

AI for Security Analyst



Devindra Chainani

The Story

Jill is a cyber security analyst, fighting an asymmetric battle against prolific, relentless and sophisticated attackers. Her employer, a Fortune 500 company, is attacked thousands of times a month. She needs to respond to threats within minutes instead of days. Overworked and with skewed work-life balance, she has requested her management to hire more security analysts. Her management has sanctioned multiple open positions, but a global shortage of 3.4 million skilled security professionals makes finding and retaining talent a cumbersome task. Jill wants to become proactive and get out of the perpetual reactive mode. Her team has built several dashboards that analyze millions of threat signals but given her long hours at work, she often struggles to create coherent trend reports and generate insights for taking preventive actions. Attackers hide behind noise and weak signals that go undetected since Jill and her security team's capacity is limited by the team's size and the natural limits of human attention.



The Solution

AI-powered,
Trustworthy Security
Assistant that enables
analysts to ***respond to***
threats in real time,
process signals at
machine speed, and
assess risk exposure in
minutes.



Top Three Scenarios

Incident response

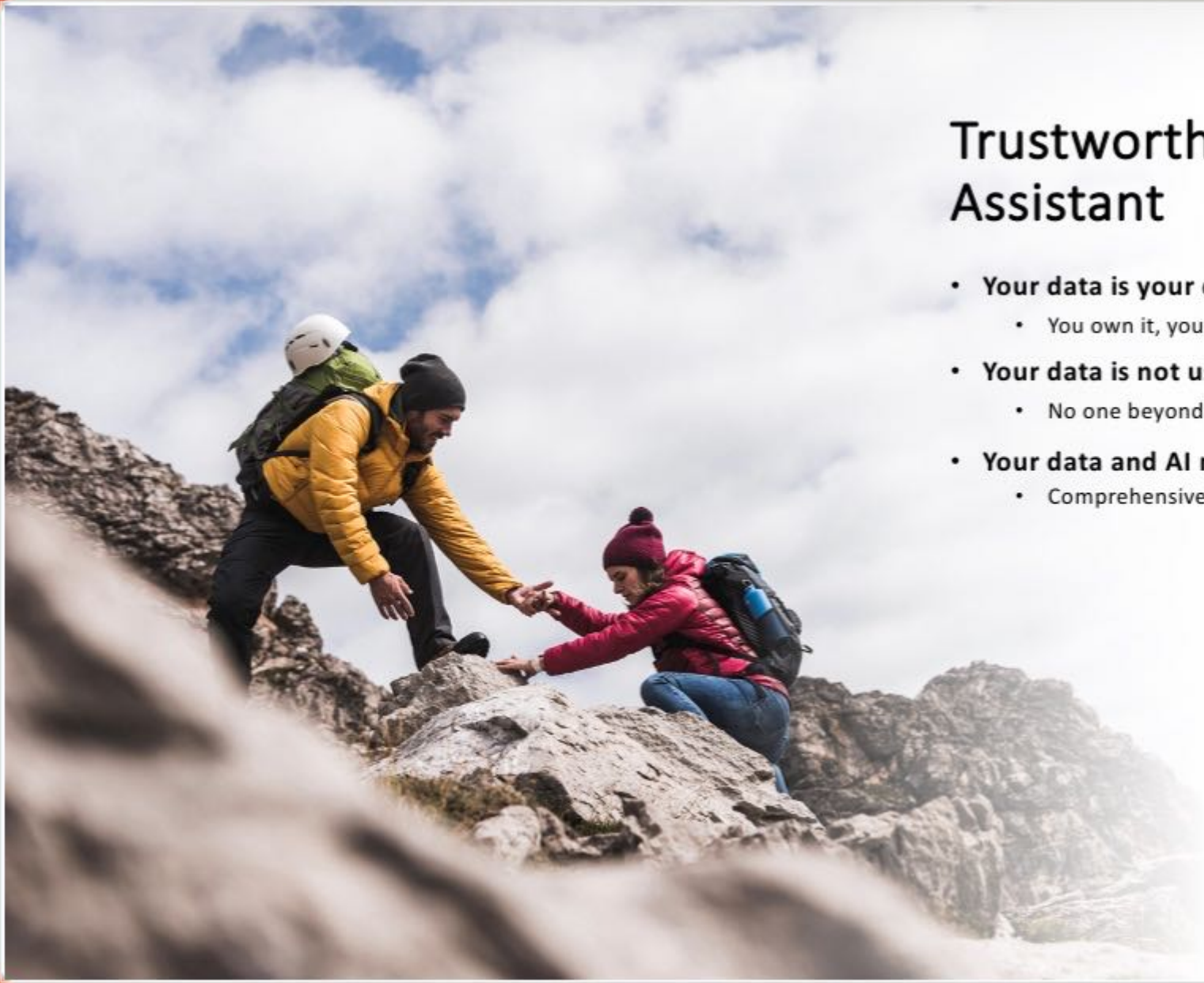
Respond to in-progress attacks in real time, get steps for remediation

Security analysis

Summarize incidents, prepare reports in a ready-to-share format

Threat hunting

Examine all assets individually to discover vulnerabilities

A photograph of two hikers on a rocky mountain trail. The hiker on the left, wearing a yellow jacket and a white helmet, is reaching out to assist the hiker on the right, who is wearing a red jacket and a red beanie. They are both carrying backpacks. The background shows a cloudy sky and rugged mountain terrain.

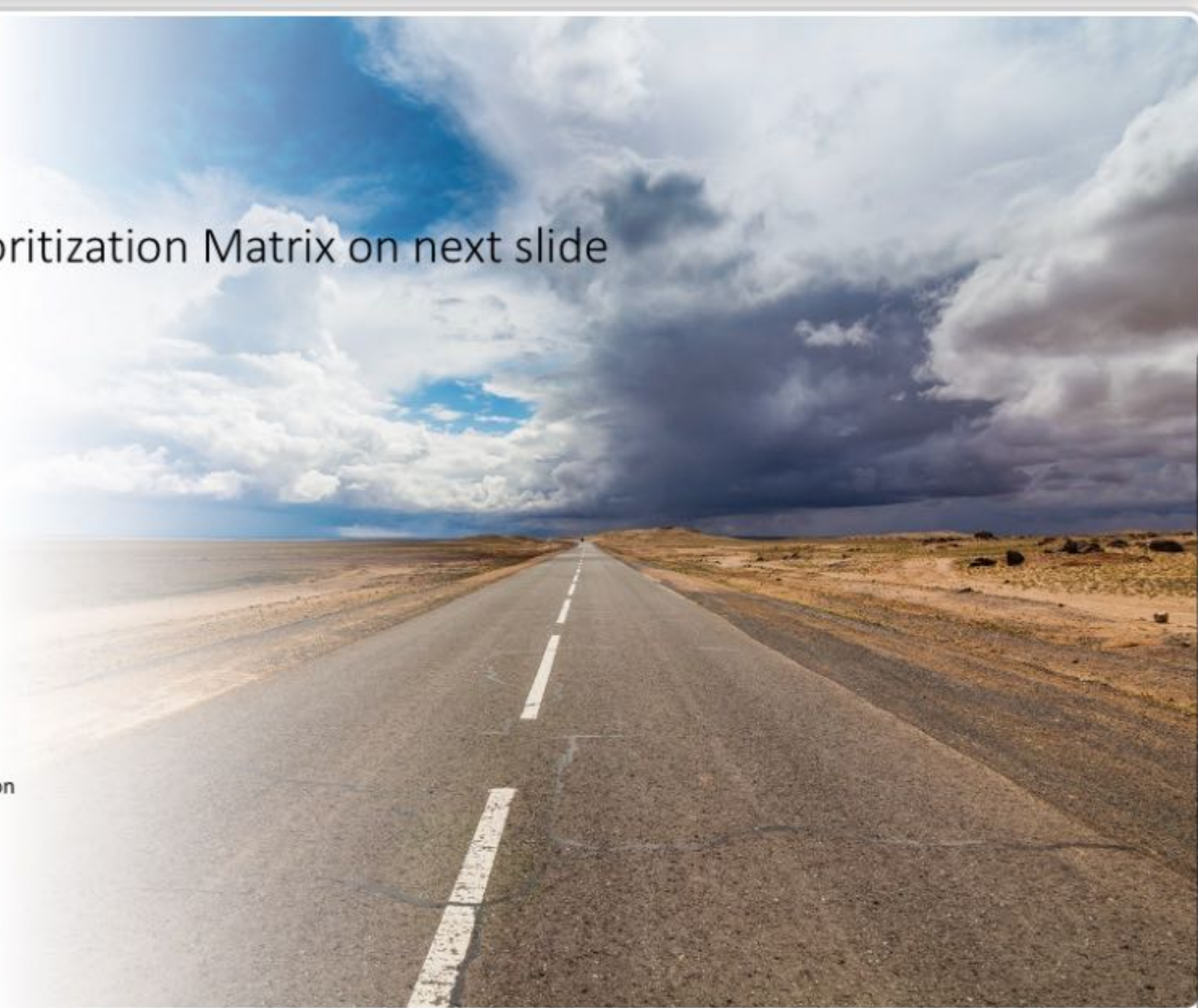
Trustworthy Assistant

- **Your data is your data**
 - You own it, you control it, you choose how to leverage it
- **Your data is not used to train foundation models**
 - No one beyond your organization benefits from your data
- **Your data and AI models are compliant**
 - Comprehensive enterprise compliance and controls

Roadmap

Stack Rank – See Prioritization Matrix on next slide

- **Incident response**
 1. Collaboration tool integration
 2. Logs and Audit reports
 3. Low-code automation
- **Security analysis**
 1. Trend analysis
 2. Data connectors
 3. Reports as presentations
- **Threat hunting**
 1. Maturity score
 2. Zero Trust recommendation
 3. Least privilege recommendation



Feature Prioritization Matrix

		Incident response			Security analysis			Threat hunting		
	Weight	Logs and audit reports	Low code automation	Collab tool integration	Data connectors	Trend analysis	Presentations	Maturity score	Least privilege reco	Zero Trust reco
Multi-Geo	5	4	8	9	8	8	9	8	7	7
Cost	6	6	3	9	3	6	9	7	7	7
Supportability cost	6	5	2	9	2	5	9	7	3	3
Documentation cost	6	5	2	8	2	5	9	6	2	2
Usage Driver	10	8	5	8	9	9	5	5	7	8
Retention Driver	8	5	9	7	9	7	5	6	6	6
Additional Revenue Driver	9	8	8	4	9	5	3	7	8	8
Thought Leader	6	3	6	2	6	9	2	9	9	9
TOTAL										
		Incident response			Security analysis			Threat hunting		
	Weight	Logs and audit reports	Low code automation	Collab tool integration	Data connectors	Trend analysis	Presentations	Maturity score	Least privilege reco	Zero Trust reco
Multi-Geo	5	20	40	45	40	40	45	40	35	35
Cost of Goods	6	36	18	54	18	36	54	42	42	42
Supportability cost	6	30	12	54	12	30	54	42	18	18
Documentation cost	6	30	12	48	12	30	54	36	12	12
Usage Driver	10	80	50	80	90	90	50	50	70	80
Retention Driver	8	40	72	56	72	56	40	48	48	48
Additional Revenue Driver	9	72	72	36	81	45	27	63	72	72
Thought Leader	6	18	36	12	36	54	12	54	54	54
TOTAL		326	312	385	361	381	336	375	351	361