ENTERPRISE
SECURITY
WWW.ENTERPRISESECURITYMAG.COM ISSN 2691-4034 DECEMBER - 21 - 2020

SECURITY AUTOMATION EDITION

JOONHO LEE,
CO-FOUNDER AND CEO

Talisai

ACCOUNTABLE AI FOR COMPREHENSIVE INSIDER THREAT RISK MANAGEMENT

$15

ENTERPRISE
SECURITY
TOP 10
SECURITY AUTOMATION
SOLUTION PROVIDERS - 2020

COVER STORY

Talisai

ACCOUNTABLE AI FOR COMPREHENSIVE INSIDER THREAT RISK MANAGEMENT

By Russell Thomas

"I'll be back." For any sci-fi movie buff, this catchphrase by Arnold Schwarzenegger will always be eternal—immediately bringing back the memory of The Terminator movie. Despite the incredible promise that Artificial Intelligence (AI) holds, the film opens the audience's eyes to the havoc caused when AI goes wrong. Although the idea of a highly-advanced AI robot, with living tissue over a metal endoskeleton, programmed to find and kill somebody might seem light-years ahead of its time, it makes one wonder and question AI's accountability. This concern further becomes paramount today, considering that the proliferation of AI, machine learning (ML), and Advanced Data Analytics (ADA) have taken the center-stage in global enterprises to generate machine-based/data-driven decisions.

While ADA and AI, coupled with large volumes of relevant data, are designed to perform discrete and measurable tasks that benefit organizations, the algorithms themselves are typically opaque "Black Boxes" of complex code that does not translate easily to business-level understanding. The "unknown" errors created by Black Boxes can compound and ultimately impact ROI alongsidecreating untraceable regulatory violations or escalated business risk. Itthen becomes crucial for companies to address the lack of traceability, visibility, and accountability in ADA and AI with a governance framework that ensures reliable and explainable results. While the necessity of "intelligence" for artificial intelligence has become crucial, deploying the same is no easy feat. For long, many companies have been digging deep to find an ideal solution that can unlock the Black Box and delve into the rationale of AI-based decisions and recommendations. It was not until recently that an apt solution to this long-standing challenge came to the fore. Founded in 2018, California-based Talisai has introduced a game-changing real-time AI and data analytics oversight platform that bridges the gap between the promises of AI and its accountable execution. "We started the company as we wanted the machine-driven decisions to be accountable. By blending in the aspect of explainability and transparency of machine-based decisions, we support our clients to improve their decision-making processes," says Joonho Lee and Jonathan Heigel, Co-Founders at Talisai.

JOONHO LEE,
CO-FOUNDER AND CEO

The Difference that AI Accountability Makes

The core objectives of AI transparency and accountability in Talisai's platform are set with the goal of optimizing integration between human-driven processes and data-driven intelligence. The platform provides independent, real-time supervision of the algorithms, data, and business processes as they are developed, integrated, and deployed. It empowers enterprises to manage algorithmic and data risk with automatic traceability, real-time monitoring and alerts, and forensics, transforming the Black Box into a core trusted business asset.

By offering a vital ADA/AI oversight framework, systemic replay capability with explanations, Talisai allows its clients to dynamically view, understand and audit ADA/AI models, relationship to data, and business performance. The solution provides oversight through a two-pronged approach: bottom-up from the data layer and top-down from the business process layer.

A Renewed Approach to Insider Threat Prevention

While AI governance and accountability hold tremendous potential across various sectors, Talisai has distilled its concept of ADA/AI oversight into the domain of insider threat prevention and people risk management. Efficient insider threat mitigation must inculcate accountability with explainable and retraceable results for further action.

Companies today need to deploy risk mitigation programs that are as sophisticated as the crimes themselves.

JONATHAN HEIGEL,
CO-FOUNDER AND COO

The first step to building such a program is to understand that the costliest and most challenging threats come from an unexpected source: trusted yet rogue insiders including vendors and contractors. Along the same lines, it is crucial to consider that human capital and supply chains are the most significant asset for a company. Be it risks posed to the people or by the people, the stakes are really high. The ongoing COVID-19 pandemic has further aggravated the situation by triggering a fresh wave of cybersecurity threats, making cyber risk management more important than ever. Throughout the pandemic, once-trusted employees with physical security controls succumbed to the immense stresses and heightened anxieties of the moment, leading to high-profile insider threat situations. As a matter of fact, the statistics relative to risks of insider threats are dismal, as an estimated 75 percent of employees have stolen at least twice from their employer, and an estimated 34 percent of data breaches are orchestrated by rogue insiders. The costs are too high to blindly trust the employee base, especially when the average data breach costs $8.19 million.

Be it good-faith mistakes or sheer negligence, the impact on business invariably remains the same. As modern threats integrate all possible attack vectors, including insiders, business processes, supply chains, and even cultural aspects, companies need to change the traditional siloed approach to risk management for ensuring business continuity and resiliency.

To this end, Talisai has teamed up with Polaris Corporate Risk Management—an industry leader in the corporate risk management space with over 50 years of global security and investigations experience. The companies have aligned their investigative, analytical, and technological expertise to address threats posed by rogue insiders with their new, state-of-the-art AI tool: "People at Potential Risk," or PAPR.

Stephen Ward, CEO at Polaris Corporate Risk explains, "Often, despite multi-layered security frameworks, companies fail to sharpen their focus on insiders, considering the inherent 'trust' bias around insider threats, which often leads to ineffective detection and significant impact."

As a cutting-edge AI tool, PAPR marries Polaris' industry-leading security and investigative strategies with Talisai's revolutionary machine-learning capabilities to successfully identify and mitigate potential threats with automated evidence chains. With this strategic partnership, Polaris Risk and Talisai aim to help organizations prevent, monitor, and respond to the various forms of insider threats, offering comprehensive services that can be deployed fully or incrementally based on an organization's specific needs.

In addition to AI-monitoring, the broader suite of Polaris and Talisai's offering includes background screenings, cyber monitoring and analytics, site inspections and assessments, data forensics, dark web monitoring, incident response, and remediation alongside investigations.

Adopting a Proactive Approach to Mitigating Human Capital Risk

The PAPR solution integrates and analyzes surveillance data from five key pillars of enterprise risk: communications, business transactions, corporate records, employees, and customers. It then executes a set of behavior analytic algorithms against this data, resulting in an explainable list of people at potential risk before an incident can even occur. Few, if any, risk management solution providers offer insider threat tools so proactive, despite the inherent urgency of internal threat events. It even provides a full evidence chain, forensically explaining the rationale for each individual's selection. Consequently, this drastically improves the productivity of cybersecurity analysts and investigators, as well as compliance and audit personnel.

> "By blending in the aspect of explainability and transparency of machine-based decisions, we support our clients to improve their decision-making processes"

STEPHEN WARD,
CEO, POLARIS CORPORATE RISK

The solution leverages both ML-based AI algorithms and analyst-designed deterministic algorithms to continually self-monitor, cross-check, train, and enhance the automated analysis. This approach strategically aligns with the corporate shift from point-in-time risk assessment to real-time risk management. It also enables companies to monitor possible biases, as well as unexpected data velocity and volumes that generate unintended anomalies before its results impacting business. Proactivity and prevention have become the primary objective when managing insider threats. In doing so, most of today's solutions face two key barriers: a lack of data transparency and a lack of analytical expertise—PAPR offers both. "We offer a probabilistic risk assessment on an ongoing basis. Every second matters during cyber breach or leak scenarios, and through our solution, we ensure that no time is wasted between an early indication of potential risk and actual incident detection," says Lee and Ward.

> “Every second matters during cyber breach or leak scenarios, and through our solution, we ensure that no time is wasted between an early indication of potential incident and actual incident detection”

While accounting for rogue insiders is vital, every facet of a company's risk profile is affected by its personnel, from supply chain, travel procedures to pandemic response planning. Though PAPR is designed to address insider threats, it also provides comprehensive and location-specific travel security coverage, international executive protection, improves external threat and supply chain risk monitoring, and effectively manages foreign facilities and situational risk, alongside pandemic training and contingency plans.

Solving Problems at the Core

Talisai offers its services with a range of installation options, both on cloud and on-premise, depending on its customers' needs. Unlike traditional user-behavior analytics products, Talisai's solution is much more pragmatic and provides an immediate return on investment with automated governance over AI and data

As a result, companies across a wide range of market segments, including highly-regulated industries like financial services and healthcare, leverage Talisai'sservices today.

For example, Talisai has been effectively helping its clients in the healthcare sector with the explainable AI analytics during the COVID-19 severity. With its core AI and data analytics oversight platform, Talisai also improves risk management tool for individuals covering weather, social unrest, and cyber-espionage successfully. The company aims to further build more vertical data and models to support large companies focusing on not only their individuals but also supply chains. Not just this, considering that digital banking and digital assets such as cryptocurrencies are increasingly being adopted in the financial services industry, which amplifies the risk of money laundering, Talisai plans to expand its platform's capabilities to bolster anti-Money Laundering measures. ES

ENTERPRISE
SECURITY
WWW.ENTERPRISESECURITYMAG.COM
DECEMBER - 21 - 2020

Talisai
TOP
SECURITY
AUTOMATION
Solution Providers
2020
Recognized by
ENTERPRISE SECURITY

Talisai

TOP
SECURITY
AUTOMATION
Solution Providers
2020
Recognized by
ENTERPRISE SECURITY

The annual listing of 10 companies that are at the forefront of providing Security Automation solutions and impacting the marketplace