

MICHIGAN STATE
UNIVERSITY

Alpha Presentation

Intelligent Network Security for High-Risk Traffic

The Capstone Experience

Team McKesson

Aneesh Kapole

Dev Khakhar

Karena Lam

Aisha Latif

Divya Nadella

Conner O'Sullivan

Department of Computer Science and Engineering
Michigan State University



From Students...
...to Professionals

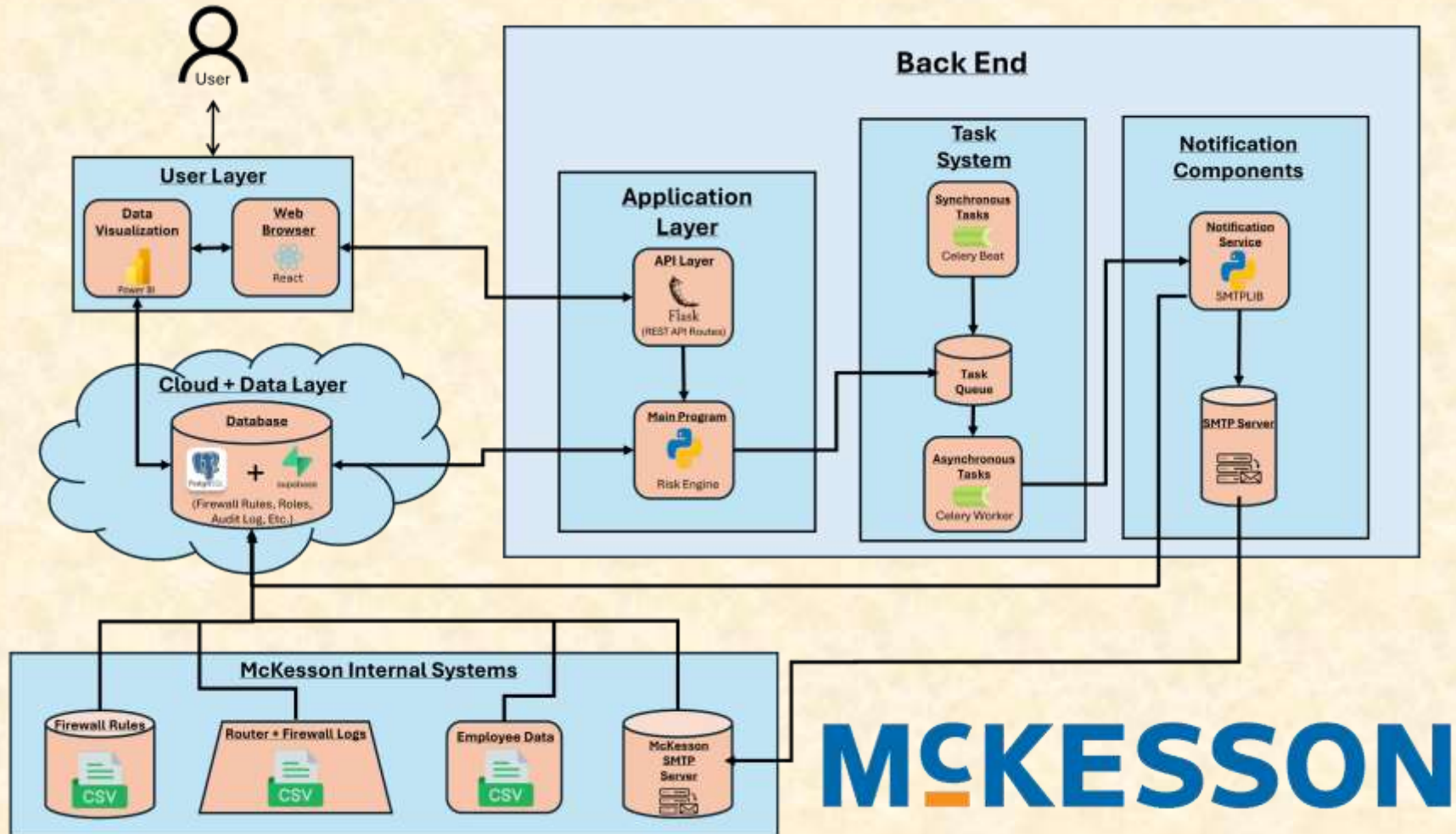
Fall 2025

Project Overview

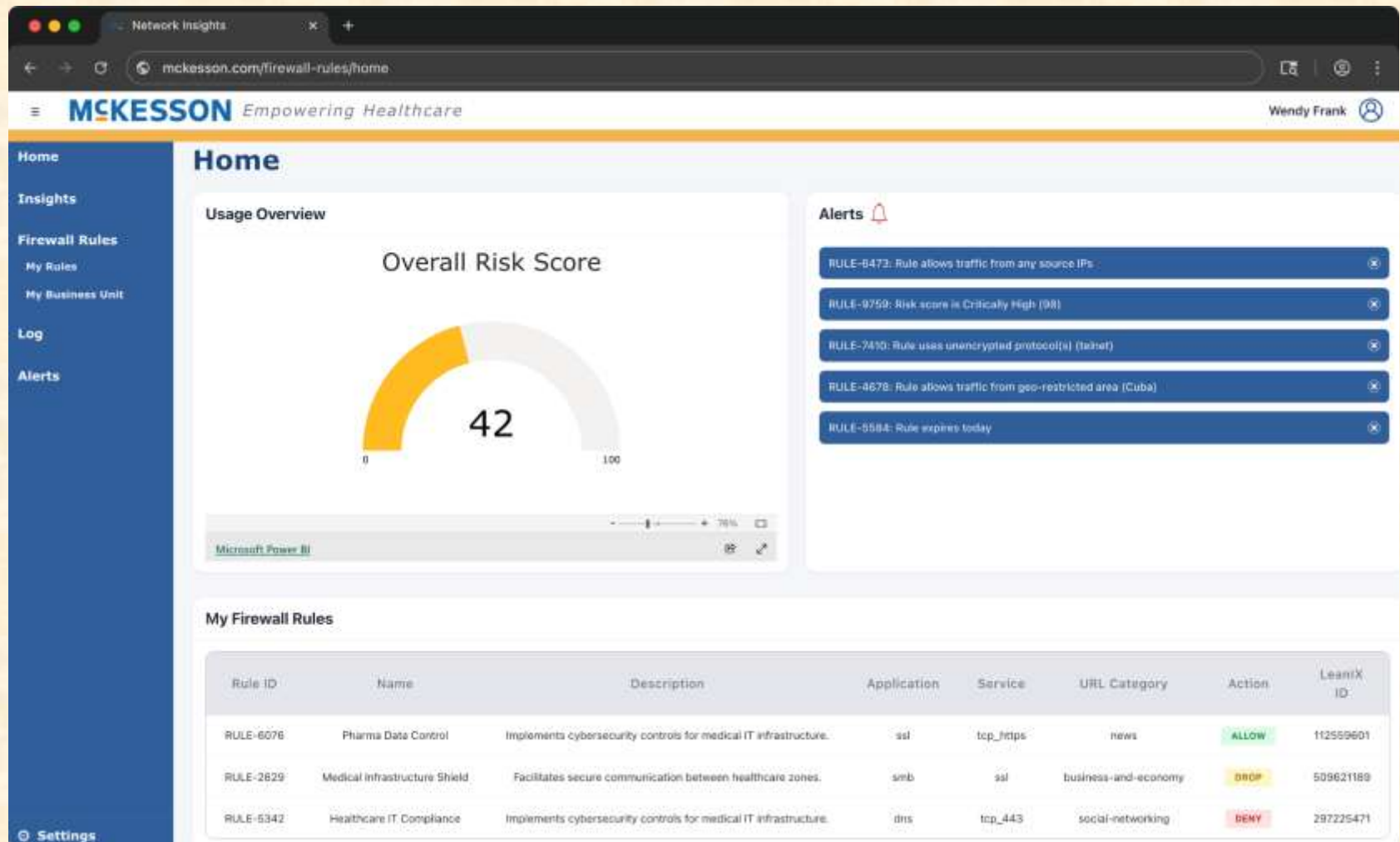
- Firewall rules help the firewall decide how to control access to networks
- Difficult for a cybersecurity unit to analyze thousands of rules
- The Intelligent Network Security system automates risk analysis process to evaluate risk of firewall rules
- Web application designed to manage firewall rules and visualize insights, alerts, and attestations



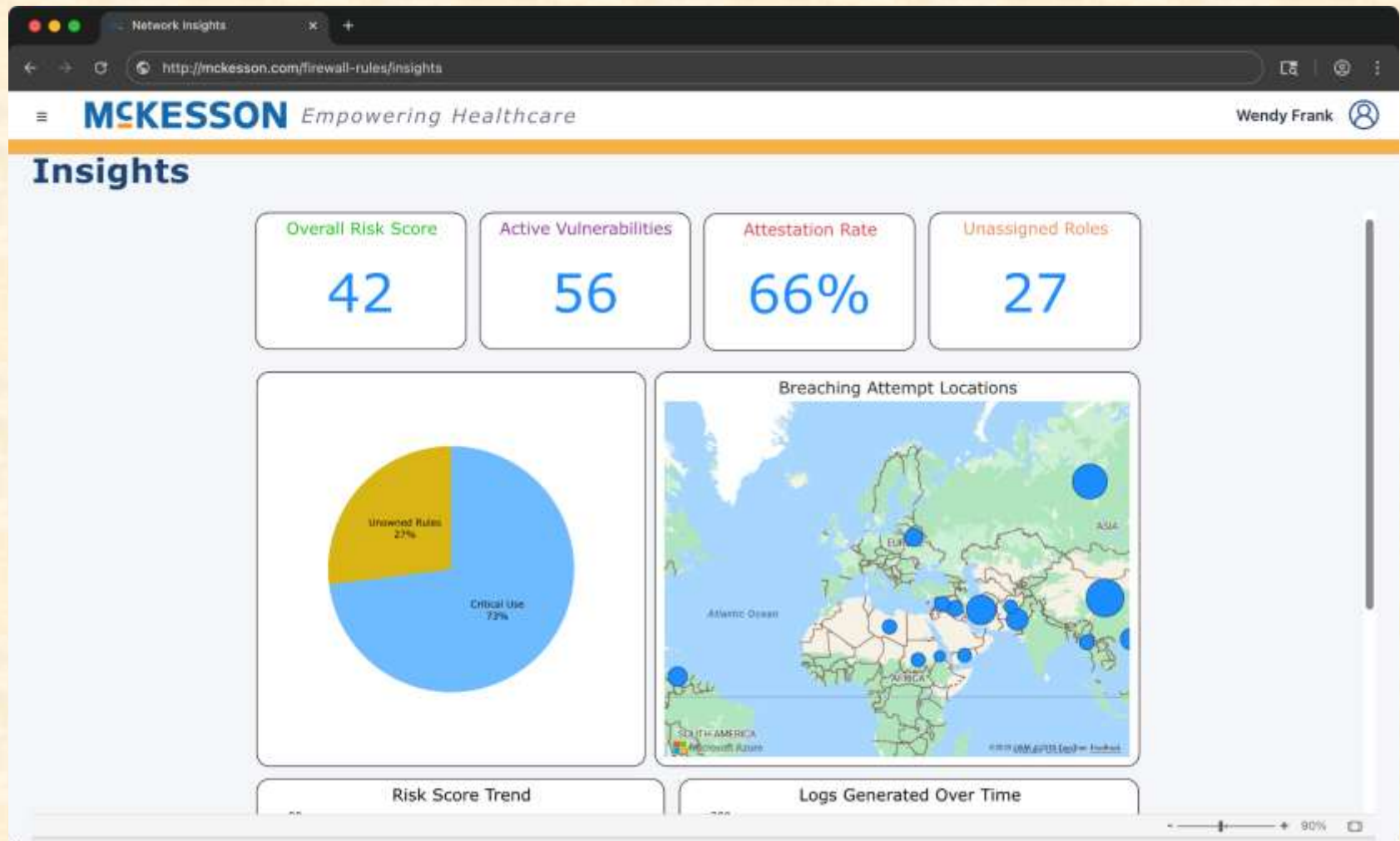
System Architecture



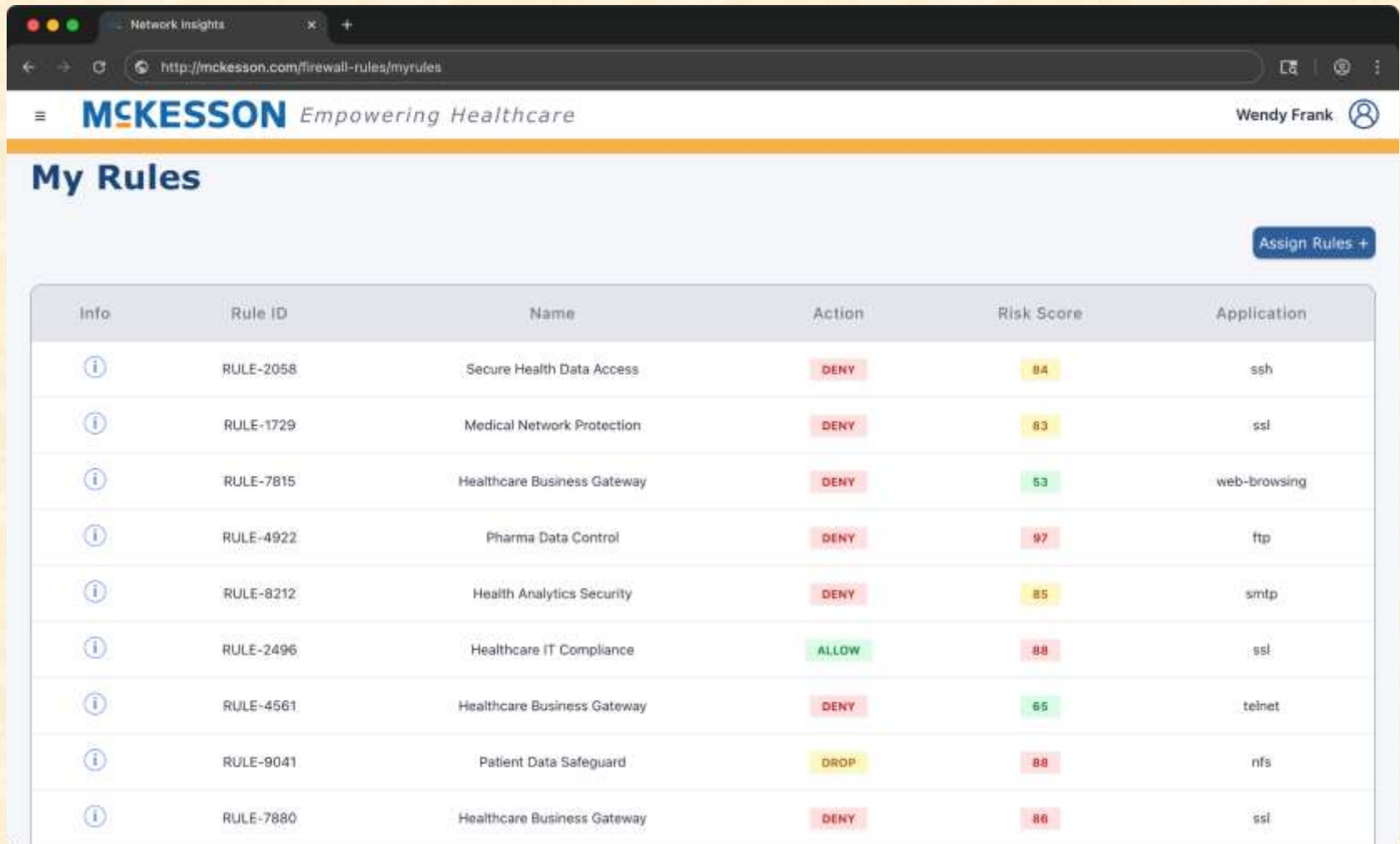
Home



Insights



My Rules



Info	Rule ID	Name	Action	Risk Score	Application
	RULE-2058	Secure Health Data Access	DENY	84	ssh
	RULE-1729	Medical Network Protection	DENY	83	ssl
	RULE-7815	Healthcare Business Gateway	DENY	53	web-browsing
	RULE-4922	Pharma Data Control	DENY	97	ftp
	RULE-8212	Health Analytics Security	DENY	85	smtp
	RULE-2496	Healthcare IT Compliance	ALLOW	88	ssl
	RULE-4561	Healthcare Business Gateway	DENY	65	telnet
	RULE-9041	Patient Data Safeguard	DROP	88	nfs
	RULE-7880	Healthcare Business Gateway	DENY	86	ssl



Alerts

Network Insights

http://mckesson.com/firewall-rules/alerts

MCKESSON Empowering Healthcare

Wendy Frank

Alerts

Unresolved Alerts

Rule ID	Risk Score	Description	Create Date	
RULE-6473	56	Rule allows traffic from any source IPs	2025-09-27T22:27:58	Resolve
RULE-9759	98	Risk score is Critically High (98)	2025-09-27T21:13:46	Resolve
RULE-7410	24	Rule uses unencrypted protocol(s) (telnet)	2025-09-27T21:13:05	Resolve
RULE-4678	10	Rule allows traffic from geo-restricted area (Cuba)	2025-09-27T21:12:12	Resolve
RULE-5584	3	Rule expires today	2025-09-27T21:10:51	Resolve

Alerts History

Rule ID	Risk Score	Description	Create Date
RULE-6473	56	Rule expires in 7 days	2025-09-27T22:28:12



What's left to do?

- Assign Rules functionality
- Data integration with Power BI
- Comparison among business units
- Add more criteria to risk engine
- Analysis of logs
- Notification system

Questions?

?

?

?

?

?

?

?

?

?

