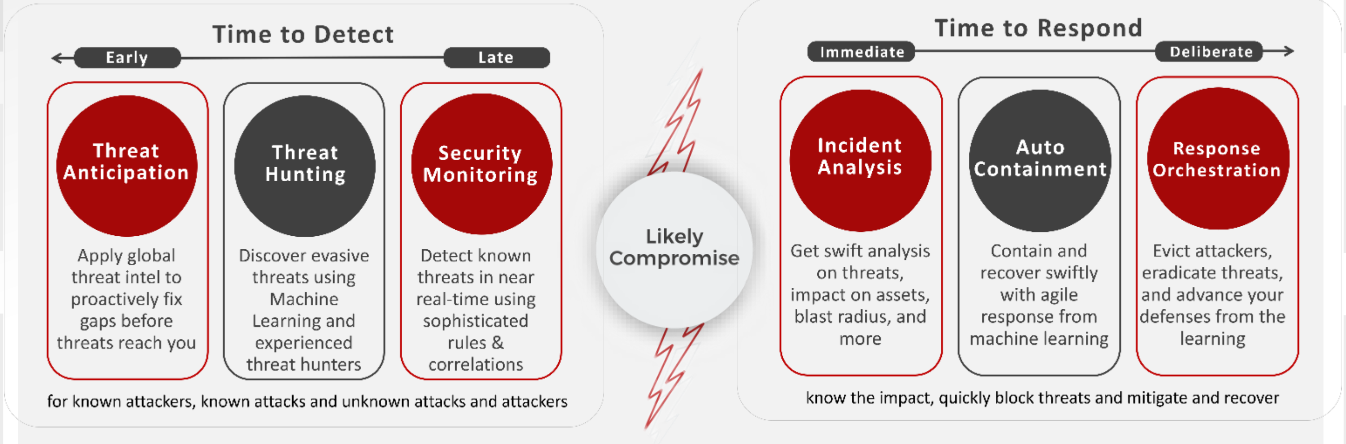
Patented AI Technology

AIsaac

100+ MDR CUSTOMERS

Recognition by Gartner, IDC, Forrester, Frost & Sullivan

Left-of-Hack to Right-of-Hack Services SM



Time to Detect

Early ← → Late

Threat Anticipation: Apply global threat intel to proactively fix gaps before threats reach you

Threat Hunting: Discover evasive threats using Machine Learning and experienced threat hunters

Security Monitoring: Detect known threats in near real-time using sophisticated rules & correlations

for known attackers, known attacks and unknown attacks and attackers

Likely Compromise

Time to Respond

Immediate → Deliberate

Incident Analysis: Get swift analysis on threats, impact on assets, blast radius, and more

Auto Containment: Contain and recover swiftly with agile response from machine learning

Response Orchestration: Evict attackers, eradicate threats, and advance your defenses from the learning

know the impact, quickly block threats and mitigate and recover

Cloud Native Multi-Cloud And Hybrid IT

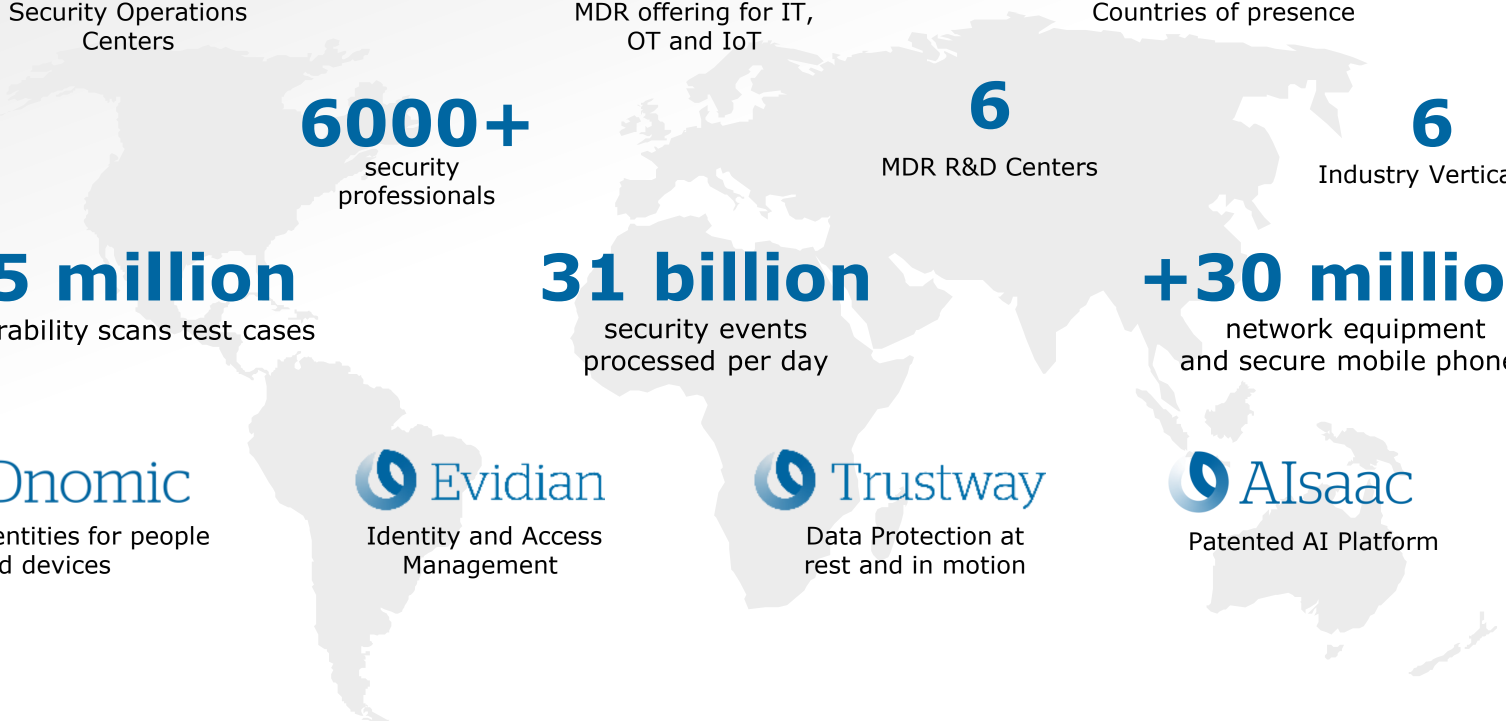
400+ SOC professionals

4 SOCs Across US, ME and India

Paladion Joins Atos
Leading the way in Managed Detection and Response

Trusted partner for your **Digital Journey**

The Genesis of Atos MDR – We bring scale with innovation



15
Security Operations Centers

1
MDR offering for IT, OT and IoT

73
Countries of presence

6000+
security professionals

6
MDR R&D Centers

6
Industry Verticals

15 million
vulnerability scans test cases

31 billion
security events processed per day

+30 million
network equipment and secure mobile phones

IDnomic
Trusted identities for people and devices

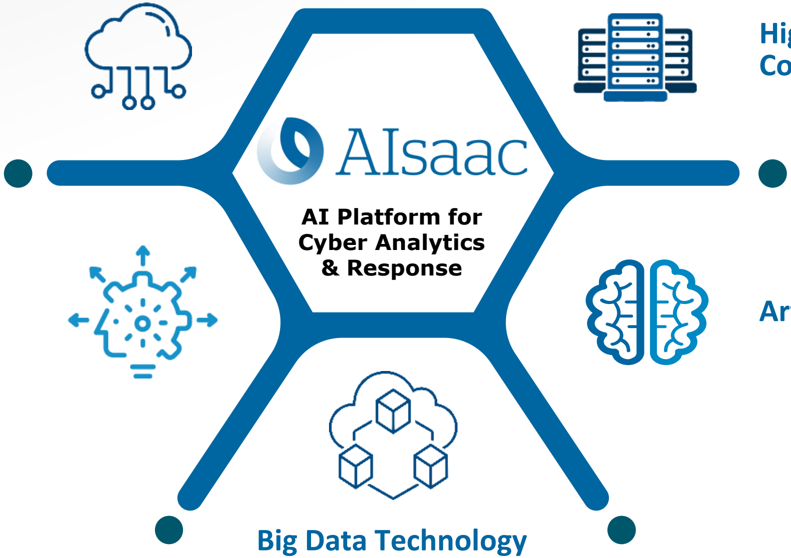
Evidian
Identity and Access Management

Trustway
Data Protection at rest and in motion

AIsaac
Patented AI Platform

AIsaac – Consolidating the technology core

OneCloud



AIsaac

AI Platform for Cyber Analytics & Response

Cloud native solution with hybrid and multi-cloud support

High Performance Computing

Intelligent Security Automation

Artificial Intelligence

Big Data Technology

What you get with our MDR service

Multi Vector Detection

End point, network, users, logs, cloud

&

Full Service Response

Investigation, verification, containment, mitigation

Delivered through

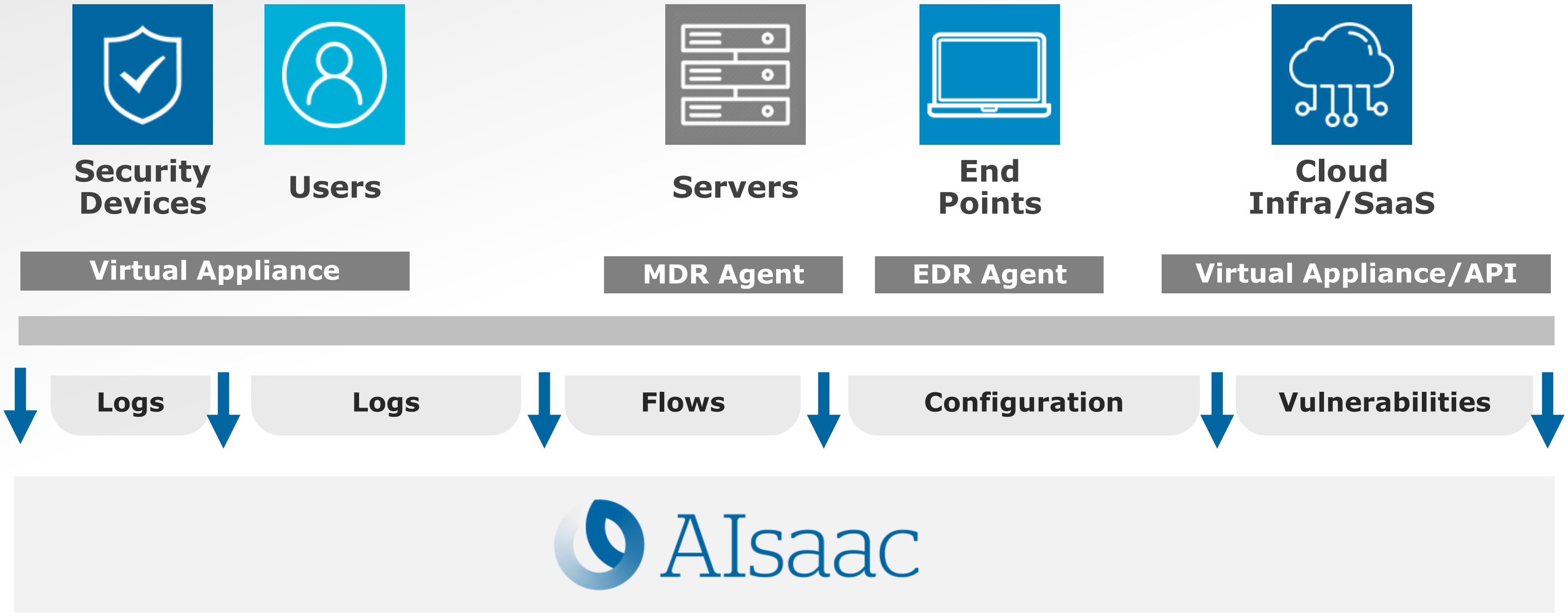
AIsaac: AI BASED MDR PLATFORM

Reduces your time to detect and time to respond

6000+ Experts in 15 SOCs

Provides high touch service

Collect & see across vectors centrally



Security Devices

Users

Servers

End Points

Cloud Infra/SaaS

Virtual Appliance

MDR Agent

EDR Agent

Virtual Appliance/API

Logs

Logs

Flows

Configuration

Vulnerabilities

AIsaac

We Mine Your Security Data Thrice

AIsaac Platform

1000+ Rules & Signatures

24x7 SOC Monitoring for known threats

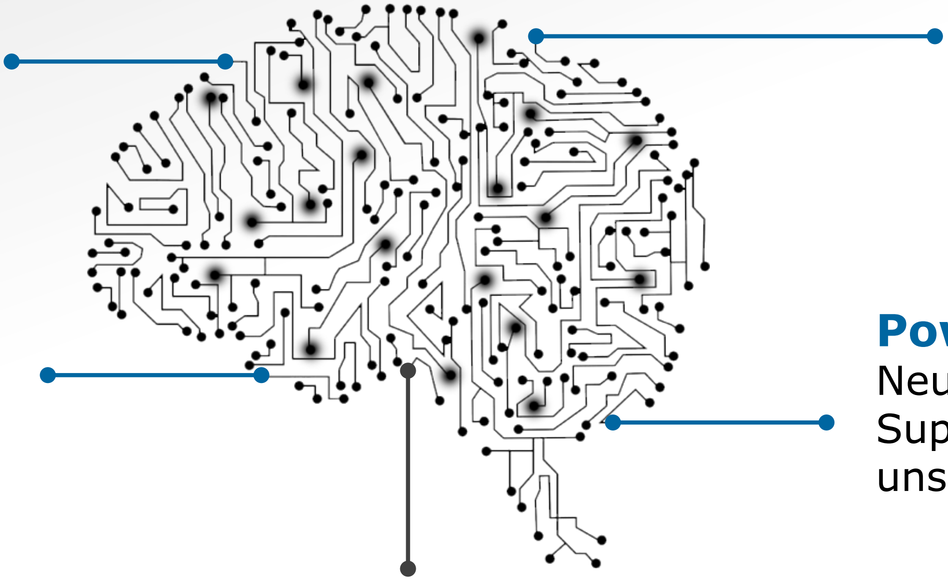
200+ Threat Intel sources

24x7 Threat Anticipation for known attackers

100+ Machine learning models

24x7 Threat Hunting for unknown threats / attackers

Detecting Advanced and Hidden Threats



Patented
AI platform

First Model
Deployed in
2011

31 Billion events
processed per day

Powered By
Neural Nets
Supervised and
unsupervised & NLP

GET DEEPER DETECTION

Client Success Stories

What We Detected With AI Models

ADVANCED MALWARE

Caught Hidden Banking Trojan
that went undetected by existing Symantec EPP, FireEye EDR, Qradar SIEM and NGFW.

DATA EXFILTRATION

Caught data leakage
that was bypassing the existing DLP and web gateway due to micro blogging.

LATERAL MOVEMENT

Detected lateral movement of attacker
from developer segment to production website which was missed by Anti-malware, NGFW and SIEM.

ROGUE SOFTWARE

Detected Rogue Software
On four servers in 450,000 nodes network even though it was cleaned up earlier by specialized IR team employed by customer.

PHISHING FRAUD

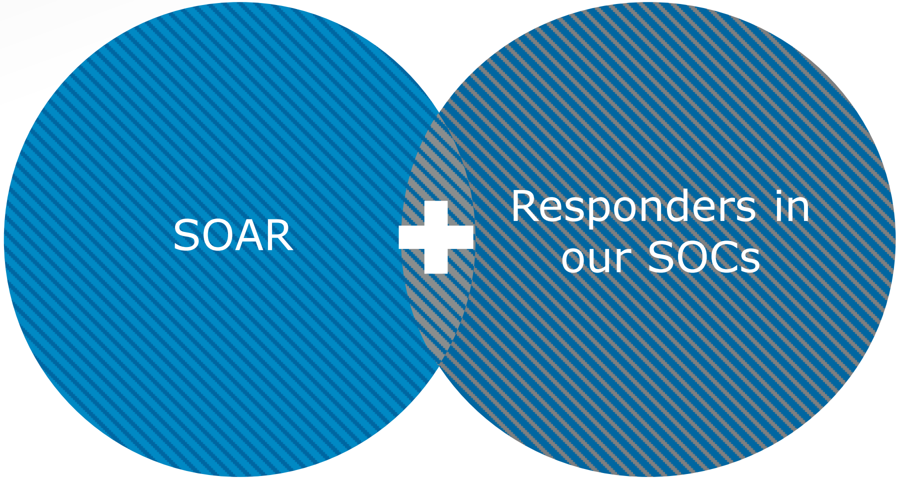
Prevented fraudulent transaction
from CEO’s email compromise in O365, which was missed by Email gateway and anti-phishing solutions.

Quickly Contain Your Threats With Automation

Auto Containment

Block attackers, quarantine machines, kill processes, remove accounts, stop connections & others

- Zero dwell time for attackers
- No effort from you

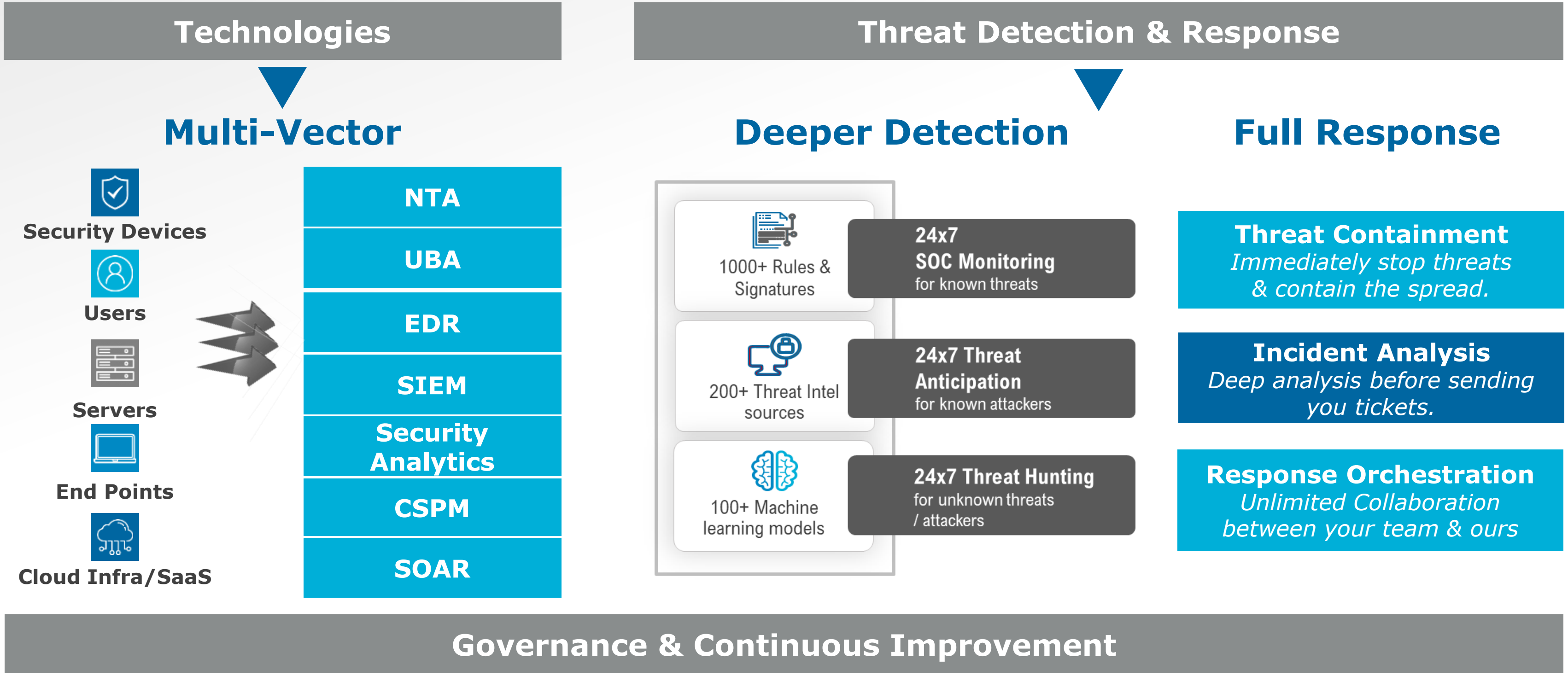


SOAR

Responders in our SOCs

The Full Solution

Managed Detection & Response



Technologies

Multi-Vector

Security Devices

Users

Servers

End Points

Cloud Infra/SaaS

NTA

UBA

EDR

SIEM

Security Analytics

CSPM

SOAR

Threat Detection & Response

Deeper Detection

1000+ Rules & Signatures

24x7 SOC Monitoring for known threats

200+ Threat Intel sources

24x7 Threat Anticipation for known attackers

100+ Machine learning models

24x7 Threat Hunting for unknown threats / attackers

Full Response

Threat Containment
Immediately stop threats & contain the spread.

Incident Analysis
Deep analysis before sending you tickets.

Response Orchestration
Unlimited Collaboration between your team & ours

Governance & Continuous Improvement

Summary of our MDR Service-Key Differentiators

Multi-Vector Technologies

Security Devices

Users

Servers

End Points

Cloud Infra/SaaS

NTA

UBA

EDR

SIEM

Security Analytics

CSPM

SOAR

Multiple technologies in a single platform - no silos

Deeper Detection

1000+ Rules & Signatures

[illegible] sources

100+ Machine learning models

24x7 SOC Monitoring for known threats

24x7 Threat [illegible] for known attackers

24x7 Threat Hunting for unknown threats / attackers

Large set of out-of-box content for detection

Full Response

Automation for fast containment

Threat Containment
Immediately stop threats [illegible]

Incident Analysis
Deep analysis before sending you tickets.

Response Orchestration
Unlimited Collaboration between your team & ours

Large team to support you at every step

Case study 1

Leader in European asset management

Company Profile

- Europe’s leading asset management firm with over 40+ offices
- $800+Bn AUA and recently been awarded Best Fund Administrator
- 2500 employees

Challenges

Since its founding in 2003, this firm has been the go-to company for many of the world’s leading private equity houses, real estate firms and private debt managers for local administrative, compliance issues and more. As a result, they dealt with sophisticated and targeted cyber attacks. It was also important that they showcase to clients that the data remains in the EU and that they conform to GDPR.

Solution

The customer needed a hybrid solution that can monitor for threats on the public cloud and their datacenters. When they came to us with a Managed SIEM requirement. But, after reviewing their needs and the risks they face. We proposed Atos MDR for their 800 assets placed across two locations; Luxembourg and Cortland.

The solution included 24/7 monitoring, and full integrations with existing security products. We further focused this client’s security posture on comprehensive Threat Hunting and incident response from our global SOC.

Why they chose Atos

- Tailored solution focused on customer needs
- Delivered as a full SaaS offering from the Atos EU cloud instance
- Mature GDPR consultants to support with compliance
- Local Project Management from Luxembourg
- Simple and straight forward implementation with clear timelines

Case study 2
Leading healthcare provider

Company Profile

- Leading healthcare provider in the United States
- Established in 1999
- Serving 100 hospitals in 26 states 24/7/365

Challenges

As a leading healthcare provider in the United States, this company brings deep clinical, operational, and technical expertise to its hospital partners. The business was aware they had gaps in their attack surface visibility across multiple sources. So, they were looking for a security vendor that can manage Crowdstrike, utilize logs from existing technology stacks, add SIEM, and auto-containment technology. And as a company working mostly with hospitals, they also needed to showcase HIPAA compliance.

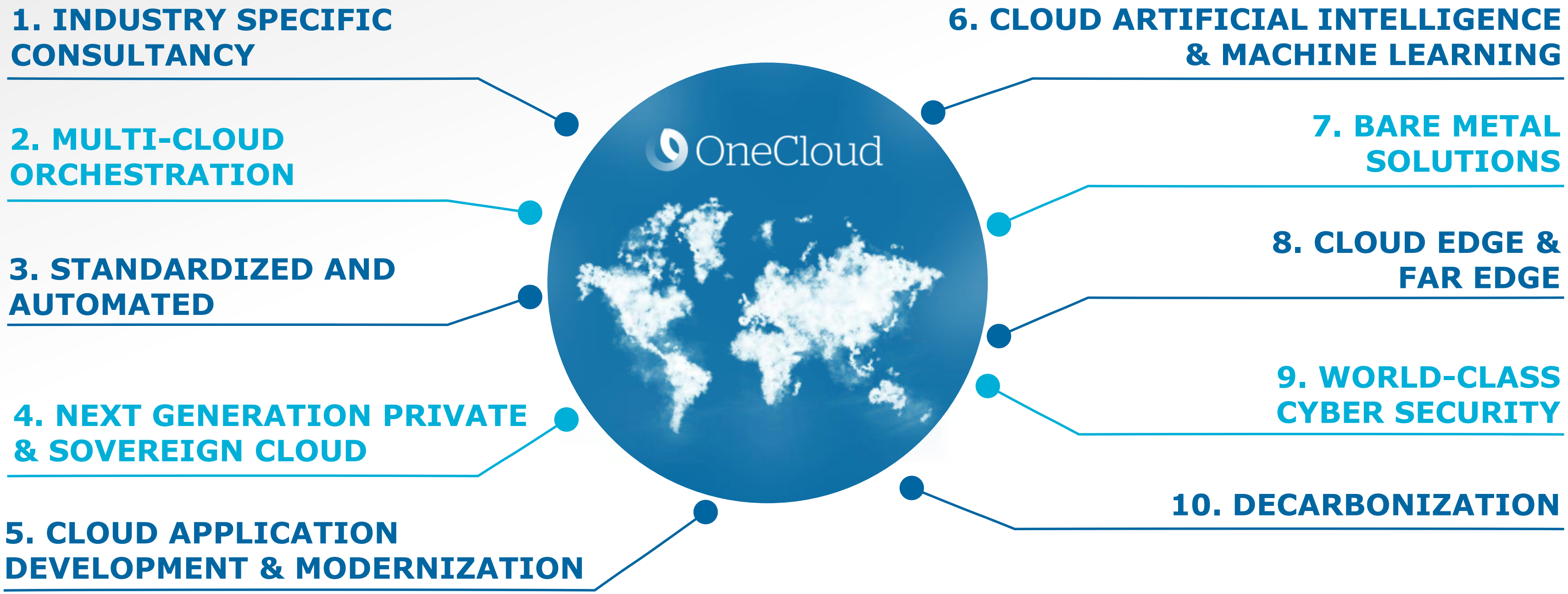
Solution

The client needed to progress from a Managed Crowdstrike service provider to a turnkey-style 24x7 MDR. Our solution consultants proposed Atos AI-Driven MDR along with Crowdstrike EDR. In Parallel to our implementation, our HIPAA consultants audited current practices and suggested a robust framework to stay compliant with HIPAA. We also suggested threat hunting to uncover low footprint threats along with 24/7 security monitoring, EDR, auto threat containment and incident response.

Why they chose Atos

- Ability to scale with the client as they grow
- Recognized managed detection and response provider - Atos<>Paladion
- Leading-edge auto containment capabilities
- Expertise delivering MDR for tele-health providers
- Threat hunting built-in to the MDR solution
- Ability to leverage and manage Crowdstrike
- Mature security compliance team with HIPAA expertise

Boost Factor for MDR GTM…..



1. INDUSTRY SPECIFIC CONSULTANCY
2. MULTI-CLOUD ORCHESTRATION
3. STANDARDIZED AND AUTOMATED
4. NEXT GENERATION PRIVATE & SOVEREIGN CLOUD
5. CLOUD APPLICATION DEVELOPMENT & MODERNIZATION
6. CLOUD ARTIFICIAL INTELLIGENCE & MACHINE LEARNING
7. BARE METAL SOLUTIONS
8. CLOUD EDGE & FAR EDGE
9. WORLD-CLASS CYBER SECURITY
10. DECARBONIZATION

Business Success Driven by Innovation

Early Wins

AI & Automation

Integration of key assets of Atos including HPC, OneCloud

Cloud Native, Multi-Cloud

Thank **YOU**

For more information please contact
Simone Glénat
simone.glenat@atos.net

Trusted partner for your **Digital Journey**

Atos