

**MICHIGAN STATE**  
**UNIVERSITY**

# Beta Presentation

## Endpoint Data Monitoring and Analysis Agent

### The Capstone Experience

Team Rook

Jared Clark

Drew Gilbertson

Bohao Gao

Jeremy Specht

Vikram Thakur

Department of Computer Science and Engineering  
Michigan State University

Spring 2018



*From Students...  
...to Professionals*

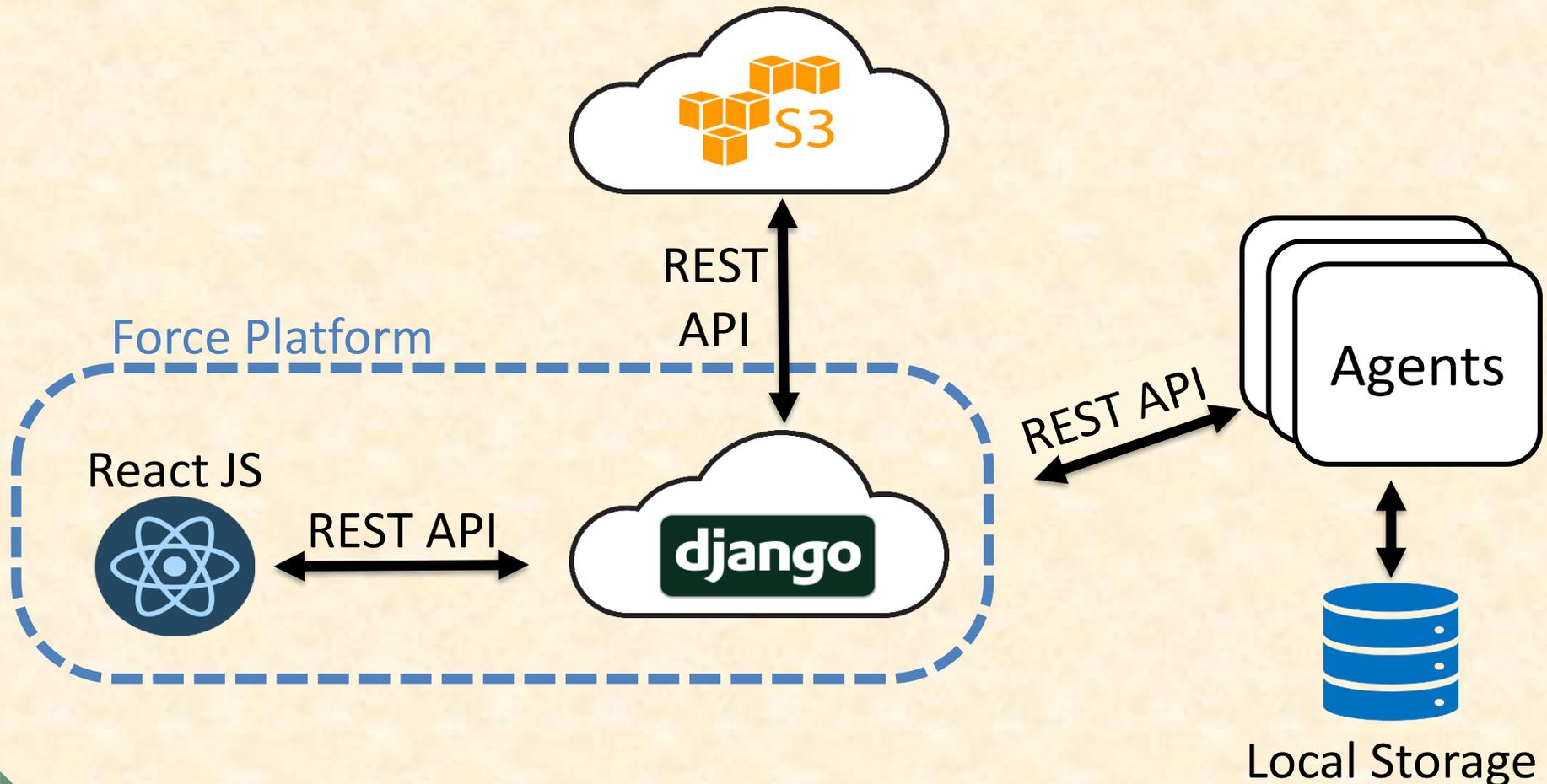
# Project Overview

---

- Endpoint Agent Log Collection
  - Cross Platform Compatible
- Communication Channels for Data
  - Configurable
- Web Application to Analyze Agent
  - Configuration
    - Log Paths, Storage Location
  - Health Analysis
    - Alert Priorities



# System Architecture



# Agent Management Console

The screenshot shows a web browser window with the URL `localhost:8082/agents/health`. The page title is "AGENT MANAGEMENT CONSOLE". The navigation bar includes "ROOK SECURITY", "WORKSPACE", "CONSOLE", "SETTINGS", "AGENTS", "SEND FEEDBACK", and a user profile "JS".

Below the navigation bar, there are buttons for "AGENT HEALTH" (with a plus icon), "CONFIGURATION" (with a gear icon), "Select Client" (with a dropdown menu showing "Dow"), "Select Agent" (with a dropdown menu showing "33"), and "MANAGE CLIENT KEYS".

The main content area is divided into several sections:

- Agent Info:** Client: Dow, Agent ID: 33, Operating System: Windows, OS Version: Microsoft Windows 10 Home, IP Address: 35.20.196.156, Hostname: DESKTOP-2013QQB.
- Log Volume (Last Hour):** Security: 0, System: 0.
- Health Status:** Agent Health Status: Unresponsive, Last Check-in: 2018-03-31 22:37:50.574851.
- Agent 33 Alerts:** Agent 33 for Dow has not made contact in 2741 minutes. Last checkin time: 2018-03-31 22:37:50.574851.
- Global Alerts:** A list of alerts for agents 1 through 6, all indicating they have not made contact in 20202 minutes. The last checkin times range from 2018-03-19 19:37:17.986950 to 2018-03-19 19:37:29.662714.



# Agent Configuration Tab

The screenshot shows a web browser window with the URL `localhost:8082/agents/config`. The page is titled "AGENT MANAGEMENT CONSOLE" and features a dark theme with yellow accents. The navigation bar includes "ROOK SECURITY", "WORKSPACE", "CONSOLE", "SETTINGS", and "AGENTS", along with a "SEND FEEDBACK" button and a user profile "JS".

The main content area is divided into two sections:

- Change Interval:** This section allows users to modify the monitoring interval. It shows a "Current Interval" of "600 Seconds" and a "New Interval" input field. An "UPDATE" button is located below the input field.
- Log File Paths:** This section displays a list of log file paths: `/var/log/syslog` and `/var/log/williflog`. Below the list are controls to "Add Path" (with an "ADD" button) and "Remove Path" (with a "REMOVE" button).

A "SAVE CHANGES" button is positioned to the right of the Log File Paths section. At the top of the configuration area, there are dropdown menus for "Select Client" (set to "Meijer") and "Select Agent" (set to "5"), and a "MANAGE CLIENT KEYS" button.



# Agent Key Management Tab

ROOK SECURITY

ACTIVE AGENT KEYS

Key Name	Client	Key	Date Created	Agents Created	
Second Key	Union Pacific	04418aa233ad59b8	2018-03-2	0	Delete
New Key	Dow	0c2dde41bb8e9113	2018-03-2	9	Delete
Second Key	Dow	3cd69b4364a3a962	2018-03-2	0	Delete
Michigan Region	Meijer	5749f6a1481de989	2018-03-2	0	Delete
First Key	Dow	62b3df4dd2b8a532	2018-03-2	1	Delete
BetaPrep	Dow	ac09af4e6bff4728	2018-03-3	1	Delete

Client Name

Key Name

CREATE NEW KEY Close

SEND FEEDBACK JS

MANAGE CLIENT KEYS

Add Path:

ADD

Remove Path:

REMOVE



# Windows Agent Product Validator

ROOK SECURITY

## ROOK Agent System

Step 1: Please Choose your Operation System

- Unix
- Windows

Step 2: Please Input your Key

Key:

Step 3: Click "Submit" button to verify your ClientKey

Submit

Welcome to ROOK Agent



# What's left to do?

---

- UI/UX Refinement
- Further Bug Testing
- S3 Credential Management [Stretch Goal]



# Questions?

---

?

?

?

?

?

?

?

?

?

